2018

Medical Identity Theft and Palm Vein Authentication: The Healthcare Manager's Perspective

Cruz Cerda III
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral dissertation by

Cruz Cerda, III

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. Nikunja Swain, Committee Chairperson,
Applied Management and Decision Sciences Faculty

Dr. Anthony Lolas, Committee Member,
Applied Management and Decision Sciences Faculty

Dr. Raghu Korrapati, University Reviewer
Applied Management and Decision Sciences Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2018

Abstract

Medical Identity Theft and Palm Vein Authentication: The Healthcare Manager's Perspective

by

Cruz Cerda III

MA, New York University, 1995

AB, Harvard University, 1993

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Applied Management and Decision Sciences

Walden University

March 2018

Abstract

The Federal Bureau of Investigation reported that cyber actors will likely increase cyber intrusions against healthcare systems and their concomitant medical devices because of the mandatory transition from paper to electronic health records, lax cyber security standards, and a higher financial payout for medical records in the deep web. The problem addressed in this quantitative correlational study was uncertainty surrounding the benefits of palm vein authentication adoption relative to the growing crime of medical identity theft. The purpose of this quantitative correlational study was to understand healthcare managers' and doctors' perceptions of the effectiveness of palm vein authentication technology. The research questions were designed to investigate the relationship between intention to adopt palm vein authentication technology and perceived usefulness, complexity, security, peer influence, and relative advantage. The unified theory of acceptance and use of technology was the theoretical basis for this quantitative study. Data were gathered through an anonymous online survey of 109 healthcare managers and doctors, and analyzed using principal axis factoring, Pearson's product moment correlation, multiple linear regression, and 1-way analysis of variance. The results of the study showed a statistically significant positive correlation between perceived usefulness, security, peer influence, relative advantage, and intention to adopt palm vein authentication. No statistically significant correlation existed between complexity and intention to adopt palm vein authentication. These findings indicate that by effectively using palm vein authentication, organizations can mitigate the risk of medical fraud and its associated costs, and positive social change can be realized.

Medical Identity Theft and Palm Vein Authentication: The Healthcare Manager's Perspective

by

Cruz Cerda III

MA, New York University, 1995

AB, Harvard University, 1993

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Applied Management and Decision Sciences

Walden University

March 2018

Dedication

I dedicate this research to my mother and father for their unwavering support and for believing in me. I graciously express appreciation for their extraordinary understanding and dedication. I also dedicate this work to the nation's families and children who live in poverty. May this study make a contribution to higher quality healthcare.

Acknowledgments

First and foremost, I would like to thank God for encouragement, support, and inspiration in assisting me in completing this dissertation, and with whom all things are possible. Secondly, I want to extend special recognition and sincere gratitude to my mentor and committee chairperson, Dr. Nikunja Swain, whose sage leadership guided me in this academic journey of discovery and allowed my dream of being the first in the history of my family to earn a Ph.D. degree. I will always be indebted. Many thanks to my committee members, Dr. Anthony Lolas and Dr. Raghu Korrapati, for contributing discerning insights and expertise that significantly impacted the quality of this study.

I extend my gratitude to Dr. Faith-Michael Uzoka for sharing his research and the research of his team and for granting me permission to use and modify his survey instrument. I also extend my sincere thanks to friends and colleagues for their constant encouragement to always move forward through the doctoral study process.

To Nevin Dolcefino, Executive Vice President, Innovative Artists, for his assistance, encouragement, and unwavering support. I am profoundly indebted.

Finally, I thank Walden University's College of Management and Technology faculty and staff and Walden University's Library staff for their great support during this journey.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

Most enterprises are cognizant of the importance of competitive tools and leading-edge information technology solutions that could assist in gaining a competitive advantage (Ahmad, Bosua, & Scheepers, 2014). Palm vein authentication, an emerging technology, is a means of automatically recognizing a person by analyzing the pattern of veins 3 mm below the surface of the human palm (Al-Juboori, Wu, & Zhao, 2013). Palm vein authentication systems use vascular patterns as personal identification data. This sophisticated technology could play a major role in protecting the assets of healthcare organizations and in improving patient safety.

Because of its success in confirming a person's identity, palm vein authentication may be an effective tool to manage the germinating problem of medical identity theft. A 2012 report by the Ponemon Institute estimated that there were 1.52 million victims of medical identity theft in 2012. In 2013 there were 1.84 million victims of medical identity theft, which represented a 19% increase from 2012 (Ponemon Institute, 2013). In 2014, the Ponemon Institute calculated the number of medical identity theft victims to be approximately 2.32 million victims, which represented a 21.7% increase from the previous year or 481,657 new cases (Ponemon Institute, 2015).

At present, palm vein authentication lacks widespread adoption in the United States; however, Japanese financial institutions have used this technology since 2004 to confirm the identity of customers (Watanabe, 2008). Given a decade of large-scale practical results and the growing problem of medical identity theft (Ponemon Institute, 2013), I investigated healthcare industry leaders' perspectives on palm vein

authentication to provide key industry decision-makers information regarding whether to invest in palm-vein-based identification systems.

Albert Camus once said, “Life is the sum of all your choices.” These choices are the results of the decision making process. Although this process manifests itself ubiquitously, I focused on one portion of the decision making process: identification. Specifically, I examined the growing problem of medical identity theft through a robust theoretical lens, the unified theory of acceptance and use of technology (UTAUT). In this Chapter, I make holistic and technical introductions to the decision making process. Moreover, I discuss the UTAUT’s links to the technology acceptance model (TAM) and seven additional models/theories that explain user acceptance of new technology, each with different sets of acceptance determinants.

This analysis gives theoretical support for my focus on the adoption and use of palm vein authentication technology as it relates to medical identity theft. In addition to a brief introduction, Chapter 1 includes a background of the study, the problem statement, the purpose of the study, research questions, the theoretical framework, the nature of the study, the definitions, the assumptions, limitations, scope, and delimitations, and the significance of the study. I prepare the reader for a thorough review of the literature relating to the process of palm vein-based identification and its application in preventing medical identity theft in Chapter 2.

Background of the Study

Business investments in information technology are consistently recognized as business operations that hold the highest potential for value creation (Maes, De Haes, &

Van Grembergen, 2015). Gartner (2015) forecasted a stable growth of 2.5% or $2.7 trillion in 2015 on information technology spending worldwide across all industry market segments in constant-currency terms, and reported that healthcare providers would be the third fastest-growing segment in 2015. De Haes and Van Grembergen (2013) stated that an important conundrum for organizations is how to ensure they realize value from their investments in information technology and from their investments in change that results from the adoption and use of a new technology. Riley and Franke Kleist (2005) suggested that customers and potential customers of biometrics products tend to be less intrigued by the devices themselves and more focused on purchasing solutions to problems. Business leaders perceive the development of a detailed business case to be an essential step in the decision to adopt and use biometric technology. Documenting the problem or opportunity is the first step in the creation of a business case.

The problem I explored in this study is that there is uncertainty surrounding the benefits of palm vein authentication adoption relative to the increasing crime of medical identity theft. Medical identity theft is the use of individual personal information without knowledge or consent to obtain, or receive payment for, medical treatment, services, or goods (Biegelman, 2012). Medical identity theft has increased dramatically since the Federal Trade Commission (FTC) estimated there were at least 250,000 victims of medical identity theft for the period of 2001-2006 (FTC, 2007). When compared to the 2007 FTC report, data in the 2013 Ponemon report indicated a 700% growth in medical identity theft (Ponemon Institute, 2013).

Judson, Haas, and Lagum (2014) reported that individual victims of medical identity theft incur damages in the tens of thousands of dollars. The financial burden on secondary victims such as hospitals, health insurance companies, and government insurance programs may be greater than the costs incurred by individual victims. In one instance at the Massachusetts General Hospital, a patient used a relative's medical identity and obtained nine months of chemotherapy and related care. Over $750,000 in charges remain unpaid to Massachusetts General Hospital. In addition to the financial burden, undetected cases of medical identity theft pose patient safety challenges (Judson et al., 2014). Medical identity theft can introduce inaccuracies into a victim's medical records with regard to blood type, medication allergies, or medical history. These inaccuracies may result in misdiagnosis or mistreatment of patient illness (Judson et al., 2014). At the organizational level, medical provider organizations usually recognize a medical identity case after insurance companies remit insurance payments. Because of contractual obligations, hospitals refund erroneous payments to the insurance companies and attempt to collect payments from other insurance companies or funding sources. Because of filing-time limits, medical provider organizations face difficulty collecting payments. Judson et al. (2014) reported that healthcare providers incur billions of dollars in financial damages from medical identity theft. Despite the increasing number of medical identity theft victims, individuals lack awareness of the seriousness of the crime (Ponemon Institute, 2013). Medical fraud endangers victims' lives and causes a loss of trust and confidence in victims' healthcare providers (Ponemon Institute, 2013). Further,

the prevalence of sharing of personal identification to obtain medical services aggravates the incidence of medical identity theft (Ponemon Institute, 2013).

In this study, I sought to fill an important gap in the research literature with regard to how healthcare managers and doctors perceive palm vein authentication technology as a tool to mitigate the risk of medical fraud. Palm vein authentication refers to the process of creating an image of the pattern of veins that lies 3 mm below the surface of the palm. Vein patterns are unique to each individual (Wu, Lu, Cheng, & Shi, 2012). In prior research, Zhang, Tang, and Kong (2014) found that although genetically identical vein patterns have additional similarity, these patterns are nonetheless distinguishable. Palm vein authentication can be applied to almost all people and is different from other biometric authentication technologies such those using the face, iris, fingerprint, and voice because it analyzes a feature within the human body. Data obtained through the process of palm vein authentication can show whether the palm presented for authentication is being used in an attempt to circumvent the authentication process; this data may include whether blood circulation exists in the presented palm and the temperature of the presented palm. As the authentication data exists inside the human body, forgery is onerous under ordinary conditions (Vaid & Mishra, 2015). Modification of this biometric feature is difficult to undertake without user cognizance. Some commercial biometric systems employ vein recognition technology, and recently those in the legal community have focused on the merits of using vein recognition technology for criminal authentication (Zhang et al., 2014). Uttam, Haridas, Durvas, and Arun (2014) posited that both large-scale practical results and experimental results indicate that palm

vein authentication has the merits of consistency and high accuracy for confirming a person's identity.

In this study, I investigated the decision by healthcare managers and doctors to adopt and use palm vein authentication technology within the framework of the UTAUT. With UTAUT as my theoretical foundation, I examined participants' perceptions of the challenges, barriers, and potential benefits of the adoption and use of a palm vein authentication system. I also explored facilitating conditions that may influence the transition from a non-palm vein authentication security environment to a palm vein authentication security environment. The topic of the study was selected for three central reasons. First, I sought to contribute to the limited literature available on the factors that affect the adoption and use of palm vein authentication technology. Second, I sought to support future research that investigates the decision to adopt palm vein authentication technology. Third, I worked from the understanding that palm vein authentication technology has the potential to stymie the rising occurrence of medical identity theft and could be a boon to individuals, commercial organizations, and society in general.

Problem Statement

The Federal Bureau of Investigation (2014) reported that cyber actors will likely increase cyber intrusions against healthcare systems and their concomitant medical devices because of mandatory transition from paper to electronic health records, lax cyber security standards, and a higher financial payout for medical records in the deep web. The Ponemon Institute (2015) calculated that there were approximately 2.32 million medical identity theft victims in 2014. This represents a 21.7% increase (481,657 new

cases) over 2013. Ratha, Connell, and Pankanti (2015) and Volner and Boreš (2015) investigated biometrics access processes in identity management systems to cater to the individual business needs. These researchers found that biometrics have a strong appeal in digital identity management and are likely to emerge as among the most critical of the big data systems. In this study, the general problem was that information theft is increasing in the healthcare sector. More specifically, there is uncertainty surrounding the benefits of palm vein authentication adoption relative to the increasing crime of medical identity theft. I used a survey methodology to elicit participant opinions and values, including both expected and counterintuitive accounts of healthcare managers and doctors, the population that comprised the investigation.

Purpose of the Study

The purpose of this quantitative correlational study was to understand healthcare managers' and doctors' perceptions of the effectiveness of palm vein authentication technology. I used a cross-sectional survey employing online questionnaires to develop an understanding of the perspectives of healthcare managers and doctors across the United States with regard to palm vein authentication systems as risk mitigation tools to manage medical fraud. Palm vein authentication adoption by more healthcare managers could lead to a reduction in medical identify thefts.

In this quantitative study, the independent variables included the following: (a) perceived usefulness, (b) complexity, (c) security, (d) peer influence, and (e) relative advantage. I used SurveyMonkey and Cint to collect electronic data from 115 healthcare

managers and doctors across the United States, 109 of whom fully completed the questionnaire.

Research Questions and Hypotheses

The research questions for the study focused on capturing the perspectives of healthcare managers and doctors with regard to the adoption and use of palm vein authentication security systems in the workplace. I developed this research study to answer the following 5 research questions:

Research Question 1: What is the relationship, if any, between the intention to adopt a palm vein authentication system and perceived usefulness?

$H_0$1: There is no statistically significant relationship between the intention to adopt a palm vein authentication system and perceived usefulness.

H_a1: There is a statistically significant relationship between the intention to adopt a palm vein authentication system and perceived usefulness.

Research Question 2: What is the relationship, if any, between the intention to adopt a palm vein authentication system and complexity?

$H_0$2: There is no statistically significant relationship between the adoption of a palm vein authentication system and complexity.

H_a2: There is a statistically significant relationship between the adoption of a palm vein authentication system and complexity.

Research Question 3: What is the relationship, if any, between the adoption of a palm vein authentication system and security?

$H_0$3: There is no statistically significant relationship between the adoption of a palm vein authentication system and security.

H_a3: There is a statistically significant relationship between the adoption of a palm vein authentication system and security.

Research Question 4: What is the relationship, if any, between the adoption of a palm vein authentication system and peer influence?

$H_0$4: There is no statistically significant relationship between the adoption of a palm vein authentication system and peer influence.

H_a4: There is a statistically significant relationship between the adoption of a palm vein authentication system and peer influence.

Research Question 5: What is the relationship, if any, between the intention to adopt palm vein authentication and relative advantage?

$H_0$5: There is no statistically significant relationship between the intention to adopt palm vein authentication and relative advantage.

H_a5: There is a statistically significant relationship between the intention to adopt palm vein authentication and relative advantage.

Theoretical Foundation

The UTAUT served as a theoretical framework I used to create a focused and robust survey instrument. The UTAUT incorporates the TAM and seven competing models to explain user acceptance of information technology (Venkatesh, Morris, Davis, & Davis, 2003; Davis, Bagozzi, & Warshaw, 1989). Based on a synthesis of constructs from the competing theoretical models, Venkatesh et al. (2003) proposed a unified model

called UTAUT. Venkatesh et al. posited four core determinants of behavioral intention and usage with regard to user acceptance of information technology. These four core determinants of user acceptance of information technology include (a) performance expectancy, (b) effort expectancy, (c) social influence, and (d) facilitating conditions. Additionally, Venkatesh et al. included four moderators of key relationships including (a) age, (b) gender, (c) experience, and (d) voluntariness of use.

Investigators reported empirical results that showed the UTAUT model accounted for 70% of variance in usage intention (Venkatesh et al., 2003). To a large extent, the UTAUT performed better than any of the original eight models/theories and their extensions (Venkatesh et al., 2003).

Davis (1989) proposed the TAM to predict behavioral intention to use an information system and actual use of an information system. Davis (1989) asserted that perceived ease of use and perceived usefulness are the two determinants of behavioral intention to use information systems technology and actual use of information systems technology. Perceived ease of use is an individual's belief that using an information technology system will be free of effort. Perceived usefulness is an individual's belief that using an information technology system will enhance job performance or life performance. In the TAM, Davis (1989) postulated the following relationships among key constructs:

- Perceived ease of use and perceived usefulness positively affect an individual's attitude towards an information system;

- An individual's attitude towards an information system positively affects an individual's behavioral intention to use an information system; and
- Behavioral intention to use an information system positively affects actual use of an information system.

Nature of the Study

This was a quantitative correlational study. I designed the study to explore whether and to what extent a relationship exists between the dependent variable, the intention to adopt a palm vein authentication system, and the independent variables, perceived usefulness, complexity, security, peer influence, and relative advantage. I collected data through an electronic survey to explore the aforementioned variables (see Rea & Parker, 2014). I selected correlation analysis as the appropriate methodology for quantifying the degree of correlation between the dependent and independent variables in the study because a causal model could not be easily determined. Causation analysis is difficult because of the numerous variables that may influence the intention to adopt a palm vein authentication system.

I considered using qualitative research approaches such as case study, phenomenological inquiry, and grounded theory but determined that they were not appropriate for the study. The case study method was not appropriate because a case study would elicit interpretive responses to a particular variable relationship. This study involved many such relationships. Additionally, a case study would require exploring causation to determine principles related to the study (Leedy & Ormrod, 2005). The phenomenological method was not appropriate for this investigation because researchers

use it to focus on participant perspectives and include participant interpretations of experiences. I did not use grounded theory because it is intended to generate new theories or expound on current ones using inductive methods (see Creswell, 2013).

Definitions

Asset: The present economic resources the entity owns and/or controls (Ao, 2015).

Biometrics: The automated measurements of physiological characteristics or behavioral characteristics that are used to authenticate, determine, or confirm the identity of a person (Sayed & Jradi, 2014).

Chief information officer: An organization's top executive responsible for the management and stewardship of an organization's information resources (Ragowsky, Licker, Miller, Gefen, & Stern, 2014).

Enterprise: An organization that is responsible for producing the maximum amount of goods and services by using the least amount of expenses to satisfy the social needs (Davidson, 2015).

Equal error rate: A measurement that indicates the accuracy of a biometric algorithm by indicating the point at which the false rejection rate equals the false acceptance rate; the performance of the biometric algorithm varies inversely with the equal error rate (Kang, Liu, Wu, & Yue, 2014).

False acceptance rate: A measurement that indicates the accuracy of a biometric algorithm by identifying the probability of falsely declaring an imposter as an authorized user (Kang, Liu, Wu, & Yue, 2014; Sayed, 2015).

False rejection rate: A measurement that indicates the accuracy of a biometric algorithm by identifying the probability of falsely declaring an authorized user as an imposter (Kang, Liu, Wu, & Yue, 2014; Sayed, 2015).

Explanation of benefits: A written statement to a beneficiary, from a third-party payer, after a claim has been reported, indicating the benefits and charges covered or not covered by the healthcare benefits plan (explanation of benefits, n.d.).

Information assurance: The technical and managerial measures designed to ensure a secure information environment in a cost-effective manner (Liu, Zhang, & Chen, 2014).

Information security: The protection of an organization's valuable resources such as computer hardware, computer software, and information by ensuring confidentiality, integrity, and availability of information (Peltier, 2013; Ahmad, Ali, & Adnan, 2012).

Information systems: The network of people, hardware, software, communications devices, and data storage devices that collectively work to convert data into information (Galliers & Leidner, 2014).

Intelligence: The ability to learn from experience and to adapt to, shape, and select environments (Sternberg, 2012).

Medical identity theft: A crime that refers to the use of identifying medical information of another person without the person's knowledge or consent to obtain or receive payment for medical treatment, services, or goods, whether the victim is alive or deceased (Olanrewaju, Yahuza, & Ali, 2014).

Organizations: Social entities that are goal-directed, are designed as deliberately structured and coordinated activity systems, and are linked to the external environment. (Draft, 2013).

Palm vein authentication: A vascular pattern recognition technology that utilizes an image of vessels within the human palm as personal identification (Gupta, 2015).

Risk: The variance in the probability distribution over possible outcomes (Fox, Erner, & Walters, 2015).

Threats: The external stimulus that creates a perception in message receivers of an individual that the person may experience a negative situation or outcome (Williams, 2012).

Assumptions

Specific assumptions helped define the framework of my research. An assumption is "a statement that is presumed to be true, often only temporarily or for a specific purpose, such as building a theory" (Vogt & Johnson, 2011, p. 16). These assumptions are things a researcher takes as true in order for the study to take place. These assumptions also govern the overall procedure of dissertation research. I conducted this investigation under the following assumptions:

1. The methodology is appropriate for this study.
2. The population is a good representation of healthcare managers and doctors across the United States.
3. The sample drawn is also a good representation of the population.

4. The participants in the study answered the online questionnaire truthfully and to the best of their knowledge.
5. The participants understood the importance of not disclosing information from this study.
6. The questions of the online questionnaire did not bias the participants to answer in a manner that was purposely intended.
7. All responses from the participants were taken into consideration.
8. The palm vein authentication implementation challenges and barriers are related to the variables explained in the questionnaire.
9. The understanding of and terminology associated with palm vein authentication differs greatly among organizational shareholders.
10. Healthcare managers and doctors operate in disparate organizational cultures.
11. Healthcare managers and doctors are resistant to studies disclosing security information surrounding their own organizations.
12. Participants in the medical domain tend to have similar levels of knowledge on the topic that was investigated, but not necessarily the same perspectives.

Scope and Delimitations

The scope of this research encompassed healthcare managers and doctors from across the United States who I recruited using a purposive sampling approach. These participants may benefit from the study's findings. Participants included healthcare managers and doctors. The data pertained to challenges and barriers healthcare managers and doctors perceive regarding the implementation of a palm vein authentication security

system. I interpreted the data collected from the online questionnaires using quantitative data analytic tools.

Delimitations are under the control of the researcher, are actively chosen by the investigator, and include the following: (a) choices of research question, (b) objectives, (c) variables, (d) populations, and (e) methods of analysis (University of Southampton, n.d.). I delimited the population for this study to healthcare managers and doctors from different areas in the United States. I did not include participants from industries other than healthcare. Additional delimitations included the use of the UTAUT to frame the variables and ultimately the online questionnaire. My use of a survey approach was another delimitation, and I did not use other research methodologies after carefully considering their relevance and feasibility. An additional delimitation was the amount of time it took to conduct the online questionnaire; this was less than a month.

Limitations

The study included healthcare managers and doctors in the United States, which limits the generalizability of the findings. Findings may not be useful to those working in other countries who do not share characteristics with the United States. I limited the methodology for this quantitative study to the use of a survey instrument. I may have presented participants with time constraints because of the use of a survey instrument such that they may not have had sufficient time to complete the surveys. Also, I limited the range of responses because I categorized the survey questions and because I required participants to respond in certain categories which limited their range of responses. The research on palm vein authentication security systems in the United States has a gap that

needs to be filled. There is not much information about the factors that influence the decision making process regarding whether to adopt a palm vein authentication system.

The focus of this study was healthcare managers and doctors. To conduct a study of the entire population of healthcare managers and doctors in the United States would be costly and logistically infeasible. The purposefully selected participants sufficiently represented the population.

Significance of the Study

In this study, I sought to discover variables that influence healthcare leaders' intentions to adopt palm vein authentication security systems in the healthcare industry. I posit that the findings could assist project managers in recognizing the challenges and barriers to implementing security systems which use palm vein authentication during the adoption and planning phases. An increased awareness of these challenges and barriers could result in a more efficient and effective implementation of a palm vein security system as part of improved understanding and use of technology in healthcare delivery. Additionally, the research is timely and contributes significant data to inform a foundational understanding of security systems which use palm vein authentication for digital identity management. Finally, the results of this investigation provided much-needed insights into the doctors' and healthcare managers' perceptions of palm vein authentication as a tool to mitigate the risk of medical fraud. Thus this study includes useful information on the contributing and preventative factors related to leaders' intentions to adopt a palm vein authentication system in a healthcare setting.

Significance to Theory

This study filled a gap in the present literature concerning the implementation of palm vein authentication security systems in the healthcare industry. Despite limited research in this field, I used theories such as the TAM and the UTAUT to understand adoption and use of technology in the healthcare industry. Although I did not develop any new theories, the findings of this study may raise awareness amongst managers in the healthcare industry about the challenges and barriers that may surface when implementing a security system which uses palm vein authentication to mitigate the risk of medical fraud.

Significance to Practice

Healthcare industry leaders and practitioners may use the finding of this study to improve the human condition. Specifically, this study may lead to positive social change in three segments of the healthcare industry:

1. Healthcare consumers constitute a segment of the healthcare industry for which findings in this study may be used to lessen the likelihood of medical adversity. The consumer may face critical, and possibly fatal, medical adversity as a result of receiving inappropriate medical treatment. Inappropriate medical treatment may occur when the consumer's medical identity is linked with another individual's medical information. In addition to experiencing critical medical conditions, consumers may sustain financial difficulties when medical providers bill medical services to the victim of medical identity theft or the victim's insurance carrier. An increase of awareness about tools to manage the

risk of identity theft would be a boon to healthcare consumers because the probability that they would receive inappropriate medical treatment and that they would sustain financial hardship would decrease.

2. Healthcare providers form an added segment of the healthcare industry that may realize positive social change. Mancilla and Moczygemba (2009) reported that fraudulent medical claims cost public and private insurers millions of dollars every year. Although the expense may be passed on to the consumer, the healthcare provider initially absorbs the cost of the services made. Additionally, medical identity theft increases the healthcare provider's exposure to legal risk and public image risk; due diligence on the part of the healthcare provider may decrease this risk.
3. Healthcare insurers may also realize positive social change. The inclusion of false information can change the loss history of a given data sample of consumers and may increase the premium prices of experience-rated insurance products; this could create an inaccurate representation on the financial statements of the insurer. Furthermore, inaccurate data could also result in mistaken epidemiological data and undermine research quality (Norman, Aikins, & Binka, 2011; Walters & Betz, 2012). Administratively, having to correct false information leads to more clinical reviews, claims processing, and auditing. As a result, insurers may also realize positive social change should they adopt strategies to manage vulnerability to medical identity theft. By

increasing understanding of palm vein authentication systems, I directly and positively influenced awareness of this risk mitigation tool.

Significance to Social Change

This doctoral study is aligned with the Walden University commitment to inspire positive social change. Walden University envisions a distinctively different 21st-century learning community where knowledge is judged worthy to the degree that it can be applied by its graduates to critical social challenges, thereby advancing the greater global good. Contemporary enterprises manage far more than paper and conventional physical assets. Individuals entrust enterprises with critical information assets such as social security numbers, home addresses, family member data, health information, and other private demographics. I may have directly and positively influenced awareness of palm vein authentication security systems within the United States. The study promotes the development of information technology tools to help mitigate the risk of medical identity theft and prevent the loss of human life. Its findings may also increase both public and stakeholder confidence in security in the healthcare industry and enable managers to better prepare for and deter a potential security breach.

Summary and Transition

In this Chapter, I introduced palm vein authentication and medical identity theft, followed by discussions on the background of the study, the problem statement, the purpose of the study, research questions, the theoretical framework, the nature of the study, the definitions, the assumptions, limitations, scope, delimitations, and the significance of the study. In Chapter 2, I provide a review of current and related

literature. In Chapter 3, I present the research method, and in Chapter 4 I discuss the results of the study. In Chapter 5, I draw conclusions and offer recommendations.

Chapter 2: Literature Review

In this Chapter, I introduce the current and relevant research on medical identity theft and palm vein authentication set using the framework of the UTAUT. Although many investigators have examined the TAM and the mechanics of palm vein authentication, there is a paucity of empirical research addressing how healthcare managers and doctors perceive palm vein authentication technology as a potential tool to confront the emerging problem of medical fraud. The purpose of this study was to understand healthcare managers' and doctors' perceptions of the effectiveness of palm vein authentication technology. In this study, the UTAUT was the bedrock on which I developed the research questions.

Literature Search Strategy

My strategy for the literature review involved a comprehensive approach to obtain diverse and quality information from the literature that could help to examine stated hypotheses, achieve study objectives, and answer research questions. The major categories of literature that I considered for the investigation were published books, peer-reviewed journal articles, academic studies, government and state publications, and other primary data including from the World Wide Web. The databases I used to search for these sources included Management and Business – ABI/Inform, Business Source, Emerald, IEEE Explore, Microsoft Academic Search, ProQuest, Questia, ResearchGate, Sage, ScienceDirect, Social Science Research Network, and SpringerLink. The keywords I used in the database searches were *palm vein authentication, palm authentication, vein matching, vascular technology, biometric identification, biometric, biometric technology,*

palm vein, medical identity theft, identity theft, medical identity fraud, identity fraud, theft, and *fraud*. There are few studies on perspectives of healthcare providers with regard to palm vein authentication as a tool to confront the expanding problem of medical identity theft. Because there is limited research on the topic of this study, I reviewed articles published more than 5 years ago.

This literature review reflects the evidence base I used to justify the study and the relevance of healthcare stakeholder perspectives on technology acceptance and adoption in relation to medical identity theft. It also includes several scholarly resources highlighting perspectives of leading authorities on topics such as survey methodology, the UTAUT, the TAM, medical fraud, and biometrics technology. I organized the literature review by critical subject area to compare and contrast the perspectives of various authors on topics relevant to the research. Given the innovative nature of the subject matter, much of the available related literature is contemporary. In this review, I synthesize, compare, and contrast the evidence base to develop a case for analyzing the potential benefits of implementing a security system which uses palm vein authentication inside an organization. To collect relevant literature, I used a broad search strategy covering several separate electronic databases for peer-reviewed scholarly articles. I then review these articles for other relevant studies via their reference lists, which were in turn reviewed for relevance. Recommendations for future research were made for any important aspects for which relevant literature could not be found.

Theoretical Foundation

Hsiao and Yang (2011) noted that investments in information systems (IS) for today's organizations have expanded dramatically, accounting for about 50% of new capital investment. Despite the considerable investments in IS, about 74% of IS and software engineering projects are delayed, exceed budget, and do not meet the functional expectations (Schepers & Wetzels, 2007). Pai and Huang (2011) asserted that "how to apply current information technology in assisting healthcare to effectively improve the quality of healthcare service [is] an important subject in healthcare information management" (p. 650). Moreover, studying the perceptions of the intended users about the system before implementation is a wise decision because researchers have found that it positively affects the actualization of the real system (Ahlan & Ahmad, 2014).

In this investigation, I used the lens of the UTAUT to examine the perspectives of healthcare managers and doctors with regard to the adoption of palm vein technology in the workplace. UTAUT is a synthesis of about 2 decades of individual-level technology acceptance research and was built upon models that have been applied to various user groups and technologies (Venkatesh et al., 2003). Although UTAUT may not be the final model for healthcare acceptance and use, I believe it is an appropriate choice as a baseline model that can be extended to the healthcare acceptance context.

UTAUT explained about 70% of the variance in behavioral intention to use a technology among employees in a workplace. Also, UTAUT accounted for 50% of the variance in actual use towards information technology. UTAUT was confirmed, and later cross validated with data gathered from four and two organizations, respectively. Such a

robust pattern of results coupled with the large proportion of variance explained by UTAUT prompted Venkatesh et al. (2003) to conclude that we may be "reaching the practical limits of our ability to explain individual acceptance and usage decisions" (p. 471). Venkatesh et al. described the UTAUT model as a combination of the constructs of eight models that have been used to explain behavioral intent within the information systems domain. These eight models are the following:

- theory of reasoned action (TRA),
- TAM,
- motivational model (MM),
- theory of planned behavior (TPB),
- combined TAM and theory of planned behavior (C-TAM-TPB),
- model of personal computer utilization (MPCU),
- innovation diffusion theory (IDT), and
- social cognitive theory (SCT).

Venkatesh et al. (2003) posited that the consolidation of these eight theoretical models can enhance understanding of factors that affect the acceptance of information technologies. Additionally, Venkatesh et al. argued that UTAUT is useful not only to observe the adoption of information systems at the individual level, but also useful to observe the successful implementation of an information application system at the organizational level. The UTAUT includes four key constructs: (a) performance expectancy (PE), (b) effort expectancy (EE), (c) social influence (SI), and (d) facilitating conditions (FC).

Venkatesh et al. (2003) posited that PE, EE, and SI directly influence behavioral intention and actual usage, and FC directly influences actual usage. PE is the degree to which individuals believe that when they use the system, the system will help them achieve gains in job performance. PE represents the extent to which using a technology will enable users to improve their job performance. EE is the degree of ease associated with the individual's use of the system. EE denotes the level of ease associated with the technology use; effort is of great concern to users during their initial use of an information system. UTAUT founders used performance to replace perceived usefulness and ease of use in the original TAM. SI is the degree to which an individual perceives that important stakeholders believe he or she should use the new system. SI refers to the level of influence exerted by the individual's social settings that could influence users' intent to use the technology. SI is one of the constructs that directly influences intention to use technology systems. FC represents the level of support and infrastructure present in an organization, which could enable system adoption or usage (Venkatesh et al., 2003). Additionally, there are four moderators (age, gender, experience, and voluntariness) of these key relationships.

The UTAUT served as a comprehensive model I used to examine the factors that contribute to the successful adoption of a new technology system. Using this theoretical framework, I explored the following research questions and associated hypotheses:

Research Question 1: What is the relationship, if any, between the intention to adopt a palm vein authentication system and perceived usefulness?

$H_0$1: There is no statistically significant relationship between the intention to adopt a palm vein authentication system and perceived usefulness.

H_a1: There is a statistically significant relationship between the intention to adopt a palm vein authentication system and perceived usefulness.

Research Question 2: What is the relationship, if any, between the intention to adopt a palm vein authentication system and complexity?

$H_0$2: There is no statistically significant relationship between the adoption of a palm vein authentication system and complexity.

H_a2: There is a statistically significant relationship between the adoption of a palm vein authentication system and complexity.

Research Question 3: What is the relationship, if any, between the adoption of a palm vein authentication system and security?

$H_0$3: There is no statistically significant relationship between the adoption of a palm vein authentication system and security.

H_a3: There is a statistically significant relationship between the adoption of a palm vein authentication system and security.

Research Question 4: What is the relationship, if any, between the adoption of a palm vein authentication system and peer influence?

$H_0$4: There is no statistically significant relationship between the adoption of a palm vein authentication system and peer influence.

H_a4: There is a statistically significant relationship between the adoption of a palm vein authentication system and peer influence.

Research Question 5: What is the relationship, if any, between the intention to adopt palm vein authentication and relative advantage?

$H_0$5: There is no statistically significant relationship between the intention to adopt palm vein authentication and relative advantage.

H_a5: There is a statistically significant relationship between the intention to adopt palm vein authentication and relative advantage.

Literature Review

Review of Technology Acceptance Model

The TAM is a part of the UTAUT. Moores (2012) reported that the TAM "is one of the most influential theories in information technology adoption and acceptance research" (p. 507). Ahlan and Ahmad (2014) reported that the TAM predicts a large part of the use or acceptance of health information technology, but the theory can be modified for better prediction. Ahlan and Ahmad (2014) suggested that the TAM is a good theory that explains healthcare providers' reaction to health information technology. In addition, it shows a significant relationship between perceived usefulness and intention to use with actual use of health information technology. Hence, promoting use and acceptance of health information technology depends on the user perceiving it as useful (Ahlan & Ahmad, 2014).

Davis (1989) found that the TAM predicts and explains system use by positing that perceived usefulness and perceived ease of use are fundamental determinants of computer usage. Davis (1989) found that the TAM accounted for 47% of variance in behavioral intention. Davis (1989) also reported that the TAM explained 51% of the

variance in actual use of information technology. The model defines the construct *perceived usefulness* as "the degree to which a person believes that using a particular system would enhance his or her job performance," and *perceived ease of use* as "the degree to which a person believes that using a particular system would be free of effort" (p. 320). Davis (1993) contended that the TAM may be applied to more than the measurement of the acceptance of specific software and suggested that the goal of the TAM is to provide an explanation of technology acceptance across a broad range of end-user computing technologies and to validate the TAM across different user populations.

Moores (2012) indicated that the most common version of the TAM holds that perceived usefulness (PU) and perceived ease of use (PEOU) jointly determine the user's attitude towards using a system (ATT). ATT and PU determine the behavioral intention to use (INT), but INT determines actual system use (USE). Holden, Brown, Scanlon, and Karsh (2012) reported that the TAM has had widespread application in explaining healthcare providers' reactions to health information technology. The recent increase in healthcare researchers' use of the TAM appears justified, with many of the relationships specified by the TAM repeatedly validated in healthcare settings and fairly large proportions of variance explained in the dependent variable (be it intention to use or actual use). Perhaps most impressive is that the relationship between PU and intention to use or actual use of health information technology is significant in every test, indicating that to promote use and acceptance, the health information technology must be perceived as useful.

Melas, Zampetakis, Dimopoulou, and Moustakis (2011) reported significant heterogeneity among studies that applied the TAM in the healthcare context. Specifically, Melas et al. (2011) highlighted five characteristics found in a majority of existing healthcare studies that used the TAM as a theoretical foundation:

- small convenience samples of medical staff,
- lack of use of moderator variables,
- lack of use of external variables,
- lack of a uniform and specific model of relationship among variables, and
- generic non-contextualized measures.

In contrast, the UTAUT is more comprehensive than the TAM. With regard to the adoption and use of palm vein technology in the healthcare context, I used the UTAUT to explore the relationships among variables and facilitating conditions (external variables).

Review of Survey Methodology

In this study, I employed the survey research strategy to investigate industry's decision making process about whether to adopt a palm vein authentication security system. Choudrie (2016) presented survey methodology as the preferred strategy when examining technology adoption issues both in the contexts of the organizations and in the context of the household. In the organizational context, most researchers used the survey methodology, and some researchers used the case study methodology. When investigating technology adoption issues in the context of the household, investigators used several methodologies: (a) survey, (b) ethnographic study, (c) time use diaries, (d) secondary data analysis, and (e) multi-methods. Choudrie (2016) reported that

researchers favored the case study method when the unit of analysis was the organization. Additionally, investigators favored the survey method when the unit of analysis was an individual user or consumer. Lastly, McPeake, Bateson, and O'Neill (2014) asserted that "surveys are an important method of collecting data in healthcare and nursing research" (p. 24).

Pai and Huang (2011) reported that investigators used the questionnaire survey method most often to evaluate healthcare information systems. Most researchers in this domain created questionnaires targeted at system use satisfaction and attitudes relevance. Investigators distinguish findings into four major categories: (a) factors which can affect the input of the system, (b) structure of the system, (c) components of the system, and (d) efficiency of the system.

The survey methodology is one approach that researchers may use in a quantitative research design. The quantitative research paradigm and the qualitative research paradigm are the two major approaches to research. Yilmaz (2013) stated that the quantitative research tradition explains "phenomena according to numerical data which are analyzed by means of mathematically-based methods, especially statistics" (p. 311). Additionally, investigators who embark on quantitative research seek to develop explanatory universal laws in social behaviors by statistically measuring what they assume to be a static reality. Quantitative researchers follow an objectivist epistemology that reality is single, tangible, and fragmentable. Furthermore quantitative investigators emphasize measurement and analysis of causal relationships between isolated variables within a framework that is value-free, logical, reductionistic, and deterministic, based on

a priori theories. Researchers who use quantitative methods and procedures can obtain generalizable findings and present them succinctly and parsimoniously. Investigators who use a qualitative research design support a constructivist epistemology and assume that reality is dynamic and socially constructed. Qualitative investigators design studies through a contextual framework to obtain a rich and holistic description of the phenomenon under investigation from multiple perspectives, including that of the investigator (Yilmaz, 2013).

To achieve a greater awareness of how healthcare managers and doctors identify and describe the barriers to, potential benefits of, and the current state of palm vein authentication to confront medical identity theft, I used a quantitative survey methodology to assess management and provider perception based on the UTAUT model.

Review of Information Security

Virus, worms, Trojans, botnets, social engineering, and advanced persistent threats are all threats impacting organizations on a daily basis (Ponemon Institute, 2012). The majority of computer crimes are committed by individuals such as disgruntled employees or contractors who have physical and logical access to unauthorized systems (Sarkar, 2014). Galicki, Havens, and Pelker (2014) found it difficult to accurately measure organizational threats, especially considering that some organizations do not report security breaches because either they are unaware of the intrusion or criminal activity as it occurs, or do not want to report the incident because of the threat that customers may lose trust in the organization. Both small and large organizations have

experienced embarrassing and often costly incidents involving physical-security breaches or loss of information-system data because of stolen or misplaced physical media. Industry researchers are calling for organizations to examine their physical-security procedures from transportation and proper disposal of sensitive items or data, to physical barriers and internal employee surveillance (Tyson, 2011).

Changing business structures, advances in information and communication-system infrastructures, and the increased reliance of organizations on information pose a large number of challenges for maintaining sound information-management practices (Dhillon, 2001). Dhillon reported that organizations have clearly fallen short of developing adequate policies to handle information-security problems, and have fallen into a "policy vacuum" when dealing with information security. Dhillon supported his argument with evidence that suggested an increase in computer intrusion attempts, and inadequate policies and procedures for authorities to handle incidents of computer crime. A vast medium for exploiting information-security gaps is the Internet. The Internet was originally developed as an open-systems environment in which advancing and improving the technology was encouraged (Quigley, 2011). Quigley reported that the Internet originally served a closed community of a few intellectuals primarily located within the United States. This mode of communication facilitated discussion and regulation of ethical and security problems. System "policing" was primarily dispensed through peer pressure (i.e., chastising the offending user).

Dhillon (2001) posited that computer intrusion and hacking attempts increased because of inadequate security policies. Quigley (2011) believed that information

technology managers became more aware of the importance of security after the September 11, 2001 United States terrorist attacks. Cantoni and Danowski (2015) classified post-September 11, 2001 information-security challenges into three categories. First, organizations were dependent upon the Internet and information for day-to-day operations. Second, an increasing number of computer, database, and network systems made up a global information-technology infrastructure. Organizations were increasingly connected, increasingly automated, and increasingly dependent on highly reliable computer information systems. Lastly, information technology managers were facing much more sophisticated and malevolent forms of attacks on these types of systems. The disruptive shocks to organizations, were no longer accidental, benign, or acts of nature, but were now deliberate and malevolent (Cantoni & Danowski, 2015).

Warkentin (2006) and Knapp and Ferrante (2012), like Quigley (2011) and Dhillon (2001), agreed that effective information management is necessary to safeguard the organization and allow organizational stakeholders to perform their corporate responsibilities effectively. Warkentin believed this can be accomplished through effective and increased corporate governance. Specifically, the author examined the role of ineffective corporate governance and argued for increased governance while examining the collapse of energy powerhouse Enron. Information systems contribute to the performance dimension of the organization, and therefore are most closely linked with the business governance component of the organization (Warkentin, 2006). Successful information-security practices are necessary to maintain the operations of information systems within an organization. Moreover, Knapp and Ferrante (2012)

highlighted the direct effects that awareness, enforcement, and maintenance of the information security policy has on the effectiveness of corporate governance.

Warkentin (2006) identified the following seven key principles of information-system governance:

- Establish clearly understood responsibilities for information systems.
- Plan information systems to best support the organization.
- Acquire information systems in a cost-beneficial manner.
- Ensure information systems are of the required quality.
- Information systems perform when required.
- Information systems conform to formal rules.
- Information systems respect human factors.

Warkentin (2006) argued that the fourth principle of ensuring information systems are of the required quality specifically refers to the various tasks performed within information-security management. Specifically, Warkentin (2006) believed this included an organization's ability to monitor security breaches, the creation of accurate procedures for measuring the effectiveness of security measures, the preparation of disaster recovery plans, and the use of enterprise risk management and additional mitigation strategies.

Yaokumah and Brown (2014) determined the impact of information security governance focus areas on risk management. Yaokumah and Brown (2014) collected and processed questionnaires using multiple linear regression analyses and frequency analyses. Yaokumah and Brown (2014) found that information security alignment,

business strategic alignment, resource management, value delivery, and performance measurement accounted for 92.7% of the variances in risk management.

Fakhri, Fahimah, and Ibrahim (2015) explained that aligning information security programs with business strategy objective requires a firm understanding of the business significance of the diverse computing technologies positioned throughout the enterprise. Additionally, alignment of information security programs with enterprise goals demands a keen understanding of a specific information security program which promotes achievement of a specific firm objective.

Chen, Ramamurthy, and Wen (2013) employed a web-based field experiment to examine compliance with information security programs and corporate culture. Drawing from compliance theory and general deterrence theory, Chen et al. (2013) found that both remunerative and coercive enforcement strategies positively affected the intent of an employee to follow a security policy. In a later study, Chen, Ramamurthy, and Wen (2015) used a web-based survey to evaluate how comprehensive information security programs affect the security culture of a business enterprise. Chen et al. (2015) found a positive association between awareness of security policies in an organization and awareness of Security Education, Training, and Awareness programs. Additionally, Chen et al. discovered that awareness of security policies contributes little to the organizational security culture.

Anderson (1980) created the first coherent framework for information-security threat and response. This framework identified the components for analyzing concepts with information security in terms of threats, risks, vulnerabilities, attacks, and

penetrations. Anderson (1980) posited that the framework facilitated shifting the primary focus of information-security managers from insider threats to external attacks from unauthorized users. The framework component of threat helps to quantify the possibility of experiencing an unauthorized attempt to manipulate or access a system. Risk is the accidental and unpredictable exposure of information. Vulnerability is a known or suspected flaw within an organizational system that exposes that system to penetration or information disclosure. Attack is the specific execution or planning to carry out a threat. Finally, penetration is a successful attack that allowed an attacker to enter an organizational system or effectuate other threats (Anderson, 1980).

Lally (2013) applied normal accident theory to understand the risk within information technology. Within the theorem, Lally (2013) argued that certain characteristics of systems would create a higher probability of failure. Accident-prone systems were found to be more complex, tightly coupled, and poorly controlled.

Information systems are inherently complex because the hardware infrastructure of most organizations is complex and contains a wide range of technologies. Software often comprises thousands of lines of code written by many different programmers. Accident-prone systems are also tightly coupled because software and hardware act together to increase the speed of processing, often with little or no human-operator approval or oversight. Accident-prone systems often do not have security features built into the initial design of the system.

Other models of risk management view risk as a location-specific phenomenon. Sutton, Khazanchi, Hampton, and Arnold (2008) proposed an assurance services model

based on three levels of perceived business risks: technical-level risks, application user-level risks, and business-level risks. Technical-level risks address whether or not technical elements are in place to successfully integrate systems and mitigate risk. Application user-level risks relate to the current business environment, organizational readiness, internal manual processes, and training. Business-level risks relate to an organization's ability to reengineer traditional business processes to incorporate risk mitigation. Risk can also be measured based on economic cost and benefit (Bojanc & Jerman-Blazi, 2008). The prevention of potentially heavy losses that may occur because of infrastructure attacks and the appropriate financial investment in security can be calculated using the authors' proposed model. This method may help business managers justify security infrastructure costs such as a palm vein authentication system to executive management.

Review of Biometric Technology

An increased interest in physical-security, information security, and human identification technology are three of many consequences from the September 11, 2001 attacks on the World Trade Center, the Pentagon, and U.S. commercial airliners. Since then the number of both internet-connected devices and internet-connected individuals has increased exponentially. In this ubiquitous network society, where individuals can almost effortlessly access their information from any internet-connected device anytime and anywhere, human consciousness of risk associated with increased exposure of personal information in cyberspace has expanded.

To navigate information systems risk, individuals employ identification cards, passwords or personal identification numbers for human identification. However, individuals can misfile or forget passwords, and unauthorized users can pilfer identification cards, personal identification numbers, and passwords. In response to these concerns, scholar-practitioners have focused on biometric authentication technology to manage information systems risk. A biometric system employs either physiological characteristics or behavioral characteristics of humans for human identification. These systems are evaluated based upon performance, acceptability, and circumvention. Performance concerns (a) the attainable recognition precision and velocity, (b) the resources required to achieve the desired precision and velocity, and (c) the environmental factors that affect the desired precision and velocity. Acceptability refers to the extent to which individuals are amenable to the use of a distinct biometric identifier in their everyday lives; whereas, circumvention expresses how readily the system can be spoofed by employing spurious tactics (Nirmal & Francis, 2014).

An essential benefit of biometric authentication is that biometric data is based on physical characteristics that stay fixed throughout a person's life unless that person suffers trauma or an ailment. Moreover, vascular patterns are arduous to fabricate or alter because of their complexity and subcutaneous location. Biometric systems are superior because they offer a nontransferable means of identifying people (Nirmal & Francis, 2014). Biometric identification can yield systematic, secured access to information; fingerprints, iris, and palm vein scans are forms of biometric identification that deliver unique data sets. Each of the different biometric modalities has intrinsic benefits and

shortcomings. Some are challenging to counterfeit; whereas others are easily created without the subject's cognizance or approval, and some are less intrusive than others.

Ahmad, Ali, and Adnan (2012) surmised that recent advances in biometric technologies coupled with the proliferation of increased threats in information security produced a management environment rich with opportunities for biometric applications. In the business domain, management applies biometric applications to safeguard information and its internal physical and logical access control systems. Of the various biometric modalities, palm vein authentication technology focuses on a physiological feature below the surface of the human body; whereas, fingerprint, palmprint, and iris authentication technologies capture features above the surface of the human body. Wu, Lee, Lo, Chang, and Chang (2013) announced that palm vein recognition technology is characterized by high safety performance, and circumventing palm vein authentication technology by falsifying an individual's vein pattern is a difficult endeavor.

In palm vein authentication, near-infrared rays analyze the subcutaneous features of the palm. The human body holds two types of blood vessels: (a) arteries that carry oxidized hemoglobin and (b) veins that carry deoxidized hemoglobin. Absorption spectra are unique for each type of hemoglobin. Deoxidized hemoglobin absorbs near-infrared light having a wavelength of approximately 760 nm. When near-infrared light is used to image a human body, the veins will appear as lines and darker than other tissues because only the vessels absorb near-infrared light (Verma & Dubey, 2015).

The required components to capture a near infrared image include the following: (a) near infrared light source, (b) near infrared pass filter, (c) image sensor, (d) diffuser material, and (d) human palm.

Because a still image is necessary to generate a vein pattern, both frame rate and spatial resolution are of lower importance; however, a good lighting system that includes near infrared pass filters and diffuser material is paramount because it must not only provide accurate contrast between the veins and the surrounding tissue but it must also minimize illumination errors (Noh, Ramli, Hanafi, & Saripan, 2015).

Vein authentication technology uses two imaging methods for vein recognition: (a) transmission and (b) reflection. The transmission method of vein authentication illuminates the vessels from the surface, the back, and the side. The reflection method of vein authentication illuminates the palm. After diffusion through the hand, both methods capture the near-infrared light as the rays interact with the region of interest that is used for identification; however, each imaging method contains a unique response to vicissitudes in the light transmittance of the hand. Light transmittance of the hand increases when the flow of the blood in the human body decreases in intensity as the vessels contract because of a lowered human body temperature. If the light transmittance of the hand is high, near-infrared light can saturate the hand. In the transmission method, a high light transmittance produces a lighter, less-contrasted image that renders the vessels less distinguishable. However, in the reflection method, a high light transmittance has a negligible effect on the magnitude of the reflected light. Hence, the reflection

method produces veins that are easily perceptible regardless of the body temperature of the individual (Watanabe, 2008).

In addition to responding to vicissitudes in light transmittance differently, the two imaging methods also differ with regard to hardware configuration. A system that employs the transmission method positions the illumination device and the capturing device in separate locations; however, a system that uses the reflection method combines the illumination device and the capturing device into one multipurpose device. Hence, smaller devices such as personal computers and smartphones are more likely to be configured with hardware that employs reflection method technology (Watanabe, 2008).

Processing of Palm Vein Images

The process of palm vein authentication includes the creation of a feature database that is composed of palm vein images created during the registration process of the palm vein authentication system. Afterwards, the registered individual presents her palm for identification purposes. Both the identification process of the individual that presents her palm for authentication and the registration process of the individual that presents her palm for authentication encompass corresponding tasks; these tasks include the following three steps: (a) vein image acquisition, (b) vein image preprocessing, and (c) feature extraction.

The registration process of the palm vein image culminates in the creation of the feature database; however, identification process of the palm vein image concludes with the authentication decision. The palm vein authentication system arrives at the authentication decision by matching features of the palm vein image created during the

registration process to the palm vein image that the individual presents during the identification process (Zeng & Jin, 2012).

The process of palm vein recognition contends with three variables that create variations in the captured image. These variables include: (a) the placement of the palm, (b) the condition of illumination, and (c) the variability in collection times. Hence the imaging process of palm vein recognition of a contactless palm creates two types of variations: (a) rotational variations and (b) translational variations. To account for these variations, the palm vein imaging system analyzes the palm vein images and minimizes not only scale variations, but also translational variations and rotational variations. From this analysis, the palm vein imaging system extracts a stable and aligned region of interest by employing stringent preprocessing steps to recover a fixed-size region of interest (Zhou & Kumar, 2011).

The authentication system effects nonlinear enhancement of vein patterns not only by constructing a coordinate system that is invariant to image variations caused by the interaction of the user with the imaging device, but also by associating the coordinate system with the palm itself because the goal is to seek the invariance corresponding to it. Simply put, the authentication system creates two webs as reference points to build the coordinate system: (a) the web between the index finger and middle finger and (b) the web between the ring finger and little finger. Next, the authentication system extracts a pattern from infrared-ray images as dark lines and captures the pattern morphologically as valleys of brightness in the palm area. Lastly, the authentication system superimposes the vein pattern on that which has been registered in a database (Manocha & Kaur, 2013).

Performance of Palm Vein Authentication

Uttam, Haridas, Durvas, and Arun (2014) explored the performance of palm vein recognition technology and reported that palm vein authentication technology offers a high level of accuracy. Uttam et al. (2014) used data of 140,000 palms from 70,000 individuals to investigate the performance of palm vein authentication and confirmed that the false acceptance rate was 0.00008% and the false rejection rate was 0.01% providing that the palm was held over the sensor three times during registration and that only one final scan was permitted to confirm authentication. Despite the lack of a publicly available palm vein pattern database provided to the research community (Lee, 2012), additional researchers investigated different technologies for palm vein authentication in subsequent years and reported the following performance results using a region of interest that is located at the center of the palm: (a) Zhou and Kumar (2011) reported an equal error rate of 0.43%; (b) Lee (2012) reported an equal error rate of 0.40%; (c) Wu et al. (2013) reported an equal error rate of 0.54%, and (d) Al-Juboori, Wu, and Zhao (2013) reported an equal error rate of 0.0333%.

Kang, Liu, Wu, and Yue (2014) and Yan, Kang, Deng, and Wu (2015) examined palm vein authentication technology and observed the following performance results using the entire palm as the region of interest: (a) Kang et al. (2014) reported an equal error rate of 0.996%, and (b) Yan et al. (2015) reported an equal error rate of 0.16%.

Zhou and Kumar (2011), Lee (2012), Wu et al. (2013), and Al-Juboori, Wu, and Zhao (2013) tested different authentication strategies to arrive at their results. Zhou and Kumar (2011) generated matching scores by employing the Hessian phase approach to

extract palm vein features and by using an approach to feature matching that compared the neighborhood of the corresponding regions characterized by rotational variations and translational variations. Lee (2012) used a near infrared low cost charge coupled device camera in conjunction with a 2-D Gabor filter to optimize resolution in both the spatial domain and the frequency domain. Wu et al. used a directional filter bank for feature extraction and a normalized Hamming distance for feature matching. Finally, Al- Juboori et al. (2013) utilized the Gaussian-Second Derivative for enhancement of the palm vein images and the Gabor Fisher Vein Feature to arrive at their authentication results. The Gabor Fisher Vein Feature extraction method uses both Gabor filter and Fisher Discriminated Analysis. Al-Juboori et al. verified the test palm images by using the Cosine Distance method.

Kang et al. (2014) investigated the entire palm region as the region of interest and focused on extracting stable local invariant features for matching. Among various palm vein recognition strategies, Kang et al. employed the RootSIFT algorithm and the histogram equalization method which investigators derived from a transformation of the cumulative distribution function to increase contrast throughout an image. Kang et al. (2014) observed an equal error rate of 0.996%. Kang et al. (2014) posited that improved recognition performance occurred by using the Hellinger kernel, rather than the Euclidean distance alone, as the dominant strategy for feature matching. Moreover, Kang et al. (2014) verified the robustness of the proposed approach to palm vein authentication by constructing a contact-free palm vein database that contained a variety of posture positions.

Yan et al. (2015) also presented a novel palm vein recognition algorithm for the entire palm region. Yan et al. based their algorithm on a multi-sampling and feature-level fusion strategy which used two image enhancement strategies, (a) Difference of Gaussian and (b) Histogram Equalization, to create a feature template of the extracted features that is compact and verifiable. Rather than using a unidirectional matching algorithm, Yan et al. utilized a bi-directional matching algorithm and observed an equal error rate of 0.16% on the CASIA Palm Vein Image. Moreover, Yan et al. posited that their proposed method is an effective palm vein authentication algorithm especially for images with remarkable posture changes because of the following findings:

- The proposed method had a higher recognition rate than the widely used scale-invariant feature transform algorithm.
- The recognition rate of the algorithm varies directly with the number of sample images that are fused.
- Establishing feature similarity thresholds permits a trade-off between recognition accuracy and recognition speed.

Sayed (2015) presented an algebraic method for palm vein authentication based on the Coset decomposition method. Sayed (2015) applied a 2-D Gabor filter, a median filter, and a local line binary pattern during feature extraction. To complete the feature matching process, Sayed (2015) used the Coset decomposition algorithm as a modified hamming distance measure. Although Sayed (2015) did not explicitly report an equal error rate, Sayed (2015) observed a false acceptance rate of 0.2% and a false rejection rate of 0.4%.

Sayed (2015) and Zeng and Jin (2012) argued that, of the various biometric technologies such as fingerprint recognition, face recognition, iris recognition, retina recognition, DNA recognition, signature recognition, voice recognition, hand shape recognition, palmprint recognition, and hand vein recognition, hand vein recognition has the most potential for development of the biometric identification modalities. Palm vein authentication has the following advantages:

- It relies on a feature that is not easily forgotten or lost.
- It relies on a feature that is available anytime and anywhere.
- It relies on a feature that is unique to each individual and difficult to falsify.
- Its contactless approach provides a healthful advantage.
- It relies on near-infrared rays that are a component of sunlight whose effect is much less than walking in sunlight (Sayed, 2015).

As a result, the safety, reliability, and validity of palm vein authentication technology is greater than the other biometric recognition technologies.

Review of Palm Vein Implementation

A project manager implements a palm vein recognition system by adopting one of the following three different management methods that are used to store feature data: (a) the store-on-client-server or personal computer method, (b) the store-on-card method, and (c) the match-on-card method. The store-on-client-server or personal computer method maintains the palm vein feature data on a client-server or a personal computer. This method incorporates highly secure storage areas reinforced with anti-tamper functionality and highly secure communication lines. Access to palm vein feature data is limited to

users that are verified or system administrators that are authorized. In contrast to the store-on-client-server method, the store-on-card method and the match-on-card method maintain palm vein feature data on a smartcard and provide users with a greater sense of security because less individuals have access to their palm vein feature data (Sayed, 2015).

The store-on-card method entails a feature matching process that occurs in an external processing unit; however, the match-on-card method matches palm vein feature data on the smartcard that also stores the feature data obtained during the initial registration process of the user. The match-on-card method permits increased security because this method eliminates any risk associated with communicating data between the smartcard and an external processing unit. For system administrators, storing palm vein feature data on a smartcard and storing palm vein feature data without a smartcard offer different advantages. System administrators reduce the cost of managing data by storing data on smartcard; however, system administrators who manage data without a smartcard benefit by not incurring the cost of the smartcard and by eliminating the labor cost associated with issuing and reissuing lost or stolen smartcards (Sayed, 2015).

Review of Palm Vein Applications

South Korea manufactured the first hand-vein recognition product in 1998; today, both South Korea and Japan lead the world in vein recognition technology. In particular, Japan's Fujitsu leads the world in palm vein recognition technology. Zeng and Jin (2012) communicated that "tens of thousands of banks, universities, hospitals and other business use the security system" (p. 884) based on Fujitsu's PalmSecure vein authentication

device. Watanabe (2008) reported that the Bank of Tokyo-Mitsubishi was one of the earliest financial institutions to adopt palm vein authentication to confirm client identification in Japan and that Banco Bradesco S.A. was one of the earliest financial organizations in Latin America to test palm vein recognition technology as a solution for client authentication. Watanabe (2008) also documented that the Chiba Institute of Technology deployed the world's first student identification system that combined palm vein recognition technology and multifunctional smartcards not only to verify the identity of students but also to permit secure access by students to their academic transcripts and other personal records. Students used palm vein recognition technology via information terminals strategically installed at various locations on the campus of the Chiba Institute of Technology. Finally, Watanabe (2014) reported that Todholm Primary School in Scotland implemented a palm vein identification system to offer a means for students to pay for school meals and promote the welfare of children in Scotland. The system at Todholm Primary School used preregistered palm vein patterns from staff and pupils to give a secure, cashless, and electronic point of sale for the catering facilities of the primary school. Moreover, because some localities provided schools with operating funds based upon attendance, investigators are researching the system at Todholm Primary School as a possible candidate for monitoring truancy levels, facilitating accurate attendance documentation of students, and improving overall time management for additional schools in other localities.

In addition, Fan, Xue, and Wu (2015) explored the application of contactless palm vein recognition technology to personnel in the valuables logistics industry. Fan et al.

(2015) combined palm vein authentication technology and the SPS mobile phone barcode gun to supervise and manage clients, couriers, managers in the valuables logistics industry. Fan et al. reported a correct recognition rate of 99.34%, a false acceptance rate of 0.66%, a false rejection rate of 0.60%, and recognition time of 0.0379 seconds. Furthermore, Fan et al. concluded that the introduction of palm vein recognition technology enabled accurate identification of employees who were responsible for valuables that were lost or damaged.

Potential Palm Vein Application - Fraud Prevention

A critical challenge that biometric vendors and customers face is how to define an environment that is cost effective for the user of biometric technology. Researchers have uncovered that many biometric industry vendors are more captivated with the technology underlying biometric devices rather than focusing on presenting biometric devices as part of a solution to a business problem for potential customers. In contrast, customers are less interested in devices and more focused on purchasing solutions to their problems (Uzoka & Ndzinge, 2009).

Adoption results from a series of decisions to embark on to using a new technology. These choices are often a result of a judgment of uncertain benefits of a new technology and the uncertain costs of adopting it. Factors that affect biometric technology usage could be economic, managerial, operational, or process related. However, an assessment of recent literature on the adoption of biometric technologies in organizations has revealed almost no research regarding the factors influencing the decision to employ biometric access technologies. A study on the adoption of security systems revealed that

although firms may be in danger of bioterrorist attacks, small to medium sized operations do not believe it is important to improve security because of the notion that the greater threat is to large businesses. They may not agree to spend significant amounts of money to upgrade security efforts, especially considering the context that they may not be convinced about the returns on investment in biometric security. Many factors affect how well or how poorly security controls will perform in any organization. Adoption and barriers to adoption of technologies differ across countries and time. Among the factors that may affect biometric authentication users are (a) the management, (b) the environment, (c) the infrastructure, (d) the cost/budget, (e) the communication systems, and (f) the existing security needs (Uzoka & Ndzinge, 2009).

Okoh and Awad (2015) concluded that biometrics technology has considerable opportunities for application in the healthcare industry. Okoh and Awad (2015) asserted that biometrics technology provides not only reliable user authentication but also secure user authentication. Of the various biometric technologies, palm vein authentication may be used to provide secure and reliable user authentication and patient identification. By enabling accurate patient identification, palm vein recognition technology may be utilized to confront the growing problem of medical identity fraud. The Identity Theft Resource Center (2015) reported that the healthcare industry accounted for the highest percentage of total information breaches for three consecutive years: 2012, 2013, and 2014. In 2014, the healthcare sector experienced 42.5% of all data breaches in the United States. In comparison, the financial sector experienced 5.5% of all data breaches in the United States in 2014. Berwick and Hackbarth (2012) estimated the annual amount of United

States medical fraud to be between $82 billion and $272 billion, and the Identity Theft Resource Center (2015) estimated that healthcare organizations who suffer breaches spend an average of $2 million over two years to manage the effects of information breaches. The Ponemon Institute (2015) reported that 2.3 million Americans were victimized by medical identity fraud in 2014, up almost 22% over 2013. Additionally, two-thirds of medical identity theft victims or 65% spent an average of $13,500 and approximately 200 hours to address the fraudulent events. Only 10% achieved a 'completely satisfactory' resolution of their case (Ponemon Institute, 2015).

Part of the problem stems from cyberattacks and security breaches at major corporations when thousands or millions of people's data are stolen in one fell swoop. Premera Blue Cross based in Washington State suffered an eight-month long cyberattack that went unnoticed until January 29, 2015. The security breach at Premera Blue Cross affected 11 million members, and 'the attackers may have gained access to claims data, including clinical information, along with banking account numbers, Social security numbers, birth dates, and other personal data' (Ponemon Institute, 2015). Criminals also attacked Anthem, the second-largest health insurer in the United States. Although Anthem stated that medical information was not stolen in its breach that affected close to 80 million people, Anthem offered identity repair assistance and credit monitoring services to current and former Anthem Blue Cross and Blue Shield in Ohio members dating back to 2004 via AnthemFacts.com in February 2015 (Ponemon Institute, 2015; Identity Theft Resource Center, 2015).

The Federal Bureau of Investigation (2015) reported that criminals are targeting the healthcare sector because individuals' personal information, credit information and protected health information (PHI) are accessible in one place, which translates into a high return when monetized and sold. In fact, PHI records can fetch up to $60 to $70 each, as opposed to about $5 for credit cards (Federal Bureau of Investigation, 2015). Currently, medical identities are 20 to 50 times more valuable to criminals than financial identities. Criminals have come to understand that medical identity fraud is more profitable than drugs, prostitution, and other crimes they may pursue. Initially, criminals steal patient identities to submit illegitimate claims to receive payment for medical services for conditions the victims never had and for services that were never provided. In Pennsylvania, a medical identity theft victim realized an imposter used his identity at five different hospitals, created medical histories in the victim's name at each facility and received more than $100,000 in medical treatments (Dixon, 2006). Moreover, the consequences of these incidents linger. Twelve years ago, a medical identity theft victim tried to donate blood for the first time; she was denied without explanation. As a result, she contacted the American Red Cross headquarters and discovered that her Social security number had been used at a free AIDS clinic. Because the information still exists within the Red Cross system, she wonders what would be the ramifications should that information become public (Identity Theft Resource Center, 2014). The Ponemon Institute found that about a third of medical identity theft victims lose their health insurance, and approximately a fifth of medical identity theft victims sustain a decrease in

their credit score and potentially an increase in the cost of credit (Ponemon Institute, 2015).

National attention focuses on patient safety (Classen et al., 2011). Patient safety gained the spotlight in 2000 when experts estimated that as many as 98,000 people die each year because of preventable medical errors (Kohn, Corrigan, & Donaldson, 2000). Moreover, as the number of medical identity theft incidents continues to escalate, inaccuracies are introduced into patients' medical records that lay the foundation for potential medical errors that could prove tragic. The false information may belong to a medical identity thief who used the victim's identity to obtain medical services, or it may be false information fabricated by the thief who used the victim's identity to generate false claims for services. Because medical identity theft can remain hidden for an extended period of time, this crime places patient safety at risk for the duration that the crime remains undiscovered (Dixon, 2006).

Patient privacy concerns partly influenced two Congressional actions in the United States: (a) the Health Insurance Portability and Accountability Act (HIPAA) of 1996, and (b) the Patient Protection and Affordable Care Act (PPACA) of 2010. Both legislative measures were championed as means to boost efficiency, reduce healthcare costs, and improve the quality of care through the use of electronic health records (EHR). As a result of these measures, healthcare providers could access information about previously prescribed medicine to avoid prescribing medication that might be harmful (U.S. Department of Health & Human Services [HHS], 2015). Also, healthcare providers could access lab results to avoid having to repeat lab tests. Consumers paid less for

healthcare in regard to copayments and deductibles, and consumers assumed less risk for radiation and other side effects from repeated exposure to x-rays and specific lab tests (HHS, 2015). However, both Congressional actions and their concomitant emphasis on digitizing medical records intensified concern over the security of computer networks (Ollove, 2014). As more doctors and hospitals useD the EHR system, the size and frequency of data breaches alarmed privacy advocates and public health officials. In a recent breach of Community Health System, Chinese hackers bypassed the hospitals' security systems and stole personal data that included Social security numbers, names, and addresses of over 4.5 million patients (Whitney, 2014).

Dixon (2006) submitted that the onus is on healthcare managers and doctors to protect the people they serve. Because patients hold healthcare providers in a position of trust, patients enter a healthcare system with a sense of security, believing that their personal medical issues and information are and will remain private. Furthermore, patients believe that their medical records have been and will remain secure and reliable to ensure quality healthcare is delivered to treat their current illnesses or injuries. Dixon (2006) suggested that healthcare provider organizations take steps to improve and ensure the accuracy of patient identification. Accurate patient identification now tops the list of 2015 national patient safety goals issued by the Joint Commission. With the top 2015 patient safety goal being "to improve the accuracy of patient identification," the Joint Commission offers the following suggestions to improve accurate patient identification:

- Use at least two identifiers to verify a patient's identity upon admission or transfer to a facility.

- Eliminate transfusion errors related to patient misidentification (The Joint Commission, 2015).

Summary and Conclusions

During the review of the literature, I found a large number of investigations of the UTAUT, the TAM, survey methodology, information technology security theory, and the mechanics of palm vein authentication; however, palm vein authentication is still not widely practiced in the United States. It is important to note that scholarly research and empirical evidence with regard to the determinants of implementing such a technology is obviously lacking. Since palm vein authentication is a relatively recent activity and has yet to be fully implemented by most companies in the United States, it must be highlighted that there has been little academic research about its accomplishments and about the obstacles to adoption. Very little is known about why some companies adopt a palm vein authentication system, and others do not. In particular, there is a paucity of empirical research that explores healthcare managers' and doctors' perceptions of the effectiveness of palm vein authentication technology as a potential means to confront the emerging problem of medical fraud. Mindful of the lack of implementation of palm vein authentication in the United States, this study, therefore, aimed to fill this research gap with an investigation into the perceptions of healthcare managers and doctors towards palm vein recognition technology. This study used research questions based on the survey methodology and the UTAUT theoretical framework to examine how healthcare managers and doctors perceive palm vein authentication technology with a particular focus on mitigating the risk of medical fraud.

Chapter 3: Research Method

The purpose of this quantitative correlational study was to understand the effectiveness of palm vein authentication technology as perceived by healthcare managers and doctors. The specific problem was the uncertainty surrounding the benefits of palm vein authentication relative to the growing crime of medical identity theft. In Chapter 3, I elucidate the methods I employed to address the core research questions. Also in Chapter 3, I present an overview of the research design, population, sampling procedures, measures, data collection processes, ethical guidelines, and analyses that I completed.

Research Design and Rationale

The research design of any study involves (a) how the investigator will administer the study, (b) what tasks the investigator will execute, and (c) why the investigator will complete the investigation in the identified manner (Saunders, Lewis, & Thornhill, 2015). Leedy and Ormrod (2015) posited that research is an endeavor to increase awareness and understanding of a perceived occurrence by deliberately and methodically collecting, analyzing, and interpreting data.

Straits and Singleton (2011) identified two types of research approaches: quantitative and qualitative approach. In the two categories, researchers further categorize research approaches into interpretive, objective, subjective, and philosophical methods (Saunders et al., 2015). In a qualitative research approach, investigators emphasize the importance of looking at variables that the investigator discovers while examining the research problem. In a quantitative research approach, researchers attempt to gather data

by objective methods to provide information about relations, comparisons, and predictions. This type of research is designed to minimize the investigator's influence/bias (Straits & Singleton, 2011). Using an objective approach permits generalization of the participants' responses in line with the research question. This generalization is common in a quantitative research study in which the investigator uses a survey instrument to gather participants' responses. Correct use of a research method is important to the validity and reliability of a research project. Using an objective approach results in strong research findings because investigators arrive at conclusions based on what actually exists rather than on subjective thoughts of the participants. Note that the participants' survey responses are subjective. Turning them into numbers doesn't change this reality.

Saunders et al. (2015) posited that researchers who use the subjective, interpretive, and philosophical approaches subscribe to the idea that people best understand a social phenomenon by considering feelings and insights that exist only in the mind rather than by using the laws of nature. The subjective, interpretive, and philosophical approaches were not appropriate for this investigation. Understanding the relationship among variables that may influence the adoption and use of palm vein authentication technology in the healthcare domain requires concrete proof of evidence. Hence, an objective approach is more appropriate for this study.

Quantitative researchers work to gather quantitative data. Quantitative data can be an outcome of research strategies ranging from frequency of occurrence to test scores. Myers (2009) reported that investigators may collect and subsequently code data for

quantitative analysis at different levels of numerical measurement. Investigators who embark on a quantitative research study follow a generalization approach. Champions of this approach arrive at conclusions based on expressed views by employing questionnaires and physical counts to input numerical values for expressed ideas. Researchers use statistical software tools to analyze and process data that culminates at generalizable findings.

In this investigation, I used a questionnaire to collect responses to research questions in order to increase scholarly understanding of how the various variables correlate in the adoption and use of palm vein recognition technology by healthcare managers. These variables were intention to adopt palm vein authentication, perceived usefulness, complexity, security, peer influence, and relative advantage. The quantitative approach primarily uses numbers to produce estimates and differences. In this investigation, I gathered, summarized, filtered, and analyzed data to ascertain answers to the research questions and thus met the objectives of this investigation. With the goal of finding answers to the research questions in mind, I devised the investigation to include a quantitative correlational design that used a purposive sampling technique. A purposive sampling technique was cost efficient and more pragmatic for the investigation given financial and time constraints. Given its widespread acceptance and use in academic institutions, researchers assign considerable credibility to survey research as a robust research technique in the social sciences and professional disciplines (Rea & Parker, 2014).

In preparation for this study, I examined five of the qualitative methods for research that Creswell identified (2013). I compared and contrasted the following qualitative research methods: (a) case study, (b) narrative study, (c) ethnography, (d) grounded theory, and (e) phenomenological research. These methods follow a similar pattern of development.

The qualitative methods use varying amounts of observations, documents, interviews, and audiovisual materials to collect data. Similarities exist in the research designs of the investigative methods. Upon initial inspection, case study research, narrative research, and ethnographic research may appear to be identical when the unit of analysis is a single individual. However, upon closer inspection, the investigator collects different types of data apropos of the research design. For instance, a narrative research design requires that the investigator explore stories recalled by an individual and organize these stories in chronological order. However, an ethnographic research design requires that the investigator explore the culture-sharing group and the culture that surrounds the stories recalled by the individual. Investigators use the case study research design to explore both a single case or multiple cases by writing a holistic description of the case. Investigators prefer to use a case study or narrative research design rather than an ethnographic design because ethnography provides a cultural context that is wider than the individual.

Nonetheless, there are fundamental differences between the five qualitative research approaches. The researcher should use main purpose or focus of the study to guide appropriate research approach. When a researcher expects to generate a theory, it is

obvious that the grounded theory approach is the target. A researcher who is interested in the cultural context should choose the ethnographic approach. Concerning data collection, differences exist among the methods in terms of emphasis and extent. Ethnographic studies consist primarily of observations; grounded theory projects consist predominantly of interviews, and only interviews comprise phenomenological studies. Case studies are unique in their inclusion of multiple data collection forms. In the data analysis area, the differences among the approaches are major. The major differences involve definition and the number of steps to be completed. Phenomenology requires the most steps, while ethnography includes the least number of steps. In all the research approaches, investigators compile the written reports from all the stages that preceded it.

In preparation for this study, I considered whether the aforementioned research methodologies would be appropriate. After careful deliberation, I chose the quantitative approach and used data from an online questionnaire to explore the research questions. McMillan and Schumacher (2014) explained that researchers using the survey tool to explore a phenomenon obtain data by selecting a sample of subjects who respond to a questionnaire or an interview. McMillin and Schumacher (2014) and Straits and Singleton (2011) highlighted that academic investigators prefer using the survey tool when investigating the following: (a) the relationships among different variables of the phenomenon under investigation, (b) the rationale for practices by market-dominant organizations, and (c) the frequency distribution of demographic characteristics or traits.

To summarize, the stimulus for narrative research is the requirement of obtaining a deeper understanding or awareness of the life of an individual. The motivation for

phenomenological research is the requirement of obtaining a deeper understanding or awareness of a lived phenomenon. The stimulus for grounded theory research is the investigator's desire to generate a theory based on data obtained during the investigation. The motivation for the case study approach is the requirement of obtaining a deeper understanding or awareness of a case or multiple cases. Finally the stimulus for a survey approach is to explore a phenomenon by assessing relationships, if any, among variables of a specific phenomenon. In the next section, I present an in-depth analysis of survey research and a justification for its use as the appropriate methodology to conduct this investigation.

Methodology

I used correlational analysis as a first step towards understanding where to focus and what variables to consider in a future causal analysis because there is a need to demonstrate the relationship among dependent variables, independent variables, moderating variables, and facilitating variables. A causal model cannot be created without first understanding the nature of the relationships that may or may not exist among the UTAUT constructs (Rea & Parker, 2014; Bosco, Singh, Aguinis, Field, & Pierce, 2015). Thus, a quantitative correlational design was appropriate for exploring the relationship among the aforementioned variables associated with the intention to adopt palm vein recognition technology as a means to mitigate the risk of medical fraud.

Additionally, a correlational design was appropriate because I designed the primary research questions to examine the associations between variables that are not subject to experimental manipulations. An experimental or quasiexperimental method

was not appropriate because the assignment of research participants was not completely random and the study did not include experimental controls (Creswell, 2013). Also, the study did not involve making predictions or examining causes and effects.

While exploring the research problem, I examined various perspectives of people and groups, and I identified many specific variables to study. Additionally, I concentrated my personal experience as a researcher on systematic analysis and comparison and technical writing rather than computer text analysis and a literary writing format. The eventual audiences of this study are technical managers, healthcare managers, and doctors.

Population

I selected the participants from a population of 1,041,300 healthcare managers and doctors employed throughout the United States.

Sampling and Sampling Procedures

I used a purposive sampling of participants who met the following criteria: (a) were 18 years or older, (b) performed work for the organization on a full time basis or a part time basis, and (c) were either a healthcare manager or doctor. The participants received a link to an anonymous self-administered online survey. The purposive sampling method is a form of non-probability sampling. It was efficient because I drew the sample from the available pool of self-selected responders (see Mills & Gay, 2015). Additionally, purposive sampling is pragmatic when the research interest is in a specific field. The purposive sampling method was cost efficient and more practical for this investigation given financial constraints and time constraints.

Researchers use purposive sampling in an attempt to obtain a diverse range of opinions from members of a defined population of interest (e.g., experts in the medical profession). Multilevel sampling is used to explore the direct influences and the interactive influences of continuous higher-level variables on lower-level outcomes (Mathieu, Aguinis, Culpepper, & Chen, 2012). Trochim, Donnelly, and Arora (2015) defined purposive sampling as sampling with a purpose in mind and noted that purposive sampling is appropriate for a variety of research approaches. However, purposive sampling does not necessarily produce a representative sample from the population. Purposive sampling was well suited for this exploratory investigation of how healthcare managers and doctors perceive palm vein recognition technology as a potential tool for managing the risk of medical fraud. I did not seek to make point estimates of population parameters for specific questions, for which a random sample would have been necessary.

Additional sampling methods that I considered but did not deem appropriate included snowball sampling, stratified sampling, cluster sampling, and random sampling. Snowball sampling requires a small sample to obtain additional participants with the same qualifications (Trochim et al., 2015). In the stratified sampling technique, researchers group participants into different subpopulations and therefore not apropos for this study. Also, I did not view cluster sampling as appropriate because there was no need to separate respondents into different clusters from which I could randomly select participants. Finally, the random sampling strategy requires that the investigator selects the population in a manner that results in an equal and nonzero likelihood of selection for

respondents. Random sampling necessitates much planning time to get the sampling correct.

The current investigation used a purposive sampling strategy. Sample size calculations were a function of alpha, effect size, and statistical power. I considered the type of statistics that would be applied to the sample data and the number of variables during sample size calculations. I utilized G*Power 3.1.9.2 software tool to calculate sample size for the Pearson product moment correlation statistic. Siegel (1988) suggested that the power for a Spearman correlation is approximately 91% as efficient as a Pearson correlation. I selected the a priori option and a medium effect size, alpha of .05, and an increased power of 0.95 to have a proposed requirement of 111 participants. Therefore, 111 participants was the minimum sample size at the onset of the study.

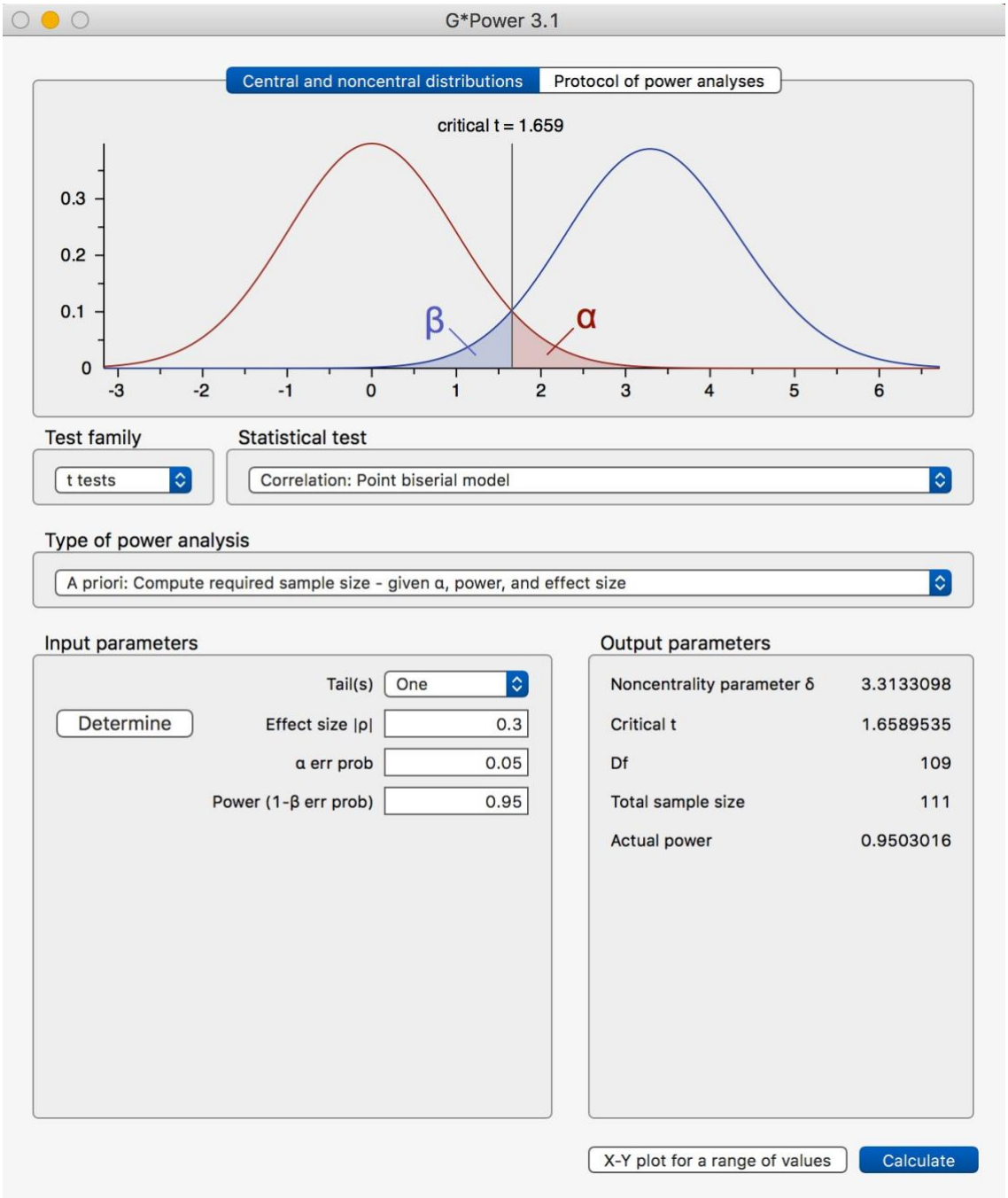


Figure 1. G*Power calculation.

Procedures for Recruitment, Participation, and Primary Data Collection

In Leedy and Ormrod (2015), the qualitative researcher searches for themes and patterns to organize data. The qualitative researcher often uses inductive reasoning. Many subject specific observations are made to generalize about a target population. On the other hand, quantitative researchers focus on using predetermined statistical procedures and objective criteria to analyze the outcomes of their procedures. Also, quantitative researchers often use deductive reasoning whereby they start with generalizations that lead them to draw specific conclusions. I obtained the sample by utilizing the following procedures.

Steps for Participant Recruitment and Data Collection

Step 1: I used SurveyMonkey to host the survey instrument that was used for purposive sampling.

Step 2: Cint initiated all contact with potential participants.

Step 3: Cint emailed an invitation to participate to potential respondents. The email contained a link to the survey for potential participants to select.

Step 4: Participants who clicked on the link landed on the first page of the survey which explained the benefits and risks of participation in the investigation and included a consent form.

Step 5: I provided a consent form for participation to each respondent to ascertain voluntary participation in the survey.

Step 6: Respondents consented by clicking consent on the survey link and by completing the survey.

Step 7: I used member checking to present survey responses back to the participants to check for inaccuracies in the replies.

Step 8: Participants used the online survey instrument to complete the member checking process prior to submission of the final survey responses.

Instrumentation and Operationalization of Constructs

I derived the questionnaire items that measured the variables in the study from a previously used instrument in consultation and with permission from Dr. Faith-Michael Uzoka. The primary instrument for the study was the palm vein authentication adoption survey (see Appendix A: Palm Vein Authentication Adoption Survey Instrument). I explored the elationship between intention to adopt palm vein authentication technology and perceived usefulness, complexity, security, peer influence, and relative advantage. I measured each variable separately with a specific hypothesis.

Research Question 1: What is the relationship, if any, between the intention to adopt a palm vein authentication system and perceived usefulness?

$H_0$1: There is no statistically significant relationship between the intention to adopt a palm vein authentication system and perceived usefulness.

H_a1: There is a statistically significant relationship between the intention to adopt a palm vein authentication system and perceived usefulness.

Research Question 2: What is the relationship, if any, between the intention to adopt a palm vein authentication system and complexity?

$H_0$2: There is no statistically significant relationship between the adoption of a palm vein authentication system and complexity.

H_a2: There is a statistically significant relationship between the adoption of a palm vein authentication system and complexity.

Research Question 3: What is the relationship, if any, between the adoption of a palm vein authentication system and security?

$H_0 3$: There is no statistically significant relationship between the adoption of a palm vein authentication system and security.

$H_a 3$: There is a statistically significant relationship between the adoption of a palm vein authentication system and security.

Research Question 4: What is the relationship, if any, between the adoption of a palm vein authentication system and peer influence?

$H_0 4$: There is no statistically significant relationship between the adoption of a palm vein authentication system and peer influence.

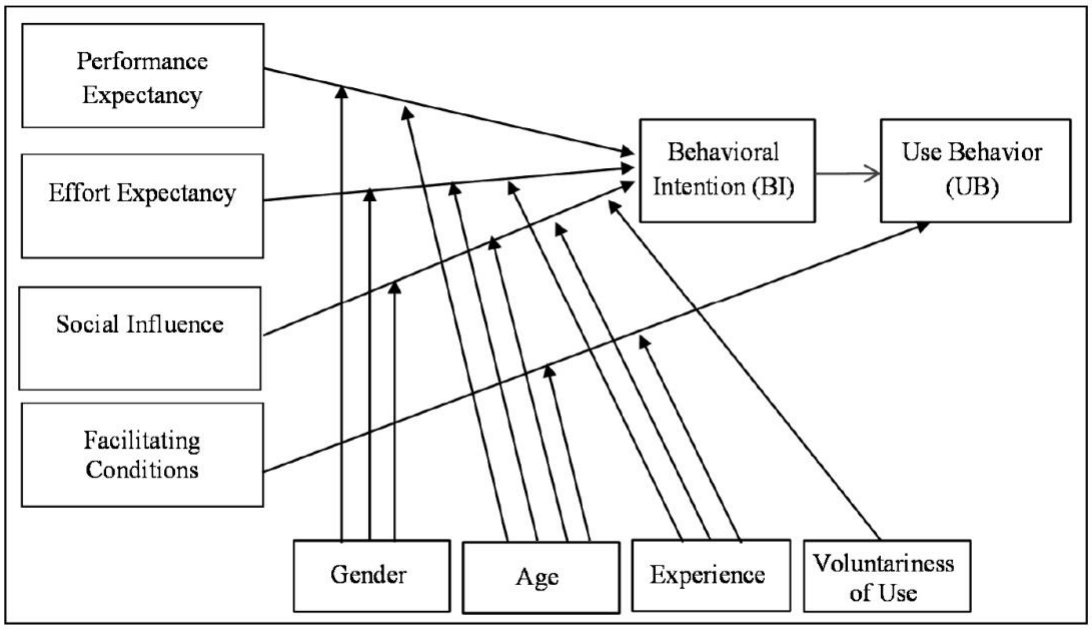
$H_a 4$: There is a statistically significant relationship between the adoption of a palm vein authentication system and peer influence.

Research Question 5: What is the relationship, if any, between the intention to adopt palm vein authentication and relative advantage?

$H_0 5$: There is no statistically significant relationship between the intention to adopt palm vein authentication and relative advantage.

$H_a 5$: There is a statistically significant relationship between the intention to adopt palm vein authentication and relative advantage.

Figure 2. Research Model



I outlined the palm vein authentication survey instrument in Appendix A, and I presented the invitational email in Appendix B. I used the palm vein authentication survey instrument to assess the following aspects of palm vein authentication:

- barriers and obstacles to palm vein authentication adoption,
- potential benefits of palm vein authentication adoption,
- prevalence and status of palm vein authentication adoption in organizations, and
- conditions that facilitate palm vein authentication adoption.

I asked healthcare managers and doctors to respond to items in each of these areas by using a five-point Likert scale that indicated the extent to which they agreed or disagreed with each statement.

Data Analysis Plan

A crucial ingredient to the success of the current investigation was obtaining data. I created the basis to support the findings of the study from the amount of data collected and the type of data collected. I achieved success in this study because of the sources of data and the types of data. I actualized high accuracy and reliability of the findings because of the data collection approach.

I used the electronic questionnaire to implement the survey approach among the participants. I used the self-administered electronic survey to collect data from 115 participants, 109 of whom fully completed the survey. I used a survey questionnaire because it was a relatively cost-effective and convenient data collection option as participants were able to complete questionnaires in my absence to avoid disruption of workplace schedules. The questionnaire instrument was an appropriate data collection strategy for the current investigation because of the quantitative nature of the data required. Also, the questionnaire instrument brought convenience and flexibility to the investigation.

I used statistical power considerations to guide the selection of the sample size for the present study. Statistical power is the prospect of rejecting the null hypothesis given a particular alpha level for rejection and effect size. Although investigators consider a power level of .8 adequate for hypothesis testing, investigators prefer a power level of .95 for hypothesis testing (Kraemer & Blasey, 2015). With a power level of .8, the likelihood that the investigator retained the null hypothesis rather than rejected the null hypothesis is 20%. With a power level of .95, the prospect that the investigator retained a false null

hypothesis is the same as the likelihood that the investigator rejected the null hypothesis when she should have retained the null hypothesis (given an alpha level of .05) (Kraemer & Blasey, 2015).

As noted earlier, statistical power is a function of the effect size and desired alpha level for rejection of the null hypothesis. Optimally, prior research findings would have indicated the average effect size to expect, and thereby would have guided the selection of effect sizes to consider. However, because this investigation was exploratory, estimates of effect sizes from prior research were not available. In the absence of a rich body of empirical studies, I relied on Kraemer and Blasey (2015) to define the effect sizes of interest for the current investigation. Kraemer and Blasey (2015) classified effect sizes as the population parameter that indicates how strong the hypothesis is according to the proportion of variance for which they account. Kraemer and Blasey (2015) graded an effect size that accounts for 10% or less of the variance in the dependent variable as weak. Moreover, Kraemer and Blasey (2015) classified an effect size that accounts for between 10 and 25% of the variance as moderate. Lastly, Kraemer and Blasey (2015) graded an effect size that accounts for more than 25% of the variance as strong. I utilized an alpha level of .05 to reject the null hypothesis as part of the power analysis for this study. An alpha level of .05 represents a widely accepted standard for rejection of the null hypothesis. This particular alpha level indicates that the observed association has less than a one in twenty chance of occurring by chance (Kraemer & Blasey, 2015). I calculated levels of statistical power using the GPOWER program (Erdfelder, Faul, & Buchner, 1996).

I designed the survey questionnaire to capture information for this study. I used frequency and percentages to measure categorically scaled variables. Additionally, I used range to measure continuously scaled variables. I captured perceptions of healthcare managers and doctors on the possibility of using palm vein recognition technology to mitigate the risk of medical fraud. To avoid difficulty in interpretation of questions in my absence, I modified the previously used survey instrument to arrive at self-explanatory questions that are easy for potential respondents to understand. As a result, the questions were in simple English using familiar healthcare terms to enable respondents to provide reliable and adequate responses to each survey question.

I adapted the survey instrument from an existing survey questionnaire used with permission from the authors (Appendices A-B). To administer the survey, I used the online approach as some participants may not be available in person for the current investigation. Moreover, the online approach is cost-effective and less time intensive. I downloaded all the data and stored them in the SurveyMonkey database and on a secure, home personal computer. After acquiring the data that informed the survey results from the participants, I re-encoded the data into IBM Statistical Package for Social Sciences (IBMSPSS) software for ease of management, data storage, and subsequent analyses. The data will remain in the secured, home personal computer for a minimum of 5 years.

Threats to Validity

External Validity

The validity of the information collected from healthcare managers and doctors is dependent on the quality of the questions inside the survey instrument (Mathieu, Aguinis,

Culpepper, & Chen, 2012). Investigators use several validation methods for both qualitative and quantitative research studies. For instance, investigators frequently employ triangulation as a strategy to examine the validity of information collected from the survey instrument. Investigators also employ member checking as another strategy for examining the validity of information collected from the survey instrument. During member checking, investigators submit responses back to the respondents to provide an opportunity for respondents to correct mistakes or add information. Investigators often use member checking to explore the validity of information collected from two research tools: (a) the interview and (b) the survey (Mathieu et al., 2012). I used member checking to present survey responses back to the survey participants to check for inaccuracies in the replies. Participants used the online survey instrument to complete the member checking process prior to submission of the final survey responses.

Aczel (2012) explained that the use of statistical tools to analyze data collected in a study would have little significance if the data were unreliable. The consistency of data collection, precision of data collection, and repeatability of the data collection method are critical research-reliability concerns.

Internal Validity

Internal validity takes different forms depending on (a) the nature of research problem, (b) the general methodology that the investigator employs to address the research problem, (c) the attributes of data collected, and (d) the strengths and weaknesses of the questionnaire. Investigators rely on five advantages of questionnaires to increase internal validity in an investigation. The five advantages are the following: (a)

economy, (b) anonymity, (c) standard questions, (d) uniform procedures, and (d) allowance for time for respondents to think about responses.

On the other hand, investigators contend with six disadvantages of questionnaires. The six disadvantages consist of the following:

1. low response rate,
2. inability to probe and clarify,
3. scoring open-ended items,
4. falsification of the answers,
5. restriction to subjects who can read and write the language that the investigator uses in the questionnaire, and
6. items that are biased or ambiguous (Leedy & Ormrod, 2015; McMillan & Schumacher, 2014; Straits & Singleton, 2011).

Construct Validity

Construct validity refers to the degree of appropriateness of the inferences that investigators formulate from the operationalizations in the investigation to the theoretical constructs that serve as the basis for those operationalizations.

Ethical Procedures

Since the data required to conclude the current investigation may be sensitive to the operations of healthcare organizations as well as to the privacy and safety of patients, the study needed to proceed carefully with regard to ethical procedures (Srivastava & Hopwood, 2009).

Therefore, I conducted the study in an ethical and responsible manner and in accordance with Walden University's Institutional Review Board guidelines. This study included only respondents who voluntarily agreed to participate. To assure this goal, every respondent received a consent form for participation to ascertain voluntary participation in the survey. I requested that the respondents consent by clicking consent on the survey link and by completing the survey. In the consent letter, the participants were able to opt out from the survey if they desired. Assistance program numbers were made available for participants on the consent form. Furthermore, I did not offer excessive inducements to solicit involvement of respondents in the study. If respondents declined to participate, then I did not penalize or sanction those persons.

I ensured complete privacy and anonymity of the respondents. No individual response has been made available to the public. I published and reported only general findings based on the analysis and summary of all the data. Also, I explained to each participant that this was academic research and that I would use participants' responses only for academic purposes and not any other purpose that may reflect on the healthcare organization's or a participant's personal image in any manner. I protected the privacy of all respondents by not revealing the accessed data to any third party. The introductory note in the questionnaire included this assurance. I ensured the anonymity of the healthcare institutions represented in the study. To achieve privacy and anonymity, I employed a strong coding framework so that no third party could use the reported results to identify the details of respondents and their organizations. I ensured the raw data

collected from the survey questionnaires remain saved in a secure password protected personal computer for at least five years to await further analysis.

Prior to beginning the survey instrument, I informed respondents about the potential risks and benefits of participating in the study. I believe participants did not encounter any unusual risk by completing the survey. I believe that participants benefited by taking part in the study in two respects. First, respondents gained an increased understanding of palm vein authentication. Secondly, respondents gained an increased understanding of the potential application of palm vein recognition technology to increase patient safety and decrease the risk of medical fraud.

Although the benefits of the research for the participants were indirect, they were also important. When malevolent parties gain access to critical information such as social security numbers, home addresses, family member data, health information, and other demographic information, individuals may experience identity theft, loss of privacy, and physical risks due to breaches of information security. From a macro perspective, society may experience increased healthcare costs, rising insurance premiums, declining productivity, loss of medical insurance, and rising cost of capital.

I presented documentation about the informed-consent process to all potential participants who visit the survey website through SurveyMonkey. Also, I provided information on the voluntary nature of the research, and I included information on the potential benefits and risks of the study in the invitational emails that I sent via the Cint tool. Furthermore, I documented the informed-consent process by requesting that the respondents indicate consent by clicking consent on the first page of the survey and by

completing the survey. I limited the sample selected for the present population to those who can complete the informed-consent process. I did not include minors in the sample. Additionally, I did not direct the sample toward vulnerable populations, e.g. persons with severe mental illness, because vulnerable populations may not have the ability to complete the informed-consent process.

To protect participants' privacy, I collected data through an anonymous server. I did not link identifying information to participants' responses to survey questions. I focused the analysis on the aggregate replies of the sample as one unit. Moreover, I did not report results for aggregate units containing fewer than 30 respondents. As a consequence, I provided assurance that the answers of a small cluster of respondents would remain confidential. I collected data on a secure survey website. I encrypted participants' responses to the survey prior to transmitting the replies via the internet. By using encryption tools, I assured that answers to the survey instrument may not be intercepted by a third party. Only authorized users with the correct username and password combination had access to the dataset collected on the survey website. I was the primary person with access to the datasets on the website. However, technical consultants who provided assistance with downloading the data and importing it into IBMSPSS for analysis accessed the datasets to facilitate the completion of the investigation.

Summary

In Chapter 3, I reported about the quantitative methodology that I used to investigate the principal research questions of the current investigation. Healthcare managers and doctors employed in the United States constituted the target population of

the research study. In the proposed study, I targeted two resources to obtain a sample of healthcare managers and doctors who are employed in diverse locations and work roles and who may be regarded as opinion leaders in matters of organizational direction and security. To this end, I used Cint and SurveyMonkey.

Respondents in the study were selected based upon purposive sampling (Mathieu & Chen, 2011). I designed the study with the assumption that I collected usable survey data from a minimum of 111 respondents. The primary instrumentation for the study was the palm vein authentication adoption survey. After obtaining the necessary permissions, I created this instrument by modifying a previously utilized instrument designed by Dr. Faith-Michael Uzoka and colleagues.

I collected data for the investigation using a secure survey website. I informed potential participants about the study with an invitational email sent via Cint. I furnished potential participants with a link to a secure website page. At this website page, I presented an opportunity for potential participants to complete the informed-consent process as part of the first page of the online survey questionnaire. Moreover, I communicated to survey respondents that a 1-2 page summary of the findings of the investigation would be made available by posting on social media and on ResearchGate after Walden University approves the findings and after I publish the results. I utilized the following data analytic tools:

1. Principal axis factoring for exploratory factor analysis,
2. Pearson's product moment correlation,
3. Multiple linear regression analysis, and

4. One-way analysis of variance (ANOVA).

I selected analytic methods to discuss the research questions. I informed potential participants about the voluntary nature of the investigation. Moreover, I informed participants about the requirement that potential participants must complete the informed-consent process to access the survey instrument. I did not offer excessive inducements to potential participants to solicit their involvement in the study. Also, I did not penalize nor sanction potential participants that declined to participate. Prior to beginning the survey, I informed potential participants about the voluntary nature of the research. Also, I informed potential respondents about the option of withdrawing from the study anytime during the process of replying to the questions in the survey.

In this Chapter, I explicated the research design that I used in this investigation. In Chapter 4, I review how I conducted the study and present empirical results and analysis for each of the five research questions. Finally in Chapter 5, I will conclude the dissertation with the following comments: (a) an interpretation of findings, (b) limitations of the study, (c) recommendations for further research grounded in the strengths and constraints of the study as well as the literature reviewed, (d) implications for social change, and (e) recommendations for practice.

Chapter 4: Results

The purpose of this quantitative correlational study was to understand the effectiveness of palm vein authentication technology as perceived by healthcare managers and doctors. The specific problem was the uncertainty surrounding the benefits of palm vein authentication relative to the growing crime of medical identity theft. Chapter 4 includes a detailed description of how I conducted the study, and collected and analyzed the data. Chapter 4 also includes the data analysis results and a discussion of how I used the findings to test the hypotheses and answer the research questions.

Data Collection

I used a purposive sampling technique. The participants included managers and doctors in the healthcare industry who use or have intention to use palm vein authentication. I sent the respondents a link to an anonymous self-administered online survey.

Of the 115 respondents who answered the questionnaire, 109 fully completed the survey. Although 109 did not meet the G*Power calculation requirement of 111, this was not a problem. Power concerns the ability of a test to reject the null hypothesis when it should be rejected and is an estimate that is used to show the feasibility of a proposed study. While the sample in this study was slightly short of the G*Power calculation (by 2), this discrepancy was not critical because the results from this study were statistically significant. I collected data over a 3-week period.

Study Results

I used Statistical Package for Social Sciences (SPSS) for data analysis. I conducted exploratory factor analysis to reduce the variables to a manageable and more relevant sets of variables (factors) that could affect the implementation of palm vein authentication. This analysis involved three stages: (a) generation of a correlation matrix for all variables, (b) extraction of factors from the correlation matrix, and (c) rotation of extracted factors in order to maximize the relationship between the variables and some factors. Finally, I carried out regression analysis on the identified factors in order to determine the extent of influence of the factors on intention to adopt palm vein authentication systems.

I used a questionnaire as the data collection instrument. The questionnaire focused on factors affecting palm vein authentication technology adoption. Based on the research model, I grouped these factors into the following four categories: (a) individual context, (b) implementation context, (c) technological context, and (d) observations. Based on the research model, I assigned the variables to the four categories in the following manner, prior to the application of exploratory factor analysis:

- Individual context – *perceived usefulness* (three variables), *relative advantage* (five variables) and *awareness* (three variables).
- Implementation context – *peer influence* (five variables), *resource facilitating conditions* (two variables), *technology facilitating conditions* (three variables), *self-efficacy* (four variables) and *security* (five variables).

- Technological context – *compatibility* (three variables), *relative advantage* (six variables), and *complexity* (three variables).
- Observations (five variables).

The variables were grouped into factors and were measured using the 5-point Likert-type scale (extending from 1 = strongly agree, to 5 = strongly disagree).

The online questionnaire data were downloaded from SurveyMonkey in an Excel spreadsheet in a comma separated values (CSV) format. I then uploaded the spreadsheet file into SPSS Version V24.0.0.0 for analysis and narrative interpretation. I reported the analysis in the following order:

1. Principal axis factoring.
2. Cronbach's alpha for the independent and dependent variables.
3. Descriptive statistics for independent and dependent variables.
4. Pearson product moment correlation analysis.
5. Data analysis and results.
6. Research Question 1 and Hypothesis 1.
7. Research Question 2 and Hypothesis 2.
8. Research Question 3 and Hypothesis 3.
9. Research Question 4 and Hypothesis 4.
10. Research Question 5 and Hypothesis 5.
11. Multiple linear regression analysis.

Principal Axis Factoring

I carried out a factor analysis using the principal axis factoring method to extract latent variables among the observed variables that could affect palm vein authentication implementation. I also generated the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy and Bartlett's test for suitability of factor analysis. The KMO measures the sampling adequacy, which should be greater than 0.5 for an acceptable factor analysis to continue. My data generated a KMO measure of 0.857. The Bartlett's test of sphericity ascertains whether the correlation matrix is an identity matrix, which would indicate that the factor model is inappropriate. The acceptable significance is 0.05 or less, while a $\chi 2$ value of 500 or more is adequate. The Bartlett's test produced a $\chi 2$ value of 2632.69 and a significance value of 0.000. The results from the KMO and Bartlett's test indicated the suitability of factor analysis. Although there is no strict rule with regard to the number of samples required in order to be able to use exploratory factor analysis, Costello and Osborne (2005) suggested that a data set with majority of loadings between 0.4 and 0.7 would be considered useful for exploratory factor analysis. Most of my loadings (rotated) were in the range of 0.4–0.8. MacCallum et al. (1999) suggested a mean communality of 0.7. My data showed a mean communality of 0.68, which is an indication of the adequacy of my sample size for exploratory principal factor analysis.

Table 1 shows all the extractable factors from the analysis. The exploratory factor analysis began with 36 variables relating to palm vein authentication adoption and acceptance that loaded on four distinct factors. The table also depicts the percentage contributions to the variability of data, eigenvalues, and Cronbach's α values for the

extracted factors. All extracted factors have Cronbach's α value greater than 0.5, which implies reliability and internal consistency of data. The extracted factors, which were considered useful for analysis included:

- Perceived usefulness: An individual's subjective perception that using the palm vein authentication system is beneficial. Fourteen variables loaded on this factor, which contributed 31.18% to data variability, internal consistency of 0.925.
- Complexity: The extent to which palm vein authentication is perceived as being relatively difficult to use and understand. Nine items loaded on this factor, which accounted for 15.57% variability in data, with internal consistency of 0.917.
- Security: The extent to which palm vein authentication is perceived to be better than other security methods. Seven variables loaded on this factor, which contributed 3.39% to data variability, internal consistency of 0.871.
- Peer influence: The extent to which palm vein authentication is perceived to be better than other security methods. Two variables loaded on this factor, which contributed % to data variability, internal consistency of 0.000.
- Relative advantage: The extent to which intention to adopt palm vein authentication is perceived to be better than a traditional security method. One variable loaded on this factor, which contributed % to data variability, internal consistency of 0.000.

Table 1

Principal Axis Factor Analysis

Factors	*Variables*	*Factor loading*	*No. of variables*	*Cronbach alpha*	*Eigen value*	*% of variance*
Perceived usefulness	I have the technical knowhow about palm vein authentication systems	.774	14	.93	11.23	31.18
	Palm vein authentication systems are convenient to use	.752				
	It is better than the other traditional methods	.743				
	I am comfortable with palm vein authentication technology.	.731				
	Palm vein authentication identification process is fast.	.713				
	Palm vein authentication system management process is simple and easy.	.690				
	Palm vein authentication system is easy to use.	.681				

(*table continues)*

Factors	*Variables*	*Factor loading*	*No of variables*	*Cronbach alpha*	*Eigen value*	*% of variance*
	It enhances job performance.	.639				
	It is a good match for the system that is currently used in my organization.	.638				
	I can use the system without assistance.	.579				
	My organization has the resources to run and maintain palm vein authentication systems.	.521				
	Palm vein authentication are accepted by people around.	.435				
	I use it because people around me use it.	.424				
	The issue of power has not been a hindrance to palm vein authentication usage.	.406				

(*table continues)*

Factors	*Variables*	*Factor loading*	*No of variables*	*Cronbach alpha*	*Eigen value*	*% of variance*
Complexity	There is always a problem while using the system.	.866	9	.92	5.60	15.57
	It is difficult to handle the system.	.857				
	It takes a lot of my time during usage.	.824				
	Using this system intimidates me.	.807				
	It is too intrusive.	.761				
	Only people with technical knowhow can use it.	.752				
	When using the system, I feel nervous.	.690				
	Delay and mismatch always occur.	.585				
	The cost of implementing and maintaining palm vein authentication is high.	.541				

(*table continues)*

Factors	*Variables*	*Factor loading*	*No of variables*	*Cronbach alpha*	*Eigen value*	*% of variance*
Security	The use of palm vein authentication systems will help improve the state of information security in healthcare.	.760	7	.87	1.22	3.39
	Palm vein authentication prevents unauthorized access to restricted information.	.680				
	Management is interested in new technology to reduce fraud.	.677				
	It is more secure and reliable than traditional forms of security/identification.	.622				
	It upholds the integrity of the information.	.564				

(*table continues)*

Factors	*Variables*	*Factor loading*	*No of variables*	*Cronbach alpha*	*Eigen value*	*% of variance*
	Using palm vein authentication will effectively and efficiently identify patients and users in the organization.	.472				
	Extra documents for identification are not needed.	.468				
Peer influence	Palm vein authentication implementation does not require managers to change their management philosophy.	.648	2			
	It does not involve a lot of process.	.526				
Relative advantage	Abuse of palm vein authentication information is unlikely.	.412	1			

Rotated Factor Matrix[a]

	Factor				
	1	2	3	4	5
q0022_0001	.774				
q0009_0001	.752				
q0014_0001	.743				
q0027_0001	.731				
q0023_0001	.713				
q0024_0001	.690				
q0007_0001	.681				
q0004_0001	.639				
q0035_0001	.638				
q0025_0001	.579				
q0047_0001	.521				
q0015_0001	.435				
q0016_0001	.424				
q0020_0001	.406				
q0034_0001					
q0045_0001		.866			
q0043_0001		.857			
q0026_0001		.824			
q0028_0001		.807			
q0049_0001		.761			
q0044_0001		.752			
q0010_0001		.690			
q0008_0001		.585			
q0048_0001		.541			
q0046_0001			.760		
q0041_0001			.680		
q0018_0001			.677		
q0031_0001			.622		
q0033_0001			.564		
q0006_0001			.472		
q0038_0001			.468		
q0021_0001					
q0040_0001					
q0017_0001				.648	
q0011_0001				.526	
q0042_0001					.412

Extraction Method: Principal Axis Factoring.
Rotation Method: Varimax with Kaiser Normalization.[a]

a. Rotation converged in 6 iterations.

Figure 3. Rotated factor matrix using principal axis factoring and varimax rotation method with Kaiser normalization.

Cronbach's Alpha for the Independent and Dependent Variables

Cronbach's alpha tests were conducted for each of the independent and dependent variables. Results of Cronbach alpha reliability testing presented in Table 2 showed all variables had scale scores above .7, indicating acceptable reliability. The Cronbach's alphas ranged from .871 to .925. There is no Cronbach alpha for peer influence because there are only two questions. A Cronbach alpha would not be useful in this case. Cronbach's alpha reliability was assessed using Green and Salkind's (2016) guidelines on reliability, where alpha values greater than .90 indicate excellent reliability, alpha values greater than .80 indicate good reliability, alpha values greater than .70 indicate acceptable reliability, alpha values greater than .60 indicate questionable reliability, and alpha values less than .60 indicate unacceptable reliability.

Table 2

Cronbach's Alpha Reliability Testing Results for the Variables

Variable	Cronbach's alpha	(*n* = number of items)
Perceived usefulness	.93	14
Complexity	.92	9
Security	.87	7
Peer influence		2
Relative advantage		1

Descriptive Statistics for the Independent and Dependent Variables

Table 3 shows descriptive statistics for perceived usefulness, complexity, security, peer influence, and relative advantage. For perceived usefulness, observations ranged from 14.00 to 58.00, with a mean observation of 29.56 (*SD* = 8.85). For complexity, observations ranged from 9.00 to 45.00, with a mean observation of 28.27 (*SD* = 8.33). For security, observations ranged from 7.00 to 23.00, with a mean observation of 13.67 (*SD* = 4.16). Means and standard deviations for continuous variables are presented in Table 3.

Table 3

Descriptive Statistics for Dependent and Independent Variables (N = 109)

Variable	*Mean*	*SD*	*Min*	*Max*
Perceived usefulness	29.56	8.85	14.00	58.00
Complexity	28.27	8.33	9.00	45.00
Security	13.67	4.16	7.00	23.00
Peer influence				
Relative advantage				

Pearson Product Moment Correlation Analysis

A Pearson product moment correlation matrix was created between perceived usefulness, complexity, security, peer influence, and intention to adopt. It was shown that

intention to adopt was significantly correlated with perceived usefulness, security, and peer influence. Table 4 shows the full correlation matrix.

Table 4

Correlation Matrix Between Perceived Usefulness, Complexity, Security, Peer Influence, and Intention to Adopt

	Perceived usefulness	Complexity	Security	Peer influence
Intention to adopt	.52**	-.09	.44**	.22*

Note. **$p \leq .010$; *$p \leq .05$.

Data Analysis and Results

Research Question 1 and Hypothesis 1

Research Question 1: What is the relationship, if any, between the intention to adopt a palm vein authentication system and perceived usefulness?

$H_0$1: There is no statistically significant relationship between the intention to adopt a palm vein authentication system and perceived usefulness.

H_a1: There is a statistically significant relationship between the intention to adopt a palm vein authentication system and perceived usefulness.

This hypothesis was tested using a Pearson product moment correlation. There was a statistically significant strong positive correlation between perceived usefulness and intention to adopt (See Table 5). Therefore, the null hypothesis was rejected. It was concluded that there is evidence to suggest that healthcare managers who have higher levels of perceived usefulness tend to have higher levels of intention to adopt palm vein authentication.

Table 5

Correlation Matrix Between Perceived Usefulness and Intention to Adopt

Pearson Product Moment Correlation Coefficient for Perceived Usefulness Versus Intention to adopt	
Correlation coefficient for perceived usefulness	.51
P value	<.001
N	109

Research Question 2 and Hypothesis 2

Research Question 2: What is the relationship, if any, between the intention to adopt a palm vein authentication system and complexity?

$H_0$2: There is no statistically significant relationship between the adoption of a palm vein authentication system and complexity.

H_a2: There is a statistically significant relationship between the adoption of a palm vein authentication system and complexity.

Table 6 shows no statistically significant correlation between complexity and intention to adopt palm vein authentication, $r = .09$, $p = .331$. Therefore, the null hypothesis was accepted and it was concluded that there is no statistically significant relationship between the intention to adopt palm vein authentication and complexity.

Table 6

Correlation Matrix Between Complexity and Intention to Adopt

Pearson Product Moment Correlation Coefficient for Complexity Versus Intention to Adopt	
Correlation coefficient for complexity	.09
P value	.331
N	109

Research Question 3 and Hypothesis 3

Research Question 3: What is the relationship, if any, between the adoption of a palm vein authentication system and security?

$H_0$3: There is no statistically significant relationship between the adoption of a palm vein authentication system and security.

H_a3: There is a statistically significant relationship between the adoption of a palm vein authentication system and security.

Table 7 shows a statistically significant moderately positive correlation between security and intention to adopt, $r = .44$, $p < .001$. Therefore, the null hypothesis was rejected and it was concluded that there is moderate evidence to suggest that healthcare managers who perceive a higher level of security tend to have a higher level of intention to adopt palm vein authentication.

Table 7

Correlation Matrix Between Security and Intention to Adopt

Pearson Product Moment Correlation Coefficient for Security Versus Intention to Adopt	
Correlation coefficient for security	.44
P value	<.001
N	109

Research Question 4 and Hypothesis 4

Research Question 4: What is the relationship, if any, between the adoption of a palm vein authentication system and peer influence?

$H_0$4: There is no statistically significant relationship between the adoption of a palm vein authentication system and peer influence.

H_a4: There is a statistically significant relationship between the adoption of a palm vein authentication system and peer influence.

Table 8 shows a statistically significant weak positive correlation between peer influence and intention to adopt, $r = .22$, $p = .019$. Therefore, the null hypothesis was rejected and it was concluded that there is weak evidence to suggest that healthcare managers who perceive a higher level of peer influence tend to have a higher level of intention to adopt palm vein authentication.

Table 8

Correlation Matrix Between Peer Influence and Intention to Adopt

Pearson Product Moment Correlation Coefficient for Peer Influence Versus Intention to Adopt	
Correlation coefficient for peer influence	.22
P value	.019
N	109

Research Question 5 and Hypothesis 5

Research Question 5: What is the relationship, if any, between the intention to adopt palm vein authentication and relative advantage?

$H_0$5: There is no statistically significant relationship between the intention to adopt palm vein authentication and relative advantage.

H_a5: There is a statistically significant relationship between the intention to adopt palm vein authentication and relative advantage.

Table 9 shows a statistically significant weak positive correlation between relative advantage and intention to adopt palm vein authentication, $r = .22$, $p = .020$. Therefore, the null hypothesis was rejected and it was concluded that there is weak evidence to suggest that healthcare managers who perceive a higher level of relative advantage tend to have a higher level of intention to adopt palm vein authentication.

Table 9

Correlation Matrix Between Relative Advantage and Intention to Adopt

Pearson Product Moment Correlation Coefficient for Relative Advantage Versus Intention to Adopt	
Correlation coefficient for relative advantage	.22
P value	.020
N	109

Multiple Linear Regression Analysis

To further explore the relationship between the dependent variable and the independent variables, I conducted a stepwise multiple linear regression analysis. I used perceived usefulness, security, peer influence, and relative advantage as the independent variable. I used intention to adopt as the dependent variable.

The results of the linear regression were significant, $F(4,104) = 10.03$, $p < .001$, $R^2 = 0.28$, suggesting that perceived usefulness, security, peer influence, and relative advantage accounted for 28% of the variance in intention to adopt. Also, the variance inflation factors for perceived usefulness, security, peer influence, and relative advantage

were all less than 3, eliminating the need to worry about multicollinearity and permitting the use of the identified predictor variables in the regression model. The individual predictors were examined further. Perceived usefulness was a significant predictor of intention to adopt, $B = 0.05$, $p < .001$, suggesting that for every one unit increase in perceived usefulness, intention to adopt increased by 0.05 units. Security was not found to be a significant predictor of intention to adopt. Peer influence was not found to be a significant predictor of intention to adopt. Relative advantage was not found to be a significant predictor of intention to adopt.

Table 10 presents a considered and useful summary of the results gleaned from the data collected.

Table 10

Results for Multiple Linear Regression with Perceived Usefulness, Security, Peer Influence, and Relative Advantage Predicting Intention to Adopt

	B	*SE*	β	*t*	*P*
(Constant)	5.60	.34		16.719	.000
Perceived usefulness	.05	.01	.45	3.50	.000
Security	.04	.03	.17	1.35	.179
Peer influence	-.04	.06	.07	.70	.487
Relative advantage	-.05	.09	.05	.51	.61

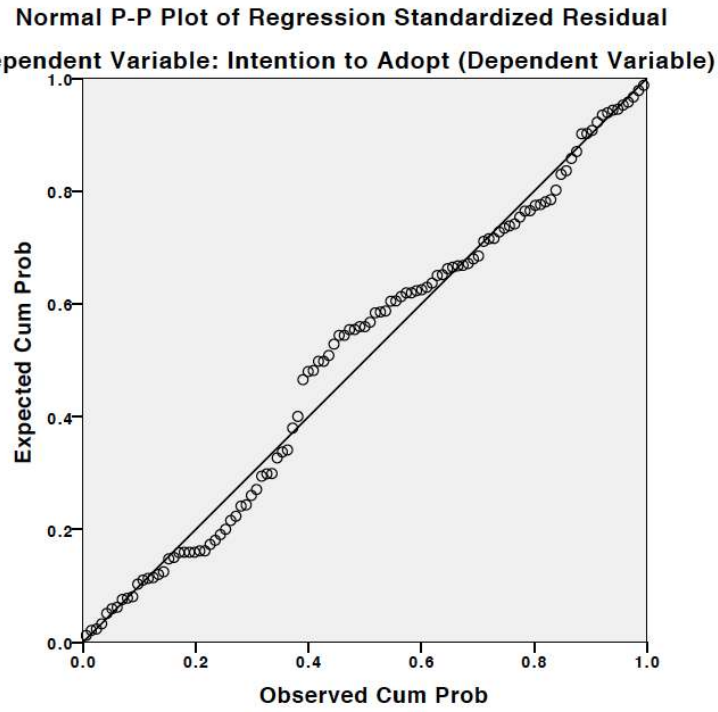


Figure 4. P-P scatter plot for normality for perceived usefulness, security, peer influence, and relative advantage predicting intention to adopt palm vein authentication.

Summary

The purpose of this quantitative study was to explore the potential relationship among the variables intention to adopt, perceived usefulness, complexity, security, peer influence, and relative advantage based on a survey of healthcare managers.

The Pearson product moment correlation coefficient was used to test the hypotheses. Results showed that among healthcare managers, perceived usefulness, security, and peer influence had a statistically significant, correlation with intention to adopt. No evidence of a relationship existed between complexity and intention to adopt. Therefore, it was concluded that healthcare providers who adopt palm vein authentication

technology tend to perceive palm vein authentication to be beneficial, to be effective at providing a sense of protection, and to view palm vein authentication as a technology that others believe should be used.

The results of the linear regression were significant, $F(4,104) = 10.03$, $p < .001$, $R2 = 0.28$, suggesting that perceived usefulness, security, peer influence, and relative advantage accounted for 28% of the variance in intention to adopt. Furthermore, perceived usefulness was found to be a significant predictor of intention to adopt, $B = 0.05$, $p < .001$, suggesting that for every one unit increase in perceived usefulness, intention to adopt increased by 0.05 units. Security was not found to be a significant predictor of intention to adopt. Peer influence was not found to be a significant predictor of intention to adopt. Relative advantage was not found to be a significant predictor of intention to adopt.

Table 11 presents a useful summary of the findings gleaned from the data collected.

Table 11

Summary of Findings

	Research Question	Research Hypothesis	Survey Questions	Type of Analysis	Result	Conclusion
RQ 1	What is the relationship, if any, between the intention to adopt palm vein authentication and perceived usefulness?	There is a statistically significant relationship between the intention to adopt palm vein authentication and perceived usefulness.	I have the technical knowhow about palm vein authentication systems. Palm vein authentication systems are convenient to use. It is better than the other traditional methods. I am comfortable with palm vein authentication technology.	SPSS-Pearson product moment	$r = 0.51$, $p <$ .001	Statistically significant, strong-moderate positive relationship between intention to adopt palm vein authentication and perceived usefulness

(*table continues)*

Research Question	Research Hypothesis	Survey Questions	Type of Analysis	Result	Conclusion
		Palm vein authentication identification process is fast. Palm vein authentication system management process is simple and easy. Palm vein authentication system is easy to use. It enhances job performance. It is a good match for the system that is currently used in my organization. I can use the system without assistance. My organization has the resources to run and maintain palm vein authentication systems.			

(*table continues)*

	Research Question	Research Hypothesis	Survey Questions	Type of Analysis	Result	Conclusion
			Palm vein authentication are accepted by people around. I use it because people around me use it. The issue of power has not been a hindrance to palm vein authentication usage.			
RQ 2	What is the relationship, if any, between the intention to adopt palm vein authentication and complexity?	There is a statistically significant relationship between the intention to adopt palm vein authentication and complexity.	There is always a problem while using the system. It is difficult to handle the system. It takes a lot of my time during usage. Using this system intimidates me.	SPSS-Pearson product moment	$r = .09$, $p = .331$	Very weak or no relationship based on both r and p. Unable to reject the null hypothesis.

(*table continues)*

	Research Question	Research Hypothesis	Survey Questions	Type of Analysis	Result	Conclusion
			It is too intrusive. Only people with technical knowhow can use it. When using the system, I feel nervous. Delay and mismatch always occur. The cost of implementing and maintaining palm vein authentication is high.			
RQ 3	What is the relationship, if any, between the intention to adopt palm vein authentication and security?	There is a statistically significant relationship between the intention to adopt palm vein authentication and security.	The use of palm vein authentication systems will help improve the state of information security in healthcare.	SPSS-Pearson product moment	$r = .44$, $p < .001$	Statistically significant, moderately positive relationship between intention to adopt palm vein authentication and security

(*table continues)*

Research Question	Research Hypothesis	Survey Questions	Type of Analysis	Result	Conclusion
		Palm vein authentication prevents unauthorized access to restricted information. Management is interested in new technology to reduce fraud. It is more secure and reliable than traditional forms of security/identification. It upholds the integrity of the information. Using palm vein authentication will effectively and efficiently identify patients and users in the organization. Extra documents for identification are not needed.			

(*table continues)*

	Research Question	Research Hypothesis	Survey Questions	Type of Analysis	Result	Conclusion
RQ 4	What is the relationship, if any, between intention to adopt palm vein authentication and peer influence?	There is a statistically significant relationship between the intention to adopt palm vein authentication and peer influence.	Palm vein authentication implementation does not require managers to change their management philosophy. It does not involve a lot of process.	SPSS-Pearson product moment	$r = .22$, $p = .019$	Statistically significant, weak positive relationship between peer influence and intention to adopt
RQ 5	What is the relationship, if any, between the intention to adopt palm vein authentication and relative advantage?	There is a statistically significant relationship between the intention to adopt palm vein authentication and relative advantage.	Abuse of palm vein authentication information is unlikely.	SPSS-Pearson product moment		

In Chapter 5, I provide an interpretation of the study results, an explanation of the limitations of the study, recommendations for action, and suggestions for future research. Also in Chapter 5, I discuss the findings of the study regarding implications for social change.

Chapter 5: Discussion, Conclusions, and Recommendations

The purpose of this study was to understand healthcare managers' and doctors' perceptions of the effectiveness of palm vein authentication technology. To understand healthcare managers' and doctors' perceptions of the effectiveness of palm vein authentication technology, I explored the potential relationship among the variables intention to adopt, perceived usefulness, complexity, security, peer influence, and relative advantage based on a survey of healthcare managers. Sayed (2015) and Zeng and Jin (2012) identified palm vein authentication as a better alternative to other biometric technologies, but it has not been adequately implemented. Healthcare organizations should study the reliability and advantages offered by these identification systems. For years, law enforcement agencies have used DNA technologies to assist in finding and arresting criminals, and even to set free some wrongly convicted people. With the growing crime of medical identity theft, organizations should study palm vein authentication as a potential solution, thereby realizing the cost savings that comes with a reduction in fraud.

The remainder of the chapter includes an overview of the study, a summary of the answers to the research questions and results of the hypothesis testing, a discussion of the results in relation to literature, limitations, implications of the results for practice, implications for positive social change, recommendation for future research, and the conclusion.

I collected data over the course of 3 weeks using Cint, SurveyMonkey, and a participant pool. The results of the study showed that intention to adopt was significantly

correlated with perceived usefulness, security, peer influence, and relative advantage. However, no relationship existed between intention to adopt and complexity.

The results of the linear regression were significant, $F(4,104) = 10.03$, $p < .001$, $R^2 = 0.28$, indicating that perceived usefulness, security, peer influence, and relative advantage accounted for 28% of the variance in intention to adopt. Also, the variance inflation factors for perceived usefulness, security, peer influence, and relative advantage were all less than 3, eliminating the need to worry about multicollinearity and permitting the use of the identified predictor variables in the regression model. I examined the individual predictors were further. Perceived usefulness was a significant predictor of intention to adopt, B = 0.51, p < .001, indicating that for every one unit increase in perceived usefulness, intention to adopt increased by 0.51 units. Security was not found to be a significant predictor of intention to adopt. Neither peer influence nor relative advantage were found to be significant predictors of intention to adopt.

Interpretation of Findings

Participants in the study included healthcare managers and doctors ($N = 109$) from a Cint online panel that I used as the respondent pool for this study. I did not collect demographic statistics. To support rejecting the null hypotheses with a confidence level of 95%, I used the statistics standard $p < .05$.

Research Question 1

Research Question 1: What is the relationship, if any, between the intention to adopt a palm vein authentication system and perceived usefulness?

$H_0$1: There is no statistically significant relationship between the intention to adopt a palm vein authentication system and perceived usefulness.

H_a1: There is a statistically significant relationship between the intention to adopt a palm vein authentication system and perceived usefulness.

To address Research Question 1, I tested the null hypothesis using the Pearson product moment correlation statistic. The result of the data analysis, $r = .52$, $p < .001$, indicated that a correlation existed and that perceived usefulness positively related to intention to adopt. Additionally, the results of the linear regression were significant, $F(1,107) = 37.97$, $p < .001$, suggesting that perceived usefulness accounted for (R^2) 26.2% of the variance in intention to adopt. Perceived usefulness was a significant predictor of intention to adopt palm vein authentication technology, $B = 0.06$, $p < .001$, suggesting that for every one unit increase in perceived usefulness, intention to adopt increased by 0.06 units. Because a p value of < .001 did not exceed significance level of .05, the null hypothesis was rejected. I concluded that healthcare managers who perceive greater levels of intention to adopt palm vein authentication tend to have a greater level of perceived usefulness.

This is the first study of its kind about the intention to adopt palm vein authentication technology. In previous studies, researchers explored the intention to adopt technology in general or the intention to adopt biometrics technology in general. As a result, a strict like-to-like comparison is not available for this study; however, a cursory analysis can quickly highlight a finding that seems irrational and warrants additional investigation. With this in mind, I found perceived usefulness to influence an individual's

intention to adopt palm vein authentication technology. The results of this study were consistent with those of Davis (1989) and Gefen, Karahanna, and Straub (2003) who examined the intention to adopt technology in general. The results of this study were also consistent with those of James, Pirim, Boswell, Reithel, and Barkhi (2006) who found perceived usefulness to positively affect the intention to adopt biometric technology. Contrarily, Akinnuwesi, Uzoka, Okwundu, and Fashoto (2016) did not find any significant relationship between perceived usefulness and intention to adopt biometrics. The implication of this discrepancy might be that individuals in developing countries may not see perceived usefulness as a motivation for adopting biometrics technology; whereas, individuals in developed countries may see perceived usefulness as a motivation for adopting palm vein authentication technology.

Research Question 2

Research Question 2: What is the relationship, if any, between the intention to adopt a palm vein authentication system and complexity?

$H_0$2: There is no statistically significant relationship between the adoption of a palm vein authentication system and complexity.

H_a2: There is a statistically significant relationship between the adoption of a palm vein authentication system and complexity.

To address Research Question 2, I tested the null hypothesis using the Pearson product moment correlation statistic. The result of the data analysis, $r = .09$, $p = .331$, indicated that there was not a statistically significant correlation between complexity and

intention to adopt palm vein authentication technology. As a result, I excluded complexity from the linear regression analysis.

Since this is the first study of its kind and I cannot make a strict like-to-like comparison, I completed a cursory analysis. With this in mind, I found complexity to have no statistically significant correlation with intention to adopt palm vein authentication technology. Uzoka and Ndzinge (2009) found that complexity associated with understanding and using a biometric system could affect an individual's intention to adopt biometric technology. However, the findings in the study did not support previous findings. A possible explanation for this could be the circumstance that a strict like-to-like comparison is not available for this study. Another possible explanation for this could be the context that most biometric methods adopted by the respondents are the simple-to-use methods.

Research Question 3

Research Question 3: What is the relationship, if any, between the adoption of a palm vein authentication system and security?

$H_0$3: There is no statistically significant relationship between the adoption of a palm vein authentication system and security.

H_a3: There is a statistically significant relationship between the adoption of a palm vein authentication system and security.

To address Research Question 3, I tested the null hypothesis using the Pearson Product moment correlation statistic. The result of the data analysis, $r = .44$, $p < .001$, indicated that a correlation existed and security positively related to intention to adopt.

Additionally, the results of the linear regression were significant, $F(1,107) = 25.42$, $p < .001$, suggesting that security accounted for ($R2$) 19.2% of the variance in intention to adopt. security was a significant predictor of intention to adopt palm vein authentication technology, $B = 0.11$, $p < .001$, suggesting that for every one unit increase in security, intention to adopt increased by 0.11 units. Because a p value of < .001 did not exceed significance level of .05, the null hypothesis was rejected. I concluded that healthcare managers who perceive greater levels of intention to adopt palm vein authentication tend to have a greater level of security.

Since this is the first study of its kind and I cannot make a strict like-to-like comparison, I completed a cursory analysis. In previous studies, researchers explored the intention to adopt technology in general or biometrics technology in general. With this in mind, I found security to influence an individual's intention to adopt palm vein authentication technology. Security encompasses the extent to which the system provides a sense of protection against loss, attack, or harm. The results of this study were consistent with those of Uzoka and Ndzinge (2009) and Akinnuwesi et al. (2016) who found that security had a significant influence on the intention to adopt biometrics technology in general.

Research Question 4

Research Question 4: What is the relationship, if any, between the adoption of a palm vein authentication system and peer influence?

$H_0$4: There is no statistically significant relationship between the adoption of a palm vein authentication system and peer influence.

H_a4: There is a statistically significant relationship between the adoption of a palm vein authentication system and peer influence.

To address research question 4, I tested the null Hypothesis using the Pearson product moment correlation statistic. The result of the data analysis, $r = .22$, $p = .02$ indicated that a correlation existed and the peer influence positively related to intention to adopt. Additionally, the results of the linear regression were significant, $F(1,110) = 5.63$, $p = .019$, suggesting that peer influence accounted for ($R2$) 4.9% of the variance in intention to adopt. Peer influence was a significant predictor of intention to adopt palm vein authentication technology, $B = 0.14$, $p = .019$, suggesting that for every one unit increase in peer influence, intention to adopt increased by 0.14 units. Because a p value of .019 did not exceed significance level of .05, the null hypothesis was rejected. It was concluded that healthcare managers who perceive greater levels of intention to adopt palm vein authentication tend to have a greater level of peer influence.

Since this is the first study of its kind and I cannot make a strict like-to-like comparison, I completed a cursory analysis. With this in mind, I found peer influence to influence an individual's intention to adopt palm vein authentication technology. The effect of peer influence varies among studies. Al-Qeisi (2009) found peer influence to be important in the early stages of an individual's experience with a new technology and when rewards and punishment are applicable. Akinnuwesi et al. (2016) did not show peer influence to be a significant factor in the adoption of biometric technology.

Research Question 5

Research Question 5: What is the relationship, if any, between the intention to adopt palm vein authentication and relative advantage?

$H_0$5: There is no statistically significant relationship between the intention to adopt palm vein authentication and relative advantage.

H_a5: There is a statistically significant relationship between the intention to adopt palm vein authentication and relative advantage.

To address research question 5, I tested the null Hypothesis using the Pearson product moment correlation statistic. The result of the data analysis, $r = .22$, $p = .020$ indicated that a weak positive correlation existed and the relative advantage positively related to intention to adopt. Additionally, the results of the linear regression were significant, $F(1,107) = 5.59$, $p = .02$, suggesting that relative advantage accounted for ($R2$) 5.0% of the variance in intention to adopt. Relative advantage was a significant predictor of intention to adopt palm vein authentication, $B = 0.21$, $p <= .02$, suggesting that for every one unit increase in relative advantage, intention to adopt increased by 0.21 units. Because a p value of =.020 did not exceed significance level of .05, the null hypothesis was rejected. It was concluded that healthcare managers who perceive greater levels of intention to adopt palm vein authentication tend to have a greater level of relative advantage.

Since this is the first study of its kind and I cannot make a strict like-to-like comparison, I completed a cursory analysis. With this in mind, I found relative advantage to influence an individual's intention to adopt palm vein authentication technology.

The effect of relative advantage varies among studies. Both Uzoka and Ndzinge (2009) and Akinnuwesi et al. (2016) did not show relative advantage to be a significant factor in the intention to adopt biometric technology. However, the results of the current study are in consonance with previous results obtained by Lau, Yen, and Chau (2001) where perceived benefit or perceived relative advantage was found to have significant influence on the intention to adopt biometric technology.

Limitations of the Study

One limitation of the study was the methodological approach used. Even though I was able to find a relationship or no relationship between the independent and dependent variables, I did not investigate cause and effect among the variables. To obtain contextual information about the impact of a palm vein authentication system on perceived usefulness, complexity, security, peer influence, and relative advantage, a mixed-method or qualitative method would be more appropriate. Because of the limited amount of close ended questions as part of the quantitative research design of the study, I limited the options available to the participants. Because of the limited number of participants in the study sample as part of the research design, I potentially limited diversity of perspectives among the participants. Another limitation of the study was the purposeful sample of healthcare managers and doctors. The purposeful selection of participants could have precluded the collection of data from individuals whose insights could have been relevant to the study. Finally, I collected data from one country. Thus, the results are not generalizable to healthcare managers worldwide.

Recommendations

This study is the first step towards understanding where to focus and what variables to consider in a future causal analysis. A study on the cause and effect of the variables may shed more light about the impact of palm vein authentication on patient safety and on the risk of medical fraud. Future researchers may want to replicate this study and explore the relationships among the demographics. One possibility may be a study in which researchers explore what the findings will be across different demographic variables. More study needs to be conducted on the relationship between palm vein authentication systems and patient safety. This study provided a base, however, more research is necessary on this subject and perhaps with a different instrument.

Implications

The data from this study affects social change by providing healthcare leaders with critical information needed to make informed decisions at the state, local, and national level. The study has practical implications for policy-makers and stakeholders who are interested in supporting the adoption of biometric technologies in the healthcare industry to reduce the risk of medical fraud and enhance patient safety. The findings of the study show that perceived usefulness was significantly positively correlated with intention to adopt a palm vein authentication system. Security was significantly positively correlated with intention to adopt a palm vein authentication system. Peer influence was significantly positively correlated with intention to adopt a palm vein authentication system.

The data in the current study contributes to the field of management by providing to healthcare leaders and policymakers the daily perceptions of healthcare managers about palm vein authentication systems. The results of this study may help leaders of hospitals and other healthcare providers understand the perspectives of healthcare managers, and therefore, enable them to shape policies and procedures that guide the adoption of palm vein authentication systems to mitigate the risk of medical fraud and improve patient identification.

Conclusions

The conduct of a quantitative study supported the exploration of how healthcare managers and doctors perceive palm vein authentication technology as a means to counteract the commitment of medical fraud. I used data gathered from an anonymous online survey to investigate how leaders with responsibility for management perceive the identification solution that palm vein authentication provides to enhance the efficacy of fraud mitigation efforts. The use of a quantitative study protocol supported the demonstration of study reliability by examining the internal consistency of the data. The use of statistical confidence limits supported the external validity of the findings. Use of the software package SPSS v.24 supported the grouping of questionnaire items into factors that I analyzed about how they related to the intention to adopt a palm vein authentication system.

Study findings seem to agree with some of the results found in previous studies on adoption of biometric technology. Because this is the first study on adoption of palm vein authentication technology, which is a specific modality of biometric technology, a strict

comparison of findings is not available. A key recommendation is the need for critical infrastructure organizations like banks and healthcare centers to study the possibility of taking advantage of the reliability and advantages offered by palm vein authentication systems. Another recommendation is the need for increased investment in palm vein authentication systems. Efforts in Japan and other developed countries show tangible benefits to society. Healthcare policymakers and leaders should work to increase medical fraud mitigation capabilities.

Among healthcare managers and doctors, a statistically significant positive correlation existed between perceived usefulness, security, peer influence, and intention to adopt a palm vein authentication system. No statistically significant correlation existed between complexity and intention to adopt a palm vein authentication system.

The results of this study may help leaders of hospitals and other healthcare providers understand the perspectives of healthcare managers, and therefore, enable them to shape policies and procedures that guide the adoption of palm vein authentication systems to mitigate the risk of medical fraud and improve patient identification.

References

Aczel, A. D. (2012). *Complete business statistics* (8th ed.). Morristown, NJ: Wohl Publishing.

Agrawal S., & Budetti P. (2012). Physician medical identity theft. *JAMA*, *307*(5), 459–460. doi:10.1001/jama.2012.78

Ahlan, A. R., & Ahmad, B. I. (2014). User acceptance of health information technology (HIT) in developing countries: A conceptual model. *Procedia Technology*, *16*, 1287–1296. doi:10.1016/j.protcy.2014.10.145

Ahmad, S. M. S., Ali, B. M., & Adnan, W. A. W. (2012). Technical issues and challenges of biometric applications as access control tools of information security. *International Journal of Innovative Computing, Information and Control*, *8*(11), 7983–7999. Retrieved from http://www.ijicic.org/ijicic-ksi-13.pdf

Ahmad, A., Bosua, R., & Scheepers, R. (2014). Protecting organizational competitive advantage: a knowledge leakage perspective. *Computers and security*, *42*, 27–39. doi:10.1016/j.cose.2014.01.001

Ahmed, M. A., Ebied, H. M., El-Horbaty, E.-S. M., & Salem, A.-B. M. (2013). Analysis of palm vein pattern recognition algorithms and systems. *International Journal of Bio-Medical Informatics and e-Health, 1*(1), 10-14. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.380.388&rep=rep1&type=pdf

Ahmed, M. A., El-Horbaty, E.-S. M., & Salem, A.-B. M. (2015). Intelligent techniques for matching palm vein images. *Egyptian Computer Science Journal*, *39*(1), 1-14.

Retrieved from http://www.ecsjournal.org/Archive/Volume39/Issue1/1.pdf

Akinnuwesi, B. A., Uzoka, F.-M. E., Okwundu, O. S., & Fashoto, G. (2016). Exploring biometric technology adoption in a developing country context using the modified UTAUT. *International Journal of Business Information Systems, 23*(4), 482–521. doi:10.1504/IJBIS.2016.080219

Al-Juboori, A. M., Wu, X., & Zhao, Q. (2013). Biometric authentication system based on palm vein. *2013 International Conference on Computer Sciences and Applications*, 52-58. doi:10.1109/csa.2013.19

Al-Qeisi, K.I. (2009) *Analyzing the Use of UTAUT Model in Explaining an Online Behaviour: Internet Banking Adoption*, A thesis submitted for the degree of Doctor of Philosophy, Brunel University Brunel Business School PhD theses [online]. Retrieved from http://bura.brunel.ac.uk/handle/2438/3620

Anderson, J. P. (1980). *Computer security threat monitoring and surveillance*. Retrieved from http://csrc.nist.gov/publications/history/ande80.pdf

Ao, X. (2015). The shortcomings of the current definitions of an asset and the substance of an asset. In *Engineering Technology, Engineering Education and Engineering Management: Proceedings of the 2014 International Conference on Engineering Technology, Engineering Education and Engineering Management (ETEEEM 2014),* 467. Retrieved from https://books.google.com/books?hl=en&lr=&id =lUZOCgAAQBAJ&oi=fnd&pg=PA467&dq=what+is+the+definition+of+an+as set&ots =ZA7tuusxTu&sig=wn5mPsEZdyPLtH2qH3HOE0kPE9E

Arandjelović, R., & Zisserman, A. (2012). Three things everyone should know to improve object retrieval. In *2012 IEEE Conference on Computer Vision and Pattern Recognition*, 2911–2918. doi:10.1109/CVPR.2012.6248018

Berwick, D. M., & Hackbarth, A. D. (2012). Eliminating waste in US health care. *JAMA*, *307*(14), 1513–1516. doi:10.1001/jama.2012.362

Biegelman, M. T. (Ed.). (2012). Medical identity theft. In *Identity Theft Handbook* (pp. 97–112). John Wiley & Sons, Inc. Retrieved from http://onlinelibrary.wiley.com/doi/10.1002/9781119203162.ch8/summary

Bosco, F. A., Singh, K., Aguinis, H., Field, J. G., & Pierce, C. A. (2015). Correlational effect size benchmarks. *Journal of Applied Psychology*, *100*(2), 431–449. doi:10.1037/a0038047

Brown, C. (2012). Health care data protection and biometric authentication policies: Comparative culture and technology acceptance in China and in the United States. *Review of Policy Research, 29*(1), 141-159. doi:10.1111/j.1541-1338.2011.00546.x

Cantoni, L., & Danowski, J. A. (2015). *Communication and technology*. Berlin, Germany: Walter de Gruyter GmbH & Co KG.

Cao, L., & Zhu, H. (2013). Normal accidents. *Journal of Data and Information Quality*, *4*(3), 1–26. doi:10.1145/2458517.2458519

Chen, H. X. (2012). *Approaches to quantitative research: A guide for dissertation students*. Cork, Ireland: Oak Tree Press.

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2013). Organizations' information security

policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, *29*(3), 157–188. doi:10.2753/MIS0742-1222290305

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2015). Impacts of comprehensive information security programs on information security culture. *The Journal of Computer Information Systems*, *55*(3), 11–19. Retrieved from http://iacis.org/jcis/articles/55-3-2.pdf

Chingovska, I., Anjos, A., & Marcel, S. (2014). Biometrics evaluation under spoofing attacks. *IEEE Transactions on Information Forensics and Security, 9*(12), 2264–2276. doi:10.1109/tifs.2014.2349158

Classen, D. C., Resar, R., Griffin, F., Federico, F., Frankel, T., Kimmel, N., … James, B. C. (2011). "Global Trigger Tool" shows that adverse events in hospitals may be ten times greater than previously measured. *Health Affairs*, *30*(4), 581–589. doi:10.1377/hlthaff.2011.0190

Costello, A.B. & Osborne, J.W. (2005). Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis. *Practical Assessment, Research and Evaluation, 10*(7), 1–9. Retrieved from http://www.pareonline.net/pdf/v10n7.pdf

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Thousand Oaks: SAGE Publications, Inc.

Davenport, T. H., & Harris, J. G. (2007). *Competing on analytics: The new science of winning*. Boston: Harvard Business School Press.

Davidson, S. (2015). The evaluation methods of an enterprise economic potential.

International Journal, (1). Retrieved from http://www.ijournales.org/archive/volume2015/issue1/46.pdf

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319–340. doi:10.2307/249008

Davis, F. D. (1993). User acceptance of information technology: System characteristics, user perceptions and behavioral impacts. *International Journal of Man-Machine Studies, 38(3), 475–487. doi:10.1006/imms.1993.1022*

De Haes, S., & Van Grembergen, W. (2013). Improving enterprise governance of IT in a major airline: A teaching case. *Journal of Information Technology Teaching Cases*, *3*(2), 60–69. doi:10.1057/jittc.2013.7

Dhillon, G. (2012). *Information-security management: Global challenges in the new millennium*. Hershey, PN: IGI Global.

Dixon, P. (2006). Medical identity theft: The information crime than can kill you. *The World Privacy Forum*, 13-22. Retrieved from http://www.worldprivacyforum.org/wp-content/uploads/2007/11/wpf_medicalidtheft2006.pdf

Daft, R. L. (2013). *Organization theory and design*. Mason, OH: South-Western Cengage

Erdfelder, E., Faul, F., & Buchner, A. (1996). GPOWER: A general power analysis program. *Behavior Research Methods, Instruments, and Computers, 28*, 1-11. doi:10.3758/bf03203630

Explanation of benefits. (n.d.) Medical Dictionary for the Dental Professions. (2012). Retrieved from

http://medicaldictionary.thefreedictionary.com/explanation+of+benefits

Fakhri, B., Fahimah, N., & Ibrahim, J. (2015). Information security aligned to enterprise management. *Middle East Journal of Business*, *10*(1), 62–66. Retrieved from http://www.mejb.com/upgrade_flash/Jan2015/Infosecurity.pdf

Fan, L., Xue, Q., & Wu, W. (2015). A new authentication method for the valuables logistics personnel. In *2015 International Conference on Automation, Mechanical Control and Computational Engineering*. Atlantis Press. Retrieved from http://www.atlantis-press.com/php/download_paper.php?id=20091

Federal Bureau of Investigation. (2014). *Health care systems and medical devices at risk for increased cyber intrusions* (FBI Cyber Division Bulletin). Retrieved from https://publicintelligence.net/fbi-health-care-cyber-intrusions/

Federal Trade Commission. (2007). *Federal trade commission - 2006 identity theft survey report*. Retrieved from Federal Trade Commission website http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf

Federal Trade Commission. (2012, August). *Medical identity theft*. Retrieved from http://www.consumer.ftc.gov/articles/0171-medical-identity-theft

Fox, C. R., Erner, C., & Walters, D. J. (2015). Field to the laboratory and back. *The Wiley Blackwell Handbook of Judgment and Decision Making, 2 Volume Set*, 43.

Freeman, I., & Hasnaoui, A. (2011). The meaning of corporate social responsibility: The vision of four nations. *Journal of Business Ethics, 100*(3), 419-443. doi:10.1007/s10551-010-0688-6

Galicki, A., Havens, D., & Pelker, A. (2014). Computer crimes. *American Criminal Law*

Review, 51, 875. Retrieved from http://www.lexisnexis.com.ezp.waldenulibrary.org/hottopics/lnacademic/?shr=t&csi=168966&sr=%20AUTHOR%28Galicki%29+AND+DATE+IS+2014

Galliers, R. D., & Leidner, D. E. (Eds.). (2014). *Strategic Information Management: Challenges and Strategies in Managing Information Systems* (4th ed.). New York: Routledge.

Gartner. (2015, October 02). *Gartner Worldwide IT Spending Forecast*. Retrieved from http://www.gartner.com/doc/3142129

Gavetti, G., Greve, H. R., Levinthal, D. A., & Ocasio, W. (2012). The behavioral theory of the firm: Assessment and prospects. *Academy of Management Annals*, *6*(1), 1– 40. doi:10.1080/19416520.2012.656841

Gefen, D., Karahanna, E., & Straub, D. (2003). Trust and TAM in online shopping: an integrated model. *MIS Quarterly, 17*(1), 51–90. Retrieved from https://misq.org/trust-in-tam-in-online-shopping-an-integrated-model.html

Green, S. B., & Salkind, N. J. (2016). *Using SPSS for Windows and Macintosh* (8th ed.). Boston: Pearson.

Groves, R. M. (2011). Three eras of survey research. *Public Opinion Quarterly*, *75*(5), 861–871. Retrieved from http://poq.oxfordjournals.org/content/75/5/861.short

Gupta, M. (2015). Biometric another way of user authentication. *International Journal of Emerging Trends in Science and Technology*, *2*(3). Retrieved from http://ijetst.in/ems/index.php/ijetst/article/view/574

Han, W. Y., & Lee, J. C. (2012). Palm vein recognition using adaptive Gabor filter. *Expert Systems with Applications, 39*(18), 13225-13234. doi:10.1016/j.eswa.2012.05.079

Holden, R. J., Brown, R. L., Scanlon, M. C., & Karsh, B.-T. (2012). Modeling nurses' acceptance of bar coded medication administration technology at a pediatric hospital. *Journal of the American Medical Informatics Association, 19*(6), 1050–1058. doi:10.1136/amiajnl-2011-000754

Hsiao, C. H., & Yang, C. (2011). The intellectual development of the technology acceptance model: A co-citation analysis. *International Journal of Information Management, 31(2), 128–136. doi:10.1016/j.ijinfomgt.2010.07.003*

Identity Theft Resource Center. (2015). *ITRC breach statistics 2005-2014*. Retrieved from http://www.idtheftcenter.org/images/breach/MultiYearStatistics.pdf

Identity Theft Resource Center. (2015, April 24). *The rising costs of healthcare data breaches*. Retrieved from http://www.idtheftcenter.org/Data-Breaches/the-rising-costs-of-healthcare-data-breaches.html

James, T., Pirim, T., Boswell, K., Reithel, B., & Barkhi, R. (2006). Determining the intention to use biometric devices: An application and extension of the technology acceptance model. *Journal of Organizational and End User Computing, 18*(3), 1–24. Retrieved from https://www.igi-global.com/article/determining-intention-use-biometric-devices/3812

The Joint Commission. (2015). *2015 National patient safety goals* [PowerPoint]. Available from

http://www.jointcommission.org/standards_information/npsgs.aspx

Judson, T., Haas, M., & Lagu, T. (2014). Medical identity theft: Prevention and reconciliation initiatives at massachusetts general hospital. *Joint Commission Journal on Quality and Patient Safety*, *40*(7). Retrieved from http://www.ingentaconnect.com/content/jcaho/jcjqs/2014/00000040/00000007/art00001

Kang, W., Liu, Y., Wu, Q., & Yue, X. (2014). Contact-free palm-vein recognition based on local invariant features. *PLoS ONE*, *9*(5). doi:10.1371/journal.pone.0097548

Kang, W., & Wu, Q. (2014). Contactless palm vein recognition using a mutual foreground-based local binary pattern. *IEEE Transactions on Information Forensics and Security, 9*(11), 1974-1985. doi:10.1109/tifs.2014.2361020

Kim, H. (2014). Enhanced identity authentication and context privacy preservation in ubiquitous healthcare system. *International Journal of Control and Automation, 7*(11), 391-400. doi:10.14257/ijca.2014.7.11.38

Knapp, K. J., & Ferrante, C. J. (2012). Policy awareness, enforcement and maintenance: Critical to information security effectiveness in organizations. *Journal Of Management Policy and Practice*, *13*(5), 66-80. Retrieved from http://ezp.waldenulibrary.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=85163694&scope=site

Kohn, L. T., Corrigan, J. M., & Donaldson, M. S. (2000). *To err is human: Building a safer health system*. Washington, DC: The National Academies Press.

Kraemer, H. C., & Blasey, C. (2015). *How Many Subjects?: Statistical Power Analysis in*

Research (2nd ed.). Los Angeles: SAGE Publications, Inc.

Lally, L. (2013). Information technology and crisis compliance: Implications for studying hurricane sandy. *2013 Northeast Decision Sciences Institute Annual Meeting Proceedings*. Retrieved from http://www.nedsi.org/proc/2013/proc/p121105003.pdf

Lau, A., Yen, J., & Chau, P.Y.K. (2001). Adoption of on-line trading in the hong kong financial market. *Journal of Electronic Commerce Research, 2*(2), 58–65. Retrieved from http://www.jecr.org/node/299

Lee, J. C. (2012). A novel biometric system based on palm vein image. *Pattern Recognition Letters, 33*(12), 1520-1528. doi:10.1016/j.patrec.2012.04.007

Leedy, P. D., & Ormrod, J. E. (2015). *Practical research: Planning and design* (11th ed.). Upper Saddle River, NJ: Pearson Merrill Prentice Hall.

Liu, Z., & Song, S. (2012). An embedded real-time finger-vein recognition system for mobile devices. *IEEE Transactions on Consumer Electronics*, *58*(2), 522–527. doi:10.1109/TCE.2012.6227456

Liu, G., Zhang, J., & Chen, G. (2014). An approach to finding the cost-effective immunization targets for information assurance. *Decision Support Systems*, *67*, 40–52. Retrieved from http://ac.els-cdn.com.ezp.waldenulibrary.org/S0167923614002061/1-s2.0-S0167923614002061-main.pdf?_tid=fb2a5286-4d04-11e5-882d-00000aab0f6c&acdnat=1440712129_60af2fc27196b9ace2fb4da74c13d0a7

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement

and validation procedures in MIS and behavioral research: Integrating new and existing techniques. *MIS Quarterly*, *35*(2), 293–334. Retrieved from http://dl.acm.org/citation.cfm?id=2017510

Maes, K., De Haes, S., & Van Grembergen, W. (2015). Exploring the business case process for IT enabled investments. *International Journal of IT/Business Alignment and Governance*, *6*(2), 14–30. doi:10.4018/IJITBAG.2015070102

Mancilla, D., & Moczygemba, J. (2009). Exploring medical identity theft. *Perspectives in Health Information Management*, 1-11. Retrieved from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2804460/pdf/phim0006-0001e.pdf

Manocha, M., & Kaur, P. (2013). Palm vein recognition for human identification using NN. *International Journal of Innovative Technology and Exploring Engineering, 3*(7), 140-143. Retrieved from http://www.ijitee.org/attachments/File/v3i7/G1411123713.pdf

Mathieu, J. E., Aguinis, H., Culpepper, S. A., & Chen, G. (2012). Understanding and estimating the power to detect cross-level interaction effects in multilevel modeling. *Journal of Applied Psychology*, *97*(5), 951–966. doi:10.1037/a0028380

Mathieu, J. E., & Chen, G. (2011). The etiology of the multilevel paradigm in management research. *Journal of Management*, *37*(2), 610–641. doi:10.1177/0149206310364663

MacCallum, R.C., Widaman, K.F., Zhang, S. and Hong, S. (1999). Sample size in factor analysis. *Psychological Methods, 4*(1), 84–99. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.536.6317&rep=rep1&t

ype=pdf

McKesson Corporation. (2014). *PatientSecure: Biometric patient identification system*. Retrieved from http://www.mckesson.com/providers/health-systems/department-solutions/access-management/patientsecure

McMillan, J. H., & Schumacher, S. (2014). *Research in education: Evidence-based inquiry*. Boston: Pearson Higher Ed.

McPeake, J., Bateson, M., & O'Neill, A. (2014). Electronic surveys: How to maximise success. *Nurse Researcher*, *21*(3), 24–26. doi:10.7748/nr2014.01.21.3.24.e1205

Michael, G. K. O., Connie, T., & Teoh, A. B. J. (2012). A contactless biometric system using multiple hand features. *Journal of Visual Communication and Image Representation, 23*(7), 1068-1084. doi:10.1016/j.jvcir.2012.07.004

Mills, G. E., & Gay, L. R. (2015). *Educational research: Competencies for analysis and applications*. Upper Saddle River, NJ: Pearson.

Mirmohamadsadeghi, L., & Drygajlo, A. (2014). Palm vein recognition with local texture patterns. *IET Biometrics*, 1–9. doi:10.1049/iet-bmt.2013.0041

Moores, T. T. (2012). Towards an integrated model of IT acceptance in healthcare. *Decision Support Systems*, *53*(3), 507–516. doi:10.1016/j.dss.2012.04.014

Mukhopadhyay, S., & Gupta, R. K. (2014). Survey of qualitative research methodology in strategy research and implication for Indian researchers. *Vision: The Journal of Business Perspective, 18*(2), 109-123. doi:10.1177/0972262914528437

Nirmal, T. M., & Francis, M. (2014). Palm vein authentication. *International Journal of Advanced Research in Computer Science and Software Engineering, 4*(6), 41-44.

Retrieved from http://www.ijarcsse.com/docs/papers/Volume_4/6_June2014/V4I6-0114.pdf

Noh, Z. M., Ramli, A. R., Hanafi, M., & Saripan, M. I. (2015). Acquiring palm vein patterns for visual interpretation. In *2015 2nd International Conference on Biomedical Engineering (ICoBE)* (pp. 1–5). doi:10.1109/ICoBE.2015.7235884

Norman, I. D., Aikins, M. K., & Binka, F. N. (2011). Ethics and electronic health information technology: Challenges for evidence-based medicine and the physician-patient relationship. *Ghana Medical Journal*, *45*(3), 115–124. Retrieved from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3266146/

Okoh, E., & Awad, A. I. (2015). Biometrics applications in e-health security: A preliminary survey. In *Health Information Science*, 92–103. Springer. Retrieved from http://link.springer.com/Chapter/10.1007/978-3-319-19156-0_10

Olanrewaju, R. F., Yahuza, M., & Ali, N. B. (2014). Investigation of medical identity theft in healthcare sector: Its statistics, effects and way out. In *Proceedings of the 4th International Cryptology and Information Security Conference, Kuala Lumpur*, 217–228. Retrieved from http://irep.iium.edu.my/38930/

Ollove, M. (2014, February 07). The rise of medical identity theft in healthcare. *MedCity News*. Retrieved from http://medcitynews.com/2014/02/rise-medical-identity-theft-healthcare/

Pai, F.-Y., & Huang, K.-I. (2011). Applying the technology acceptance model to the introduction of healthcare information systems. *Technological Forecasting and Social Change*, *78*(4), 650–660. doi:10.1016/j.techfore.2010.11.007

Peltier, T. R. (2013). *Information Security Fundamentals* (2nd ed.). Boca Raton, Florida: Auerbach Publications.

Pettypiece, S. (2015, May 7). Rising cyber attacks costing health system $6 billion annually. *The Bloomberg Business*. Retrieved from http://www.bloomberg.com/news/articles/2015-05-07/rising-cyber-attacks-costing-health-system-6-billion-annually

Pezzulo, G., Verschure, P. F. M. J., Balkenius, C., & Pennartz, C. M. A. (2014). The principles of goal-directed decision-making: From neural mechanisms to computation and robotics. *Philosophical Transactions of the Royal Society of London B: Biological Sciences*, *369*(1655). doi:10.1098/rstb.2013.0470

Ponemon Institute. (2012). *2012 The impact of cybercrime on business* (Ponemon Institute Research Report). Retrieved from http://www.ponemon.org/local/upload/file/Impact_of_Cybercrime_on_Business_FINAL.pdf

Ponemon Institute. (2013). *2013 Survey on Medical Identity Theft* (Ponemon Institute Research Report). Retrieved from http://clearwatercompliance.com/wp-content/uploads/2013/10/2013-Medical-Identity-Theft-Report-FINAL.pdf

Ponemon Institute. (2015). *Fifth Annual Study on Medical Identity Theft* (Ponemon Institute Research Report). Retrieved from http://medidfraud.org/2014-fifth-annual-study-on-medical-identity-theft/

Ponemon Institute. (2015). *Fifth Annual Study on Privacy and Security of Healthcare Data* (Ponemon Institute Research Report). Retrieved from

http://lpa.idexpertscorp.com/acton/ct/6200/s-06d1-1505/Bct/l-7ca6/l-7ca6:e29/ct7_0/1?sid=NOVBjLkgb

Quigley, M. (2011). *ICT Ethics and Security in the 21st Century: New Developments and Applications* (1st ed.). Hershey, PA: IGI Global.

Ragowsky, A., Licker, P., Miller, J., Gefen, D., & Stern, M. (2014). Do not call me chief information officer, but chief integration officer: A summary of the 2011 detroit CIO roundtable. *Communications of the Association for Information Systems*, *34*(1), 1333–1346. Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=3792&context=cais

Ratha, N. K., Connell, J. H., & Pankanti, S. (2015). Big data approach to biometric-based identity analytics. *IBM Journal of Research and Development*, *59*(2/3), 4:1–4:11. doi:10.1147/JRD.2015.2394514

Rea, L. M., & Parker, R. A. (2014). *Designing and conducting survey research: A comprehensive guide* (4th ed.). San Francisco, CA: John Wiley and Sons, Inc.

Riley Jr, R. A., & Franke Kleist, V. (2005). The biometric technologies business case: A systematic approach. *Information Management and Computer Security*, *13*(2), 89–105. doi:10.1108/09685220510589280

Roberts, N., & Grover, V. (2012). Leveraging information technology infrastructure to facilitate a firm's customer agility and competitive activity: An empirical investigation. *Journal of Management Information Systems*, *28*(4), 231–270. doi:10.2753/MIS0742-1222280409

Rua, E. A., Maiorana, E., Castro, J. L. A., & Campisi, P. (2012). Biometric template

protection using universal background models: An application to online signature. *IEEE Transactions on Information Forensics and security*, *7*(1), 269–282. doi:10.1109/TIFS.2011.2168213

San Martín, H., & Herrero, Á. (2012). Influence of the user's psychological factors on the online purchase intention in rural tourism: Integrating innovativeness to the UTAUT framework. *Tourism Management*, *33*(2), 341–350. doi:10.1016/j.tourman.2011.04.003

Sarkar, A. (2014). *Cybercrime: A Seminar Report*. Retrieved from http://www.slideshare.net/ArindamSarkar9/cybercrime-a?utm_source=slideshow02&utm_medium=ssemail&utm_campaign=share_slideshow

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2015). Research methods for business students, 7th ed. (7 edition). New York: Trans-Atlantic Publications, Inc.

Sayed, M., & Jradi, F. (2014). Biometrics: Effectiveness and applications within the blended learning environment. *Computer Engineering and Intelligent Systems*, *5*(5), 1–8. Retrieved from http://iiste.org/Journals/index.php/CEIS/article/download/12806/13126

Sayed, M. (2015). Palm vein authentication based on the coset decomposition method. *Journal of Information security*, *6*(3), 197–205. doi:10.4236/jis.2015.63020

Schepers, J., & Wetzels, M. (2007). A meta-analysis of the technology acceptance model: Investigating subjective norm and moderation effects. *Information and Management*, *44*(1), 90–103. doi:10.1016/j.im.2006.10.007

Siegel, S., & Castellan, N. J., Jr. (1988). *Nonparametric statistics for the behavioral sciences* (2nd ed.). Boston, MA: McGraw Hill.

Straits, B. C., & Singleton, R. (2017). *Approaches to social research* (6th ed.). Oxford University Press.

Sternberg, R. J. (2012). Intelligence. *Dialogues in Clinical Neuroscience*, *14*(1), 19–27. Retrieved from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3341646/

Taitsman, J. K., Grimm, C. M., & Agrawal, S. (2013). Protecting patient privacy and data security. *New England Journal of Medicine*, *368*(11), 977–979. doi:10.1056/nejmp1215258

Tang, D., Yang, J.-B., Bamford, D., Xu, D.-L., Waugh, M., Bamford, J., & Zhang, S. (2012). The evidential reasoning approach for risk management in large enterprises. *International Journal of Uncertainty, Fuzziness, and Knowledge-Based Systems*, *20*(Supp 1), 17–30. doi:10.1142/S0218488512400028

Tome, P., & Marcel, S. (2015, May). *On the vulnerability of palm vein recognition to spoofing attacks*. Paper presented at the 8th IAPR International Conference on Biometrics, Phuket, Thailand. Retrieved from http://infoscience.epfl.ch/record/206815/files/Tome_ICB2015-SpoofingPalmvein.pdf

Trochim, W., Donnelly, J. P., & Arora, K. (2015). *Research methods: The essential knowledge base* (2nd ed.). Boston: Wadsworth Publishing.

Tyson, D. (2017). *Security convergence: Managing enterprise security risk*. Boston: Butterworth-Heinemann.

Department of Health and Human Services, Office for Civil Rights [HHS]. (2015). *Privacy, security, and electronic health records*. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/privacy-security-electronic-records.pdf

University of Southampton. (n.d.). *Defining scope of research*. Retrieved from http://www.erm.ecs.soton.ac.uk/theme8/defining_scope_of_research.html

Uttam, P. R., Haridas, S. R., Durvas, S. Y., & Arun, A. A. (2014). Palm vein authentication. *International Journal of Engineering Development and Research*, *2*(1), 683–687. Retrieved from http://www.ijedr.org/viewfulltext.php?&p_id=IJEDR1401124

Uzoka, F.-M. E., & Ndzinge, T. (2009). Empirical analysis of biometric technology adoption and acceptance in Botswana. *Journal of Systems and Software*, *82*(9), 1550–1564. Retrieved from http://www.sciencedirect.com/science/article/pii/S016412120900106X

Vaid, S., & Mishra, D. (2015). Comparative analysis of palm-vein recognition system using basic transforms. In *2015 IEEE International Advance Computing Conference (IACC)*, 1105–1110. doi:10.1109/iadcc.2015.7154875

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425–478. Retrieved from http://www.jstor.org/stable/30036540

Verma, D., & Dubey, S. (2015). Processing and enhancement of palm vein image in vein pattern recognition system. *International Journal of Computer Science and*

Mobile Computing, *4*(4), 137–141. Retrieved from http://ijcsmc.com/docs/papers/April2015/V4I4201502.pdf

Vij, S., & Farooq, R. (2014). Knowledge sharing orientation and its relationship with business performance: A structural equation modeling approach. *IUP Journal of Knowledge Management*, *12*(3), 17–41. Retrieved from http://ezp.waldenulibrary.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=98188203&scope=site

Vogt, W. P., & Johnson, R. B. (2011). *Dictionary of statistics and methodology: A nontechnical guide for the social sciences* (4th edition). Thousand Oaks, CA: Sage.

Volner, R., & Boreš, P. (2015). Biometric Techniques in Identity Management Systems. *Elektronika Ir Elektrotechnika*, *95*(7), 55–58. Retrieved from http://www.sace.ktu.lt/index.php/elt/article/view/10045

Walters, W., & Betz, A. (2012). Medical identity theft. *Journal of Consumer Education*, 75–79. Retrieved from http://thekeep.eiu.edu/fcs_fac/16

Warkentin, M. (2006). *Enterprise information systems assurance and system security: Managerial and technical issues*. Hershey, PN: Idea Group.

Watanabe, M. (2008). Palm vein authentication. In N. K. Ratha & V. Govindaraju (Eds.), *Advances in biometrics* (pp. 75-88). London: Springer.

Whitney, E. (2014). *Are your medical records vulnerable to theft?* Retrieved from Kaiser Health News website http://khn.org/news/are-your-medical-records-vulnerable-to-theft/

Williams, K. C. (2012). Fear appeal theory. *Research in Business and Economics Journal*, *5*(1), 1–21. Retrieved from http://m.www.aabri.com/manuscripts/11907.pdf

Wiseman, R. M., Cuevas-Rodríguez, G., & Gomez-Mejia, L. R. (2012). Towards a social theory of agency. *Journal of Management Studies*, *49*(1), 202–222. doi:10.1111/j.1467-6486.2011.01016.x

Wu, K.-S., Lee, J.-C., Lo, T.-M., Chang, K.-C., & Chang, C.-P. (2013). A secure palm vein recognition system. *Journal of Systems and Software*, *86*(11), 2870–2876. doi:10.1016/j.jss.2013.06.065

Wu, W., Lu, F., Cheng, G., & Shi, C. (2012, November). A vein based biometric experiment and some new developments. In *2012 Third Global Congress on Intelligent Systems,* 131-135. doi:10.1109/gcis.2012.74

Wu, W., Lu, F., Cheng, G., & Shi, C. (2012). A vein based biometric experiment and some new developments. *2012 Third Global Congress on Intelligent Systems*. doi:10.1109/gcis.2012.74

Yan, X., Kang, W., Deng, F., & Wu, Q. (2015). Palm vein recognition based on multi-sampling and feature-level fusion. *Neurocomputing*, *151*(2), 798–807. doi:10.1016/j.neucom.2014.10.019

Yang, J., & Shi, Y. (2012). Finger-vein ROI localization and vein ridge enhancement. *Pattern Recognition Letters, 33*(12), 1569-1579. doi:10.1016/j.patrec.2012.04.018

Appendix A: Palm Vein Authentication Survey Instrument

Introduction to the Participant

The purpose of the study is to understand the effectiveness of palm vein authentication technology as perceived by healthcare managers and doctors. Healthcare managers and doctors have not frequently been research participants in palm vein authentication studies. As medical fraud increases, it will become more critical to explore mitigating strategies to minimize risk to the organization and to the patient.

Despite the increasing number of medical identity theft victims, individuals lack awareness of the seriousness of the crime. On average, victims learn about the theft of their credentials more than three months following the crime. Moreover, 30% do not know when they became a victim. In addition, 54% of medical identity theft victims who discovered an error in their Explanation of Benefits did not know to whom to report the claim. Also, victims report losing trust and confidence in their health care provider.

Palm vein authentication is one of the vascular pattern authentication technologies. Vascular pattern authentication includes vein pattern recognition using the vein patterns of the palm, back of the hand, or fingers as personal identification data, and retina recognition using the vascular patterns at the back of the eye as personal identification.

Medical Identity Theft, Palm Vein Authentication
The Manager's Perspective

Participant Demographics

Instructions

Please select the best appropriate answer for each of the questions below:

* 1. Which category best describes your type of organization?

- ◯ Hospital
- ◯ Private Practice
- ◯ Non Profit

* 2. Indicate the extent of your experience using a palm vein authentication system.

- ◯ 1-No experience whatsoever
- ◯ 2-Done something very similar
- ◯ 3-Something done before

* 3. Indicate your willingness to use a palm vein authentication system.

- ◯ 1-Not willing at all
- ◯ 2
- ◯ 3-Moderately willing
- ◯ 4
- ◯ 5-Very willing

Medical Identity Theft, Palm Vein Authentication
The Manager's Perspective

Factors Affecting Acceptance and Adoption of Palm Vein Authentication

Instructions

Please examine each statement and select the response that best indicates your degree of agreement. Your responses will be aggregated and will serve as a basis for determining the extent of acceptance and adoption of a palm vein authentication system in the healthcare sector.

* 4. It enhances job performance.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 5. It removes the need to remember passwords and pins.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 6. Using palm vein authentication will effectively and efficiently identify patients and users in the organization.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 7. Palm vein authentication system is easy to use.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 8. Delay and mismatch always occur.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

Medical Identity Theft, Palm Vein Authentication
The Manager's Perspective

Factors Affecting Acceptance and Adoption of Palm Vein Authentication

* 9. Palm vein authentication systems are convenient to use.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 10. When using the system, I feel nervous.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 11. It does not involve a lot of process.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 12. I have knowledge on how to use palm vein authentication system.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 13. Palm vein authentication systems are being used by most organizations in health care.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

Medical Identity Theft, Palm Vein Authentication
The Manager's Perspective

Factors Affecting Acceptance and Adoption of Palm Vein Authentication

* 14. It is better than the other traditional methods.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 15. Palm vein authentications are accepted by people around.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 16. I use it because people around me use it.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 17. Palm vein authentication implementation does not require managers to change their management philosophy.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 18. Management is interested in new technology to reduce fraud.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

Medical Identity Theft, Palm Vein Authentication
The Manager's Perspective

Factors Affecting Acceptance and Adoption of Palm Vein Authentication

* 19. Management support the use of palm vein authentication.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 20. The issue of power has not been a hindrance to palm vein authentication usage.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 21. Palm vein authentication system is cost-effective for the organization.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 22. I have the technical knowhow about palm vein authentication systems.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 23. Palm vein authentication identification process is fast.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

Medical Identity Theft, Palm Vein Authentication
The Manager's Perspective

Factors Affecting Acceptance and Adoption of Palm Vein Authentication

* 24. Palm vein authentication system management process is simple and easy.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 25. I can use the system without assistance.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 26. It takes a lot of my time during usage.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 27. I am comfortable with palm vein authentication technology.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 28. Using this system intimidates me.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

Medical Identity Theft, Palm Vein Authentication
The Manager's Perspective

Factors Affecting Acceptance and Adoption of Palm Vein Authentication

* 29. Palm vein authentication system is trustworthy.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 30. Palm vein authentication can prevent unauthorized access to restricted information.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 31. It is more secure and reliable than traditional forms of security/identification.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 32. Palm vein authentication eliminates the unreliability associated with pins and passwords.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 33. It upholds the integrity of the information.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

Medical Identity Theft, Palm Vein Authentication
The Manager's Perspective

Factors Affecting Acceptance and Adoption of Palm Vein Authentication

* 34. The system can be used alongside the traditional systems.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 35. It is a good match for the system that is currently used in my organization.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 36. Users will easily adapt to palm vein authentication systems.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 37. It is easier to use than the traditional system.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 38. Extra documents for identification are not needed.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

Medical Identity Theft, Palm Vein Authentication
The Manager's Perspective

Factors Affecting Acceptance and Adoption of Palm Vein Authentication

* 39. It eliminates time spent on identifying patients.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 40. Palm vein authentication relieves me from remembering patient names.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 41. Palm vein authentication prevents unauthorized access to restricted information.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 42. Abuse of palm vein authentication information is unlikely.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 43. It is difficult to handle the system.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

Medical Identity Theft, Palm Vein Authentication
The Manager's Perspective

Factors Affecting Acceptance and Adoption of Palm Vein Authentication

* 44. Only people with technical knowhow can operate it.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 45. There is always a problem while using the system.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 46. The use of palm vein authentication systems will help improve the state of information security in healthcare.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 47. My organization has the resources to run and maintain palm vein authentication systems.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

* 48. The cost of implementing and maintaining palm vein authentication is high.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
○	○	○	○	○

Medical Identity Theft, Palm Vein Authentication
The Manager's Perspective

Factors Affecting Acceptance and Adoption of Palm Vein Authentication

* 49. It is too intrusive.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
◯	◯	◯	◯	◯

* 50. Palm vein authentication is the next best thing in security.

Strongly Agree	Agree	Not Sure	Disagree	Strongly Disagree
◯	◯	◯	◯	◯

Appendix B: Email Invitation to Potential Participants

Subject: Request to Complete Doctoral Study Survey

Good day to you,

My name is Cruz Cerda III. I am a doctoral student at the School of Management at Walden University with a Bachelor's degree in economics from Harvard University and a Master's degree in education from New York University. I am conducting research on the effectiveness of palm vein authentication technology as perceived by healthcare managers and doctors. Healthcare managers and doctors have not frequently been research participants in palm vein authentication studies. As medical fraud increases, it will become more critical to explore mitigating strategies to minimize risk to the organization and to the patient. I would like to gain your perspective on how you view palm vein authentication technology as a tool to manage medical fraud. If you are either a healthcare manager or doctor, are 18 years or older, and perform work for the organization on a full time basis or a part time basis, you are a candidate for participation in this research. The goal of this research is to develop an understanding of the perspectives of healthcare managers and doctors across the United States with regard to palm vein authentication systems and medical identity theft.

I am studying the manager's perspective with regard to the effectiveness of palm vein authentication technology as a means to manage medical identity theft, which includes researching how different variables relate to the adoption of technology. If you decide to participate, you will be asked to acknowledge a consent form, answer eight

demographic questions, and then rank a response via a 5-point Likert scale to 47 survey questions.

Participation is confidential and no personally identifiable information will be asked on the survey.

Taking part in the study is your discretion. You may choose to quit at any time prior to submission if you prefer not to complete. There are no ramifications for not completing the survey. If you have any questions regarding the survey, you may contact me at cruz.cerda@waldenu.edu. Your participation may help leaders realize the benefit of palm vein authentication technology as a means to manage medical fraud.

Thank you for your consideration. If you would like to participate, please begin by navigating to the following link: [Link inserted]. Please complete prior to [Due date inserted].

Thank you,

Cruz Cerda III cruz.cerda@waldenu.edu