8-26-2025

Exploring Cybersecurity Strategies Used to Protect Personal Health Information From Cyberattacks When Using Telemedicine

Samara Torres
Walden University

Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Samara Torres

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. Constance Blanson, Committee Chairperson, Information Technology Faculty
Dr. Jon McKeeby, Committee Member, Information Technology Faculty

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

Walden University
2025

Abstract

Exploring Cybersecurity Strategies Used to Protect Personal Health Information

From Cyberattacks When Using Telemedicine

by

Samara Torres

MS, Walden University, 2018

MA, Webster University, 2006

BBA, Colegio Universitario del Este, 1994

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

August 2025

Abstract

The healthcare industry has been impacted by an increase in cybersecurity breaches because of cyberattacks when using telemedicine. It is crucial that information technology (IT) managers in the private healthcare industry protect personal health information (PHI) to uphold patients' right to privacy, maintain their trust, prevent legal ramifications, and to comply with government regulations. This qualitative pragmatic research used the integrated system theory (IST) as a road map to explore effective cybersecurity strategies used to protect PHI in telemedicine. The participants were seven IT managers in the private healthcare industry within the United States who had experience with cybersecurity strategies implementation to protect PHI from cyberattacks when using telemedicine. Data were collected using semistructured face-to-face online/virtual interviews, voice recordings and researcher notes, and publicly available online documents. The analysis focused on five major themes: (a) protection from unauthorized disclosure, (b) risk management, (c) cybersecurity awareness and education, (d) privacy, and (e) data-loss prevention. Some recommendations for IT managers are to implement an integrated data protection strategy that includes security mechanisms, such as encryption and access control, while keeping a balance between confidentiality, integrity, and availability, as well as to ensure that personnel receive cyber awareness training and education to recognize threats. The implications for positive social change rest on the potential for IT managers to enhance cybersecurity measures to reduce PHI data exposure in telemedicine, thus improving healthcare outcomes for individuals and potentially increasing individuals' quality of life.

Exploring Cybersecurity Strategies Used to Protect Personal Health Information

From Cyberattacks When Using Telemedicine

by

Samara Torres

MS, Walden University, 2018

MA, Webster University, 2006

BBA, Colegio Universitario del Este, 1994

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

August 2025

Dedication

I would like to dedicate this study first to my heavenly father who guided me and was (still is) with me every step of the way. Thank you. To my late parents, Jose and Gloria, who always believed in me; to my family Jose, Lourdes, Francis, Meilyn, and my nephews and niece who lifted me when I fell. Some relatives and friends who motivated me to pursue my goals, my aunt Lourdes, Miguel and Gisela, Cathy, Marty, and to those who are no longer with me, Aida, Evelyn, and Adalberto, I will always carry your words of encouragement with me. Last, but not least, I would like to thank my church family for supporting me with their prayers. Thank you, Betel, Calvary, and Generation.

Acknowledgments

First, I would like to thank God, for allowing me to reach the summit of this journey, overcoming major efforts and challenges. To my committee, Dr. Constance Blanson, who say this accomplishment would not have been possible without the guidance and encouragement, I am blessed to have her as my chair. I would like to acknowledge our Dean Dr. Miles, thank you for your support, and Dr. McKeeby, thank you for your guidance. Also, other faculty members who in one way or another inspired me to continue this DIT, Dr. Barilovits, for example. And Dr. Case for challenging us to do better and improve as scholars. The rest of Walden's teams, academic advising, and the military office team, thank you.

Table of Contents

List of Tables iv

List of Figures v

Section 1: Foundation of the Study 1

Background of the Problem 1

Problem Statement 2

Purpose Statement 2

Nature of Study 3

Research Question 4

Interview Questions 5

Conceptual Framework 6

Definition of Terms 7

Assumptions, Limitations, and Delimitations 8

Assumptions 8

Limitations 9

Delimitations 9

Significance of Study 9

Contribution to Information Technology Practice 9

Implications for Social Change 10

A Review of Professional and Academic Literature 10

Application to the Applied IT Problem 12

Conceptual Framework: Integrated System Theory 13

Analysis of Contrasting Theories.. 29

Analysis of Potential Themes 31

Relationship of the Study to Previous Research 39

Transition and Summary..40

Section 2: The Project...42

Purpose Statement...42

Role of the Researcher..42

Participants...44

Research Method and Design 46

Research Method 46

Research Design.. 50

Population and Sampling 52

Ethical Research...57

Data Collection 59

Instruments.. 59

Data Collection Techniques 61

Data Organization Techniques.. 64

Data Analysis Technique 65

Reliability and Validity...67

Dependability.. 67

Credibility 68

Transferability.. 68

Confirmability ... 69

Data Saturation ... 69

Transition and Summary ... 70

Section 3: Application to Professional Practice and Implications for Change ... 71

Introduction ... 71

Presentation of Findings ... 72

Theme 1: Risk Management ... 73

Theme 2: Protection From Unauthorized Disclosure ... 75

Theme 3: Cybersecurity Awareness and Education ... 78

Theme 4: Privacy ... 81

Theme 5: Data-Loss Prevention ... 83

Application to Professional Practice ... 84

Implications for Social Change ... 86

Recommendations for Action ... 87

Recommendations for Further Research ... 88

Reflections ... 89

Conclusion ... 90

References ... 91

Appendix A: Interview Questions ... 130

Appendix B: Interview Protocol ... 131

List of Tables

Table 1. Publicly Available Documents 72

Table 2. Main Themes 73

List of Figures

Figure 1. Integrated System Theory Conceptual Framework 20

Section 1: Foundation of the Study

Background of the Problem

Telemedicine technology offers a great advantage in communication, especially since the development of smart technology, such as smartphones, tablets, wireless monitoring, face-to-face (video) calls, and messaging, including capabilities of utilizing many applications (apps) simultaneously. In the past decade, the proliferation of this technology has made possible its use to provide healthcare services at a distance; this concept is known as *telemedicine* (Chellaiyan et al., 2019). A consumer-driven adoption of telemedicine technology is positively impacting society with lower cost patient care service by having access to healthcare from a remote location (Haleem et al., 2021).

Telemedicine's benefits go beyond the medical realm; it brings socioeconomic benefits and health education growth, increases healthcare quality, and, more importantly, leads to a better quality of life (Salsabilla et al., 2021). Although society benefits from the use of telemedicine, there are still concerns about protecting personal health information (PHI) and meeting security challenges encountered with the Health Insurance Portability and Accountability Act (HIPAA; Wasserman & Wasserman, 2022). The extensive use of this technology might increase the exposure of PHI used in telemedicine (Sethuraman et al., 2020). Nevertheless, it is important to explore and learn from those who have embraced this technology, along with all the benefits telemedicine brings to communities, societies, and countries.

Problem Statement

Cybersecurity gaps in the protection of PHI are affecting patient care and the safe implementation of telemedicine in the healthcare industry (Bhuyan et al., 2020). The U.S. Department of Health and Human Services in the 2019 Civil Rights Breach Report indicated that healthcare records exposure had increased by 82% from the previous year (Chua, 2021). The general information technology (IT) problem is that some IT managers in the healthcare industry lack cybersecurity strategies to protect their customers' PHI. The specific IT problem is that some IT managers in the healthcare industry lack cybersecurity strategies to protect their customers' PHI from cyberattacks when using telemedicine.

Purpose Statement

The purpose of this qualitative pragmatic research was to explore successful strategies that some IT managers in the healthcare industry use to protect their customers' PHI from cyberattacks when using telemedicine. The target population consisted of seven IT managers in the private healthcare industry within the United States who had experience with cybersecurity strategies implementation to protect PHI from cyberattacks when using telemedicine. The implication for positive social change rests on the potential to reduce PHI data exposure in telemedicine from cyberattacks, inadvertently accessed, shared, sent, and/or received. The reduction of data exposure, therefore, improves healthcare at a distance and has the potential to increase individuals' quality of life that otherwise would be at risk by the lack of cybersecurity on PHI used for patient care.

Nature of Study

For this research, qualitative, quantitative, and mixed-methods methodologies were considered. The qualitative method was selected and was deemed appropriate for this study based on the need to obtain insight into participants' experiences on the subject being studied. Ngenye and Kreps (2020) affirmed that through the qualitative method participants could express their ideas and share their lived experiences. Therefore, the qualitative methodology was selected because it allowed me to explore and learn from the participants' experiences. Bloomfield and Fisher (2019) explained that the quantitative methodology uses statistical data to evaluate a hypothesis. It cannot provide an in-depth description to explore an issue; the qualitative methodology can deliver those life experiences. The quantitative methodology was not selected because quantitative methods focus on empirical data and do not allow participants to share their experiences. Mixed-methods methodology integrates elements of qualitative and quantitative research approaches (Akerblad et al., 2021). Consequently, the mixed-methods approach was not selected because I was not using the quantitative research approach. Therefore, the qualitative research methodology was the most appropriate for this study.

For the research design, case study, narrative, phenomenology, ethnography, and pragmatic inquiry were considered. Pragmatic inquiry design was chosen because it was deemed to be the most appropriate research design that could be used to gain direct access to IT managers, their real-world experiences and explore the issue being studied. According to Kelly and Cordeiro (2020), pragmatic research design focuses on the participants' practical experiences, which yields deep insights on the topic studied.

Furthermore, Ramanadhan et al. (2021) assured that pragmatic inquiry is an efficient and excellent approach and could be used to answer the *whys* and *hows* of an issue and can be tailored to explore a research question. Therefore, pragmatic inquiry was selected because it allowed me to reach IT managers (decision makers) and gain deep insight into the strategies they use to protect their customers' PHI when using telemedicine. Pino Gavidia and Adu (2022) suggested that narrative design is an ontological category that is focused on the lived human condition. The narrative design was not selected because the human condition is not going to be studied. According to Asenahabi (2019), phenomenological design is philosophical. Therefore, the phenomenological design was not selected because this research was not focused on studying a phenomenon. This research focused on gaining insight into cybersecurity strategies used to protect PHI. Polukhina (2022) suggested that ethnography design focuses on the observation of primitive cultures for an extended period, such as anthropology and sociology research. Thus, ethnography design was not selected because the focus of this study was not studying primitive cultures. The ability to tailor the pragmatic inquiry towards the in-depth exploration of the issue being studied and to answer the research question were the reasons that pragmatic inquiry design was chosen.

Research Question

What effective strategies do IT managers in the healthcare industry use to protect their customers' PHI from cyberattacks when using telemedicine?

Interview Questions

1. What types of cyberattacks have you experienced against customers' PHI when using telemedicine?
2. What security policies do you use to protect customers' PHI against cyberattacks when using telemedicine?
3. How does the implementation of those security policies protect customers' PHI against cyberattacks when using telemedicine?
4. What do security policies maintenance do for customers' PHI against cyberattacks when using telemedicine?
5. What strategies do you use to minimize the risk of cyberattacks when using telemedicine?
6. How do you manage those strategies to mitigate the risk of cyberattacks to protect customers' PHI when using telemedicine?
7. How do you measure the performance of the security controls implemented to protect customers' PHI against cyberattacks when using telemedicine?
8. What factors do you consider when auditing the strategies for protecting customers' PHI against cyberattacks when using telemedicine?
9. What strategies do you use to protect customers' PHI against cyberattacks when using telemedicine?
10. How do you respond to cyberattacks against customers’ PHI when using telemedicine?

Conceptual Framework

The conceptual framework used in this study was the integrated system theory (IST) of information security management, developed by Hong et al. in 2003. The IST is based on five theories, *security policy theory, risk management theory, control and audit theory, management system theory,* and *contingency theory* (Sindhuja, 2021). The IST of information security management (ISM) integrates the necessary areas to provide PHI protection used in telemedicine. According to Hong et al., the *security policy theory* addresses establishing, implementing, and maintaining information security policies to meet organizational security requirements. The *risk management theory* indicates that through analysis and evaluation, threats and vulnerabilities can be assessed to minimize the risk. The *control and audit theory* establishes and implements information security control systems and conducts audit procedures to measure control performance. The *management system theory* establishes and maintains an information security management system (ISMS) to regulate and guard information assets. And the *contingency theory* includes strategies to prevent, detect, and respond to threats and vulnerabilities impacting the organization.

Diesch et al. (2020) suggested that implementing an integrating approach makes a strong basis for information security management. The IST of ISM was chosen as the conceptual framework because it aligned with the protection of PHI in telemedicine. An integrated approach is especially necessary for the healthcare industry, where the organization’s mission and business strategies must be taken into consideration because lives depend on it. The IST was used to explore how the private healthcare industry’s strategies were used to protect customers' PHI from cyberattacks and meet government security requirements. Also, it was used to explore how IT managers in the private healthcare industry analyze and evaluate vulnerabilities to minimize risks, perform control over information security, and conduct audits to maintain an appropriate security level. Additionally, I sought to explore how IT managers implement ISMS to protect assets and explore the strategies they implemented to detect and respond to threats impacting the healthcare industry.

Definition of Terms

Cybersecurity: The use of policies, processes, procedures, and/or technology to prevent unauthorized access to systems or information (Ahmed et al., 2022).

IT managers: IT professionals who possess certain education and skills in cybersecurity who have the authority to make changes or impact the outcome of a decision (Shaikh & Siponen, 2023).

Mobile health (mHealth): The practice of using mobile devices such as smartphones and tablets in the practice of medicine and public health (Moreno-Ligero et al., 2023).

Cyberattacks: Malicious activities that deny and/or disable access to information to compromise resources such as systems, data, and personal information, which in turn are used to exploit businesses or individuals, such as phishing attacks (Alabdan, 2020).

Personal health information (*PHI*): Also referred to as *protected health information* under the privacy rule. Refers to information that is stored or transmitted by cover entities (i.e., medical facility) and can be used to identify an individual, regardless of its format (verbal, electronic, or paper), with the exception of education and employment records (National Institute of Standards and Technology [NIST], n.d.).

Southeast Region of the United States: Refers to Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina, and Tennessee (Wage and Hour Division, n.d.).

Telehealth: The use of technology to deliver healthcare, health information, or health education from a distance (Mseke et al., 2023).

Telemedicine: The delivery of health services via remote telecommunications (Cardile et al., 2023).

Assumptions, Limitations, and Delimitations

Assumptions, limitations, and delimitations are necessary activities of a study that affect the research and outcome; those influencing this study are described next.

Assumptions

According to Caster (2020), assumptions are statements believed to be true, normally, and have not been verified, or for a specific purpose such as building a theory, such as circumstances under the statistical techniques that produce valid results. It was assumed that participants understood the importance of this study and responded honestly to the collection of instruments. Also, it was assumed that IT managers shared successful cybersecurity strategies they implemented, thus helping to further validate my study and its societal impact.

Limitations

Limitations are conditions beyond the researcher's control that need to be identified because of the impact they can have on the outcome of a study. Limitations could place restrictions on methodology and conclusions that may potentially affect the research results (Greener, 2018). Data quality becomes a limitation in a qualitative pragmatic inquiry because the researcher has no control over the data collected and their appropriateness (Hayashi et al., 2019). Some of the limitations of this study were the accuracy of data collected and validating the data, which depended on participants' honesty.

Delimitations

Delimitations are the conditions the researcher imposes on a study (Theofanidis & Fountouki, 2019). The delimitations in this study included the target population of IT managers with experience implementing or using cybersecurity strategies to protect PHI from cyberattacks when using telemedicine. Additionally, participating IT managers had to be from the United States and work for the private healthcare industry (not be public industry employees) or work supporting healthcare, which constituted a smaller pool than IT managers from other industries that could provide additional information, such as government industry (federal/local).

Significance of Study

Contribution to Information Technology Practice

In looking for scholarly articles or studies that could provide some insight into cybersecurity strategies used to protect PHI and that have been implemented in the healthcare industry to provide healthcare at a distance, little information was found about the topic. These study findings have the potential to benefit IT practice by filling the gap in the effective implementation of cybersecurity strategies of PHI protection used in telemedicine.

Implications for Social Change

These study findings benefit society by potentially reducing PHI exposure from cyberattacks, increasing telemedicine adoption, and reaching people at remote locations in which healthcare is scarce or nonexistent. Enhancing PHI protection by limiting data access to those with the need to know and preventing data exposure could potentially benefit individuals, patients, the community, the government, and other organizations that directly or indirectly work in the healthcare industry. Moreover, this study affects social change by motivating readers to promote the well-being of society, encouraging self-worth, and increasing health education by learning about the strategies to protect PHI. Another way to impact social change is making myself available to the community and dedicating this study to raise awareness on approaches to secure PHI that others can use as guidance.

A Review of Professional and Academic Literature

This literature review emphasized three main aspects of the study: (a) cybersecurity strategies used to protect PHI in telemedicine, (b) use of the IST as the conceptual framework, and (c) resources to increase cybersecurity strategies implementation, providing a background for and insight into exploring effective cybersecurity strategies IT managers use to protect PHI in telemedicine.

The literature review includes an introduction, a critical analysis and synthesis of the literature, the conceptual framework, and a discussion of the five major themes surrounding data cyberattacks: (a) protection from unauthorized disclosure, (b) risk management, (c) cybersecurity awareness and education, (d) privacy, and (e) data-loss prevention. The literature review revealed the most common themes that impacted PHI in the healthcare industry. Those themes were identified through literature review. The themes were analyzed and synthesized against various sources of information. Furthermore, the themes offer cybersecurity strategies and contextual information on issues encountered throughout the literature review.

The search strategy started with a broad exploration using keywords from the topic being researched, such as *security and privacy*, *cybersecurity strategies*, and *PHI*. It was then narrowed down, adding other keywords such as *mHealth*, *telemedicine*, and *telehealth* to make the search more specific to the topic. Articles from the Walden University Library were searched. Thoreau, a multidata base search tool, was used to query Walden's University Library collections and ERIC databases. Google Scholar was used to broaden the search beyond the Walden University's library.

The literature review incorporated data from multiple sources about the topic that was studied. Snyder (2019) indicated that a good literature review shows a suitable approach to searching for or choosing sources. The literature review contains eighty-two sources such as research reports, scholarly journals, seminal scholarly articles, and theses and dissertations, of which 90% were peer reviewed. Also, 91% of all the sources have a publication date within the last 5 years. To ensure that the publications were peer-reviewed, they were verified via the Ulrich database.

Through this study, readers are provided an understanding of challenges IT managers encounter when attempting to protect their customers' PHI from cyberattacks when using telemedicine. The next section focuses on the application of the applied IT problem. It entails a synthesis and analysis of the literature about the conceptual framework to include supporting and contrasting theories/conceptual models and how it relates to the protection of PHI used in telemedicine.

Application to the Applied IT Problem

The purpose of this qualitative pragmatic inquiry was to explore effective strategies used by IT managers in the private healthcare industry to protect customers' PHI from cyberattacks when using telemedicine. Cybersecurity strategies vary, depending on the assets needing to be protected. Iwaya et al. (2020) mentioned that addressing cybersecurity to protect PHI includes several aspects that need to be considered: the type of telemedicine device technology, when the data are in motion, and when the data are at rest. Some of those aspects to protect PHI identified by Iwaya et al. included in this study are secured transmission such as virtual private network, transfer protocols, using certificates for authentication, authorization and permissions, data encryption, secure storage, data access, and cybersecurity awareness and training. Ogbonna (2020) mentioned data encryption as an essential aspect to protect PHI data in motion. Rothstein et al. (2020) argued that encrypting data at rest for telemedicine could improve privacy and security issues with PHI, biometrics, identity, and credit card information exposures. Rothstein et al. (2020) added that government agencies should hold manufacturers accountable for the inadequate built-in security on devices used for telemedicine. For this study, I focused on a target group of seven IT managers in the private healthcare industry performing distinct roles. Tejay and Mohammed (2023) said that IT managers' roles can be found in executive-level management such as chief technology officer (CTO), chief information officer (CIO), and chief information security officer (CISO); mid-level management such as IT and audit directors; low-level management such as team lead and information security (IS) managers; and personnel such as security analysts and cyber architects or engineers, among others. Likewise, Obitade (2019) identified IT managers in executives' roles such as vice presidents of IT, directors, and CIOs. Furnell (2021) stated that IT managers include technical and nontechnical individuals such as cybersecurity analysts, IT risk information security manager, information assurance engineer, information security manager, information security officer, chief information security architect, pen tester, and threat analyst, policy, and organizational security culture. Houston (2019) said that IT managers range from system architects to lawyers and mentioned roles such as digital forensics specialist, analysts, cyber operations planners, technical support, IT project managers, and information system security managers (ISSMs), adding that IT managers need to be able to interact and communicate with non IT individuals.

Conceptual Framework: Integrated System Theory

According to Malodia et al. (2021), a conceptual framework can be used as a roadmap to help readers understand various aspects of a topic and construct an integrated policy foundation. The IST of information security management was chosen as a roadmap to help understand effective strategies IT managers could use to protect PHI in telemedicine. Hong et al. (2003) said that the IST of information security management enhanced information (data) confidentiality, integrity, and availability (CIA), by ensuring that they complement each other. Hong et al. explained that the IST evolved out of necessity while in search of information security material. Hong et al. identified a lack of research in information security and developed the IST to further information security management with the intent of applying it to many different environments; each theory was based on previous work by other scholars. Alawonde (2020) used the IST as the framework for the study he conducted on information security strategies in the financial industry; he mentioned that the five theories that compose the IST are security policy theory, risk management theory, control and audit theory, management system theory, and contingency theory. Sindhuja (2021) assured that the five theories that encompass the IST are founded on information security concepts. Sindhuja added that when organizations assume information security management concepts, they line up with the organization's objectives. Alawonde said that when the five individual theories are combined, they form a strong framework suitable to address confidentiality, integrity, and availability issues to protect data.

The Security Policy Theory

The security policy theory developed by Hong et al. in 2003 was based on policies that measure establishing, implementing, and maintaining information security policies to protect organizational resources. Researchers Zaini et al. (2018), Zaini et al.

(2020), and Wu et al. (2020) used factors such as establishing, implementing, and maintaining information security policies to protect PHI data and resources. Likewise, Zaini et al. (2020) utilized the data protection factor as a key element to address organizational practices. Their results showed that although these factors are essential, if not implemented appropriately, they could negatively impact the organization. Zaini et al. (2018) evaluated how to protect the organization's data and people, while Zaini et al. (2020) utilized data protection to address organizational policies, plans, and procedures. Although Zaini et al. (2018) and Zaini et al. (2020) used similar factors to those of Wu et al., their research results were different from those of Wu et al. They all measured implementation and maintenance factors of the security policy, but Wu et al. measured the effectiveness of information security as well, which they included in their research about smart cities systems using green energy. Although the researchers used varied factors to measure security policy, they all attained the desired data protection in their environment.

The Risk Management Theory

The risk management theory involves aspects of risk management process and risk analysis and includes factors such as managing, analyzing, evaluating, assessing, and controlling risk within an organization. Researchers Pal and Mukhopadhyay (2018), Arogundade et al. (2021), and Muraguri et al. (2019) used factors such as risk analysis and evaluation, assessment, and control to decrease risk levels and risks costs for organizations. Their research results showed that by incorporating the necessary factors that pertain to the specific organization's environment, risk management can be accomplished. Pal and Mukhopadhyay established their research framework on the risk management theory and measured how risk analysis and assessment identify attack types to decrease the organization's risk levels and risk costs. Arogundade et al. evaluated how an organization could use the risk management process to identify critical information, security risks and control measures to protect an organization's assets. Muraguri et al. implemented the risk management theory to analyze and evaluate, assess, and control risk that resulted from vulnerabilities, and they assessed how to protect organizational assets. Even though all researchers utilized the risk management theory in their research, not all measured the same factors, but they customized them to fit their organizational needs. Thus, they reached the same outcome of protecting organizational assets.

Control and Auditing Theory

The control and auditing theory was developed by Hong et al. in 2003; it was based on previous research papers about the establishment, implementation, and audit information security controls from unauthorized access events. Researchers Muraguri et al. (2019), Zaini et al. (2020), and Bratu (n.d.) considered factors of the control and auditing theory to measure personnel, systems, and network security controls to improve the cybersecurity posture of an organization's assets. Their research results showed that many of the threats were from internal sources. Thus, establishing a cybersecurity training and awareness program, in addition to implementing more access control over systems vulnerabilities, could decrease the threat level.

Muraguri et al. (2019) measured personnel, systems, and network security controls to examine risk in systems security vulnerabilities that resulted from inappropriate configurations. Likewise, Zaini et al. (2020) measured the same factors Muraguri et al. did, but in addition Zaini et al. considered the access control factor to protect the organization from internal and external threats. Bratu (n.d.) measured the same factors as Zaini et al. (2020) and audited security controls established to reduce internal threats, which increased the organization's cybersecurity posture. All researchers used control and auditing theory in their research and measured the same factors. Muraguri et al. achieved a cybersecurity readiness to protect organizational assets, while Zaini et al. (2020) measured an additional factor, access control, which achieved an integrated approach to protect organizational assets. Bratu measured the same factors as Zaini et al. (2020) to protect organizational assets as well. All reached the same conclusion that people are the main issue, and technical control alone are not sufficient to achieve a strong cybersecurity posture, but cyber awareness and training/education are necessary to protect from internal threats.

The Management System Theory

The management system theory grew from organizational requirements and an information security architecture that Hong et al. (2003) used to establish an information security management system to oversee assets. Researchers Hong et al. and Alawonde (2020) used factors such as policy definition and management of risk, which are important within an organization's assets. Their results showed that although these systems are critical, if not implemented correctly, they could negatively impact the organization. Alawonde's research evaluated how policy definition and management of risk impacted organizational assets. His research results are like those of Hong et al., as the researchers used the same factors in determining if management systems are important within organizations. Although the researchers used different variables to measure security management, their research demonstrated that management systems encompass multiple facets of the organization (Alawonde, 2020). Alawonde, contrary to Kitsios et al. (2022), explained that organizations simply base their plans and policies on an information security management system, even if the management system encompasses multiple facets of the organization overall.

The Contingency Theory

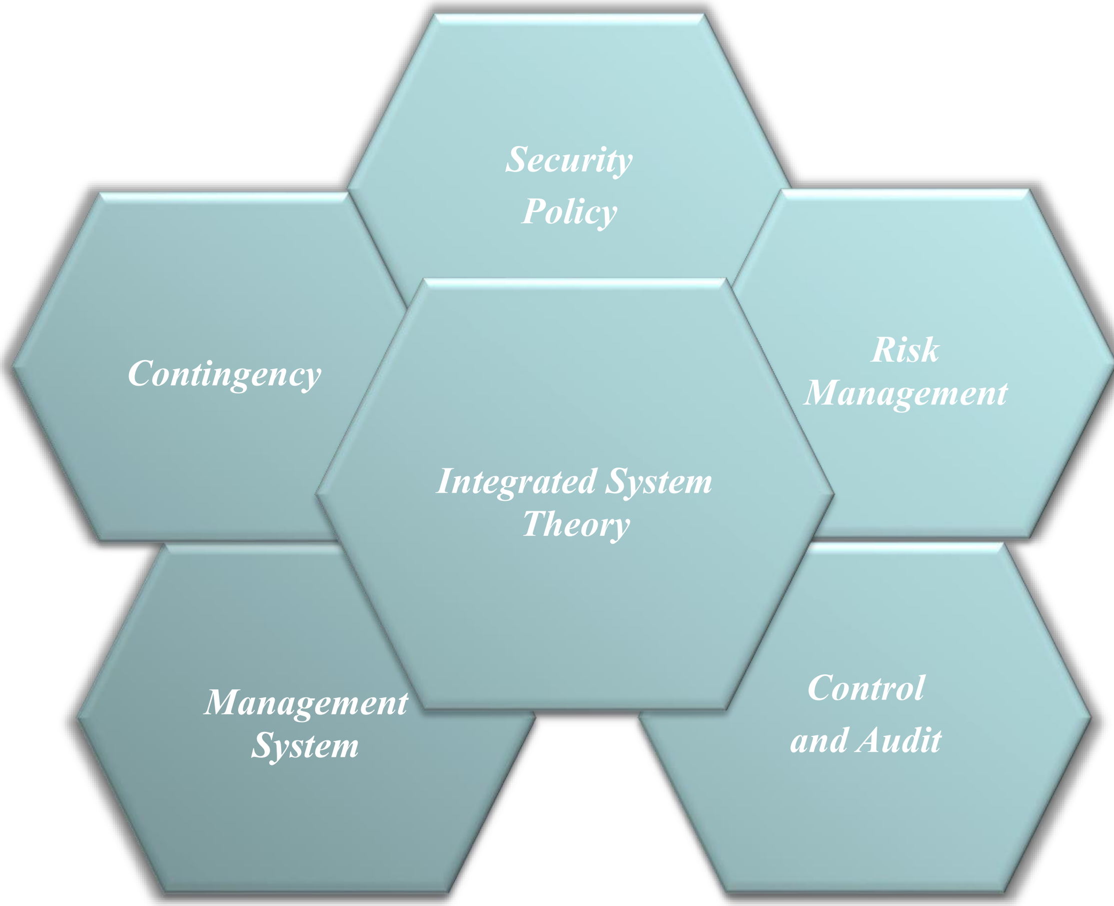
Hong et al. (2003) developed the contingency theory as part of the IST. The contingency theory evolved from the need to meet the demands of the emerging changes in the settings of information security because of technological advances (Hong et al., 2003). The contingency theory focuses on factors such as preventing, detecting, and reacting to threats and vulnerabilities while meeting the organization’s objectives (Hong et al., 2003). Researchers Zaini et al. (2020), Wu et al. (2020), and Alawonde (2020) considered contingency factors such as prevention, detection, and reaction to threats and vulnerabilities to improve cybersecurity posture in an organization. Their research results showed that by implementing those factors, they increased contingency management, which is a crucial part of information security. Thus, enhancing cybersecurity posture. Zaini et al. (2020) measured detection and response factors to implement an initiative-taking cybersecurity posture.

Wu et al. (2020) used the contingency theory as the foundation for their study to measure virus prevention and detection of information security policy to evaluate its efficacy. Alawonde (2020) included the contingency theory as part of his study framework, which measured prevention, detection, and reaction to cyber vulnerabilities and threats in the financial industry to prevent cyber exploits, which increased organizational cybersecurity posture. All researchers measured the same factors in the contingency theory in diverse ways and applied them to different industry settings, and they all managed to increase cybersecurity posture in organizations.

The integration of the five theories mentioned in the above paragraphs formed the IST, which is universally used in different industries and facets/settings in today's organizations, economy, and society. Figure 1 depicts a visual representation of the IST, which consists of five individual theories: security policy theory, risk management theory, control and audit theory, management system theory, and contingency theory, integrated into one.

Figure 1

Integrated System Theory Conceptual Framework



IST in Recent Research

The IST was developed based on the need to protect information, assets, and resources from different perspectives, since using a security policy alone was not enough (Hong et al., 2003). Previous research focused on an integrated approach necessary to implement information security and protect assets. According to Herrera Montano et al. (2022), insider's threat is one of the biggest security vulnerabilities an organization possesses. In more recent years, Erceg (2019) used concepts of the IST in an organization's environment; he stated the importance of an integrated system approach to protect assets such as data and operational procedures from insiders' threats. In recent research, IST, which is already an integrated theory, has been integrated further with other theories to further enhance security for information systems, organizations, social theories, communities, and societies that use smart technology. Gul (2019) adopted the IST framework to the big data security concept, which applies the five IST theories to big data: big data security policy, big data risk management, internal controls/security measures, big data auditing, and contingency management. Gul (2019) said that big data purpose security is data access protection by focusing on confidentiality, integrity, and availability.

Zaini et al. (2018) based their research on the IST, which integrates human interactions and the protection of information systems assets. Zaini et al. (2018) said that the IST can be used in organizations according to a specific situation (internal/external). Another example is the use of the IST to protect organizations from data breaches. Sindhuja (2021) suggested that the IST approach is critical to assess the security of an organization that operates supervisory control and data acquisition (SCADA) to prevent attacks and minimize failures. Sindhuja (2021) used the IST and applied it to his study to measure information security strategies in organizations and the organizations' awareness in implementing security measures where necessary.

Similarly, Chai and Zolkipli (2021) argued that information security strategy in organizations (ISSiO) is essential to the organization's settings, technology, and management. Another recent research involving IST is the smart city development in

Taiwan, Wu et al. (2020) based their study in the IST developed by Hong et al. (2003) with a slight modification, their framework used the contingency theory as a basis and integrated the other four theories as activities of information security management. Wu et al. (2020) explained that a smart city is considered a city's digital information integrated with cloud computing, mobile devices, information security, and Internet of Things (IoT). Wu et al. (2020) examined information security policies, implementation, characteristics, effectiveness, and maintenance of Taiwan smart cities.

Analysis of IST

The IST was developed as an integrated approach to protect organizations' resources and assets such as data, hardware, and software by using a combination of different approaches (Hong et al., 2003). Information is the most significant asset any organization could have; therefore, a combination approach such as the IST, which integrates more than a security management policy alone, is required to protect it (Erceg, 2019). Erceg (2019) agreed with Hong et al. (2003) to safeguard information (data), one needs an integrated approach that considers varied factors such as policies, procedures, strategies, and security. The IST integrates the necessary elements that can be used to protect PHI in telemedicine.

You et al. (2016) agreed with Hong et al. (2003) and Erceg (2019) in that a combined approach is key in protecting data from cyberattacks, by implementing cybersecurity policies, risk management, internal control and auditing, management systems, and contingency approaches in IST is what makes a strong basis for information security management. You et al. (2016) claimed that the IST developed by Hong et al.

(2003) became the cornerstone for researchers studying information security with a combined approach. Furthermore, Muraguri et al. (2019) urged organizations leaders/executives to get involved in cybersecurity strategies, policies, and their implementation.

In the security policy theory, Hong et al. (2003) addressed information security policies that meet organizational security requirements. In the risk management theory Hong et al. (2003) addressed threats and vulnerabilities can be evaluated to minimize the risk by using analysis and evaluation. In the control and audit theory, Hong et al. (2003) established and implemented information security control systems and conducted audit procedures to measure control performance. In the management system theory Hong et al. (2003) established and maintained an information security management system (ISMS) to regulate and guard information assets. In the contingency theory, Hong et al. (2003) addressed strategies to avoid, detect, and respond to threats and vulnerabilities impacting the organization.

Hong et al. (2003) with the IST framework introduced the integration of multiple information security management components developed to protect information systems assets and assist organizations in identifying behaviors towards information security practices. An approach such as the IST is suitable and needed to protect PHI. The complexity of today’s telemedicine technology and their intricate communication features and capabilities need a diverse protection that takes into consideration practical methods and the human factor in an organization, government, and society, such as the IST. De Oliveira et al. (2021) reiterated the intricacy of cyberattacks require a unified approach; although they did not use the IST in their study, they came to the same conclusion as Hong et al. (2003), both concurred in the use of an integrated approach to protect assets and align the organization's information security management and business practices.

Likewise, Iwaya et al. (2020) concluded that an integrated approach was crucial to protect PHI for mHealth, a form of telemedicine. Iwaya et al. (2020) used an integrated framework that focused on security and privacy of PHI in telemedicine, but as De Oliveira et al. (2021), he did not use the IST. Therefore, You et al. (2016) argued that it is essential to utilize an integrated approach tailored to information security management among different organizations in different environments that are focused on a common goal, data protection. You et al. (2016) perception and analysis of the IST seemed to indicate that the IST would be necessary for the healthcare industry where the organizations' mission and business strategies must be taken into consideration because lives depend on it.

Analysis of Supporting Theories

Before the IST conceptual framework was chosen to base this study on, other frameworks or theories related to cybersecurity strategies to protect PHI in telemedicine were considered. Some of the discovered theories specified Telehealth and others included healthcare security in their topic, but many theories focused on adoption, not on the technical aspect of the technology to protect data. The following section discusses the Integrated System for Information Security Management (ISISM) and Information Security Management (ISM) Holistic Approach as supporting frameworks revolving around the research question to address the security aspect of the issue but were not select.

Integrated System for Information Security Management (ISISM). The ISISM framework was implemented by Yang, Ku, and Liu in 2016, it consists of an integrated approach focusing its foundation on the knowledge of security requirement engineering. Yang et al. (2016) included a risk analysis approach in their integrated framework like Hong et al. (2003), but they used a security requirement engineering method as a foundation, contrary to Hong et al. that used a contingency theory as the foundation of their framework. ISISM consists of the Security Quality Requirements Engineering (SQUARE) to address security requirements, a National Institute of Standards and Technology (NIST) guide for risk management, the CCTA Risk Analysis and Management Methodology (CRAMM) for risk assessment, and the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Allegro methods with a focus on security risk assessment process, and asset vulnerability and thread analysis with the organizational goals (Yang et al., 2016).

SQUARE is used to generate and document systems and software security requirements, such as security policies; it is supposed to increase security by performing security measures, risk assessment requirements, and to protect assets while considering the cyberattacks perspective for the ISISM framework (R. A. Khan et al., 2023). *NIST* guide for information technology systems, such as *NIST 800-30*, is used to strengthen information security and provide technical and nontechnical individuals with risk assessment processes and procedures in risk identification, risk analysis, risk evaluation, and risk management to mitigate risk for their IT assets (Fikri et al., 2019). *CRAMM* was developed by a British organization and designed for broad industries, large organizations, and governments to conduct risk analysis (ENISA, n.d.). Yang et al. (2016) adopted CRAMM to compute the risk in assets value vs. the vulnerabilities (risk analysis) and to provide users with options like avoiding, reducing, or accepting risks (risk management). *OCTAVE Allegro* is used to assess information security risks, to develop risk management processes that evaluate and identify the organization's risk tolerance, mission-essential assets and its vulnerability and threats, and to determine and evaluate potential threats if they occurred (Gerardo & Fajar, 2022). The adoption of those approaches in the ISISM formed a unified framework that organizations can use to accomplish the evaluation of business impact analysis, risk analysis, and to generate information security policies that meet organizations' practical requirements, in which processes for information security management are handled appropriately (Rivers, 2020). However, ISISM focuses on the risk analysis aspect of information security engineering, creating a gap that could potentially expose PHI, thus I did not select it.

Information Security Management (ISM) Holistic Approach. A comprehensive approach is essential for information security management to be successful (Ali et al., 2021). According to Soomro et al. (2016) information security management is the primary concern due to the increase in data breaches exposing PHI, by identity theft and online cyberattacks that impact organizations; thus, an ISM comprehensive approach was developed. Tu et al. (2019) agreed with Soomro et al. (2016) and utilized the information security management comprehensive approach, which aligns IT and human resources management, but added information security activities such as policy, compliance, and awareness, which significantly impacted the management of information security.

The factors involved in the ISM Holistic approach used by Soomro et al. (2016) includes *information security and management* focusing on the alignment of information security policies and business strategies, with the involvement of the C-suite/top management, such as CIO, CHIO, CFO, and CEO (Shaikh & Siponen, 2023). *Information security policy awareness and training* include a comprehensive policy, security control features, and an awareness and training program to achieve an integrated approach (Perez-Gonzalez et al., 2019). *Information security and integration of managerial and technical activities*, refers to the integration of technical actions such as the acquisition of security hardware, software, and types of internal controls to process the organization's data, as well as nontechnical actions such as developing a security policy, providing information security policy awareness training to ensure success in information security management (Soomro et al., 2016).

Information security management and the human aspect refers to taking into consideration the human factor in the organization and not relying on the technical aspect only, by adopting a comprehensive approach (technical and nontechnical aspects) information security compliance may be enhanced (Tanoh et al., 2022). The lack of employees' awareness in information security is responsible for data breaches such as those caused by cyberattacks (Muraguri et al., 2019). *Information security as an overall business security issue* focuses on the management of risk mitigation and its impacts to the organization’s business, its market value, and its business reputation; moreover, if management becomes more involve in information security, it could potentially increase organization’s compliance (Soomro et al., 2016).

Strategic alignment of business and IT/IS and security management issues refers to the business strategies aligned with IT security, budget, and policies, for the organization’s security compliance to be successful (Soomro et al., 2016). *Business/enterprise information architecture, infrastructure and security management* focuses on the enterprise relationship between information architecture and information security as a holistic approach, to include business architecture plans and design security solutions, and argued that for the organization’s assets to be protected, top management needs to ensure the business architecture and information security management aligned and are managed appropriately (Soomro et al., 2016). *Social media and security management* refers to the significant role social media plays in our society, especially the sharing of information, and the security and privacy concerns of sensitive information potentially exposed (Soomro et al., 2016). Soomro et al. claimed that social media practices and an organization’s desire for information security are not aligned. So, despite the advantages social media offers, Al-Muhtadi et al. (2019) recommended their comprehensive approach to have organizations incorporate social media controls, such as security policy, education and training, incident planning and response.

Analysis of Contrasting Theories

The following section includes and clarifies why the technology acceptance model (TAM), and technology-organization-environment (TOE) Frameworks were not appropriate and did not fit the intended research purpose.

Technology Acceptance Model (TAM)

TAM at first seemed to align with the research topic and the world view presented in some of the articles, which acceptance of the new MHealth technology was a commonly mentioned subject. According to Nie et al. (2023), TAM was developed by Fred Davis in 1985, to show users interaction and acceptance of emergent technologies. Furthermore, Zin et al. (2023) indicated that TAM was later expanded to predict users' acceptability of a technology. Zin et al. (2023) added that TAM could be used to predict patients' and healthcare providers' intention to utilize telemedicine technology. Alsyouf et al. (2023) indicated that TAM is frequently used to predict users' adoption of emergent technology, and it would be an excellent theory to study users' behavior towards the use of a personal health record system, in which security and privacy were the main factors. Alsyouf et al. (2023) went on to say that telemedicine implementation depends significantly on security and privacy issues addressed. Zin et al. (2023) described TAM as the most recognized model for healthy IT implementation and utilized processes. Alsyouf et al. (2023) added that TAM clarifies the different intentions human behavior may have about adopting technology. However, the study is not about acceptance of the use of technology but about cybersecurity strategies used to protect PHI. Although TAM seems relative to the study researched, its use resulted in a contrasting theory.

Technology-Organization-Environment (TOE) Framework

TOE is another theory/framework that I initially thought was suitable but resulted in being contrasting. The TOE framework is used in adopting innovative technology, to include user interaction, challenges, and aspects that impact the embrace of that technology (Y. Kim & Kim, 2021). Furthermore, Ullah et al. (2021) assured that the TOE delivers an all-inclusive user approach to emergent technology, and it is considered as a risk management framework. Likewise, Ngongo et al. (2019) indicated that that TOE does not address many cybersecurity aspects and decided to add to the TOE framework cybersecurity factors aspect which in turn theory to study mHealth adoption at a healthcare organization in Africa. S. Wallace et al. (2020) stated that the TOE is a theory that concentrates on technology adoption and that is widely used for healthcare technology systems adoption. Aligarh et al. (2023) added that the TOE framework could be used as an analytical tool to learn how different organizations adopt many emergent technologies. Das and Bala (2023) offered some examples of industry and settings in which the TOE was utilized to understand the adoption of different technology, such as understanding information systems in healthcare, grasping telemedicine, and understanding the basic aspects influencing cloud computing adoption. Yang et al. (2022) claimed that TOE is an appropriate framework to be used in the healthcare industry to understand modern technology adoption. Nevertheless, as was ascertained, the TOE focuses on adoption of technology and usefulness, thus it was not appropriate to adopt as a framework for this study.

Summary of Conceptual Framework

In the conceptual framework section of the study, the selected framework IST is presented. Supporting theories/approaches such as the ISISM, and the ISM Holistic Approach, both integrated approaches, were unsuitable. Two contrasting theories/frameworks such as the TAM and TOE were considered, however, both focused on technology adoption. There was another framework not included but worth mentioning, the MHealth Apps Security Framework (MASF) by Hussain et al. (2018). Although MASF approach includes security and privacy aspects of telemedicine using mHealth apps, its focus is specifically on the smartphone Android platform. Therefore, MASF is not the appropriate framework for this study. In this study the focus was on cybersecurity strategies used in telemedicine to protect PHI that could be used across devices and not specific to a mobile device platform, such as Android or Apple. The IST of ISM is the most suitable because it offers protection from different angles, encompasses multiple facets of security for the organization, and aligns IT strategies with the organization’s goals.

Analysis of Potential Themes

There were many themes identified during the review of literature and five main themes were the most common ones; these included (a) protection from unauthorized disclosure, (b) risk management, (c) cybersecurity awareness and education, (d) privacy, and (e) data-loss prevention. The main themes are discussed in more detail in this section under each subtopic.

Protection From Unauthorized Disclosure

Protection from unauthorized disclosure refers to securing the data by utilizing security strategies to prevent sensitive data from being accessed/disclosed (Butt et al., 2023). The Security Policy Theory of the IST framework addresses protection from unauthorized disclosure by identifying the establishing, implementing, and maintaining information security policies to protect organization's data and sensitive information resources. According to Seh et al. (2020), unauthorized disclosures have been linked directly to data breaches on healthcare organizations as results from cyberattacks. Seh et al. (2020) added that almost 30% of the data breaches in the last decade were results of unauthorized disclosure. Their research indicates sensitive data breaches impacted over 157 million people in the healthcare industry between 2015 and 2020. Protection from unauthorized disclosure is challenged by users' roles and permissions, poor security implementation design, and lack of access policies, consequently impacting healthcare data breaches.

Some security strategies used to protect data from unauthorized disclosure include access control, encryption, and firewalls (Bandari, 2023). Access control, encryption, and firewalls improve protection from unauthorized disclosure by potentially preventing data breaches when physical security strategies fail (Basil et al., 2022). Access control is a technique used to protect data by controlling who has access to it, such as username and password to logon and/or security group membership (Jin et al., 2020). Furthermore, access control is key in the protection of PHI and a HIPAA requirement (Jin et al., 2020). Encryption is a mechanism used to make the data unreadable to unauthorized users, preventing the disclosure of data such as PHI (Bandari, 2023). Firewalls are utilized to protect from unauthorized disclosure by blocking unauthorized users from gaining access to the network, thus preventing data breaches (Basil et al., 2022).

Another threat to unauthorized PHI disclosure is the poor security when using telemedicine, which impacts not only patients, but healthcare professionals alike (Sendelj & Ognjanovic, 2022). Many healthcare organizations have written telemedicine guidelines that identified security risks associated with sensitive data exposure and the protection from unauthorized disclosure, such as implementing encryption when using telemedicine (El Komy et al., 2023). Protection from unauthorized disclosure can be accomplished by implementing the security strategies mentioned above, which focus on preventing sensitive data from reaching the wrong people but making sure that the right people can get it and keep the data safe.

Risk Management

Risk management refers to processes or actions taken to minimize risk, such as assessment, evaluation, and mitigation activities among others (Fikri et al., 2019). Risk management is addressed in the IST framework by the Risk Management Theory, which surrounds risk management process in its entirety, from managing, analyzing, evaluating, assessing, and controlling risk within an organization. It is addressed in the Management System Theory, which focuses on measuring how to manage risks of information security management systems and policies definition negatively impacting the organization overall, if not implemented properly. Risk management is a critical aspect to organizations that want to protect their resources from cybersecurity attacks, from prevention, mitigation, and remediation (Shaikh & Siponen, 2023). D. Kim et al. (2020) presented the Risk Management Framework (RFM), created by NIST to protect healthcare organizations' resources and networks from cyberattacks, which addresses sensitive data exposure in telemedicine. The RMF consists of technical safeguards, security policies, and procedures established that when integrated with other factors in organizations reduces the risk and potential to cyberattacks (D. Kim et al., 2020). Risk management entails different measures to protect assets in organization types, which can be applied in the healthcare industry to protect PHI when using telemedicine.

Risk management in the healthcare industry focuses on methods to protect sensitive data, such as PHI. However, to control cybersecurity risk in the healthcare industry, it is crucial to implement a risk management process to protect PHI from cyberattacks (Sardi et al., 2020). Grayson et al. (2023) used the RMF and assessed privacy risks from cybersecurity attacks in telemedicine that showed Phishing as a high-risk threat in the exposure of PHI. Furthermore, Grayson et al. (2023) identified ways to protect and mitigate the compromise of PHI by implementing an integrated approach comprised of technical safeguards, policies, and procedures such as encrypting in telemedicine. Poleto et al. (2021) stated that risk management when using telemedicine involves risk identification, risk analysis, and risk evaluation by implementing policies and procedures, establishing a baseline, assessing the risk, and notifications of events related to risks. PHI can be protected in the healthcare industry when using telemedicine, despite the challenges that healthcare organization face can be addressed by the implementation of a robust risk management plan.

Cybersecurity Awareness and Education

Cybersecurity awareness and education as addressed in the IST framework by the Control and Audit Theory, focuses on improving organization's cybersecurity posture by protecting its assets from internal threats, while exercising control over the network and managing risk of their resources. Cybersecurity awareness and education is not only a critical element but a requirement for the healthcare industry to protect PHI from cyberattacks on data, assets, and resources (Nifakos et al., 2021). Cybersecurity awareness and education enhances employees' understanding of recognizing potential cyberattacks such as cyber and reducing organizational risk (Pranggono & Arabo, 2021). Likewise, Aldawood and Skinner (2019) agreed with Pranggono and Arabo (2021) that educating employees in cybersecurity reduces organizational risk to cyberattacks. According to Niki et al. (2022), cyberattacks are the main cause of cybersecurity breaches in the healthcare industry. Ali et al. (2021) stated the importance of cybersecurity awareness and training especially for IT professionals and claimed that IT professionals are responsible for 70% of security incidents in organizations. Niki et al. (2022) elaborated that cyberattacks affect everyone, not only IT employees in the healthcare industry, therefore, education and/or awareness and training in cybersecurity must consider an integrated education approach.

Pranggono and Arabo (2021) research evaluated cyberattacks in the healthcare industry during the COVID-19 pandemic in 2020 and found phishing and ransomware attacks to be the most common and effective cyberattacks. Furthermore, cyberattacks have become more elaborate, to the point that they portray legitimate by using a secure socket layer (SSL) connection (Pranggono & Arabo, 2021). Aldawood and Skinner (2019) research evaluated a cybersecurity training and awareness program that focused on social engineering. Aldawood and Skinner (2019) found that there is a lack of cybersecurity awareness and training in social engineering such as Phishing among the organization's employees. A critical factor in protecting from social engineering attacks such as cyber, is the lack of user education, which can reduce organization's risks (Chanti & Chithralekha, 2022). Niki et al. (2022) found that cybersecurity awareness and training delivery methods need improvement and a way to connect with a diversity of employees.

Similarly, Zwilling et al. (2022) identified the need for IT professionals to receive education from a university with a cybersecurity curriculum, to include Phishing simulator training, so an increase in initiative-taking cybersecurity posture is developed. Consequently, cybersecurity employee awareness and education should utilize delivery methods like gamification and simulations, as well as including essential factors in protecting an organization's assets such as types of cyberattacks, common attackers' activities, and employee contribution in protecting PHI (Niki et al., 2022). Cybersecurity awareness is a necessity for everyone, and initiative-taking education is the key to protection.

Privacy

Privacy refers to an individual's right to have their PHI protected/safeguarded (Alfawzan et al., 2022); it limits what others are allowed to see. Data privacy involves educating users on how to use and share sensitive data, employing technical safeguards such as encrypting the data, and awareness of how to manage and protect the PHI (Basil et al., 2022). Privacy is addressed in the IST framework by the Management System Theory, which establishes information systems policies definition and risk management to protect organizations' assets and resources. Also, privacy is addressed by the Security Policy Theory, which focuses on protecting PHI by applying policies and procedures across the organization. Bhuyan et al. (2020) presented concerns with PHI privacy in telemedicine. According to Bhuyan et al. (2020), cybersecurity breaches in the healthcare industry are compromising patients' data. Privacy is key to telemedicine, according to Al-Muhtadi et al. (2019). The absence of controls to collect, use, and disclose sensitive information places PHI at risk. Bai et al. (2022) stated that the risk of PHI exposure have increased when using telemedicine, because of the poor privacy and security features such as authentication, access control, and encryption to protect PHI from cyberattacks, thus exposing PHI to security breaches.

Privacy is not only necessary but required to oversee PHI data in the healthcare industry. On multiple cyberattacks perpetrated in 2022 among three healthcare organizations, in one the PHI privacy was compromised for 54,000 individuals, in another cyberattack compromised over 8,000 patients' data (Alabdulatif et al., 2022). Furthermore, Alqurashi et al. (2023) claimed that PHI privacy is one of the biggest concerns in telemedicine, hindering society from engaging more in telemedicine. Bhuyan et al. (2020) suggested that limited regulations governing PHI protection in telemedicine are a security challenge and current HIPAA laws are not defined to address current technologies. Cartwright (2023) stated that out of date hardware is a high-risk and common vulnerability that makes organizations more propense to data breaches and potentially exposing PHI.

Data-Loss Prevention

Data-loss prevention (DLP) is a countermeasure to minimize data compromise from cyberattacks (Shahbaznezhad et al., 2021). DLP involves blocking actions taken to extract or obtain sensitive data from organizations' systems as results from cyberattacks (Ansari & Khaliq, 2022). DLP is addressed in the IST framework by the Contingency Theory, which focuses on countermeasures to prevent, detect, and react to cyberattacks on sensitive data like PHI, preventing it from leaving the organization. Some cybersecurity strategies involving DLP are encryption to protect sensitive information such as PHI, authentication such as multi factor authentication (MFA) to ensure the right people have access to the data, and data backups to restore systems data as a response/reaction from cyberattacks (Javaid et al., 2023). Grayson et al. (2023) stated that DLP can increase the chances of keeping sensitive data such as PHI safe, whether the data is at rest or in-transit (F. Khan et al., 2021). Keeping sensitive data protected is key to any business, but when it comes to healthcare in which people's lives are at stake, it becomes essential.

There are strategies used in DLP today that include the protection of sensitive data. Alshammari (2020) studied the DLP topic and found that DLP can protect PHI regardless of the data state (at rest, in motion, or in use). Alshammari (2020) concurred with Javaid et al. (2023) in that encryption is a crucial strategy in protecting PHI and added that security policy and compliance, data identification, and access control are needed for DLP to be successful. Likewise, Herrera Montano et al. (2022) agreed with Alshammari (2020) in using encryption in DLP to protect sensitive data, such as PHI in the healthcare industry. Furthermore, Herrera Montano et al. (2022) suggested an integrated approach in DLP strategies, in addition to encryption the use of hash to verify if the data being retrieved matches the predefined value, biometrics (MFA) to authenticate authorized users. DLP can be accomplished in the healthcare industry using trigger alerts, blocking action, and when used with an integrated approach of strategies, it can be successful.

Relationship of the Study to Previous Research

It was not until a decade ago that cybersecurity research on telemedicine gained attention, but IT research on cybersecurity protecting PHI from cyberattacks in the healthcare industry when using telemedicine is scarce. Studies focused on the use, adoption, and acceptance of telemedicine. Lang (2018), in an article for the information systems security association (ISSA), presented telemedicine from the cybersecurity point of view and expressed the lack for cybersecurity strategies such as built-in security in software or application design, automated security policies, and access control, when using telemedicine. Shahbodin et al. (2019) discussed a telemedicine cybersecurity strategy that accentuated factors regarding its privacy, security, and confidentiality. The research highlighted the crucial role telemedicine plays in society by facilitating remote care with lower costs but increasing privacy and security risks that could potentially expose PHI (Shahbodin et al., 2019).

Similarly, Jalali et al. (2021) authored an article emphasizing the importance of securing sensitive data by applying security and privacy techniques to protect the data while using telemedicine. Moreover, Jalali et al. (2021) stated that cyberattacks have proliferated in telemedicine since the COVID-19 pandemic, exposing PHI and patient data. Likewise, Alabdulatif et al. (2022) identified a research gap in cybersecurity for the healthcare industry and the lack of use an integrated approach to address the protection of sensitive data in telemedicine. Iqbal et al. (2022) stated that sensitive data needs to be protected from cyberattacks when using telemedicine and key aspects to protect it involve privacy and security. Dey (2023) presented a potential security solution, encrypting the communication session by synchronizing the patient session key with the medical provider session key, forming an exclusive key, when using telemedicine to protect sensitive data.

Cyberattacks are still at large, but there is new research and viable solutions in the horizon. This study helps to close a gap in the literature about cybersecurity strategies to protect PHI in the healthcare industry when using telemedicine. Moreover, closing that research gap with this study positively impacts on the IT professionals, healthcare professionals, and society overall.

Transition and Summary

In section 1 of this research study, the background of the problem, which provides an overview and introduction of the topic, is presented. The problem statement states the gaps in the study and introduces the challenge of PHI security in telemedicine. The purpose statement presents the intention, benefits, and implications for social change in this study. The nature of the study shows the methodologies considered and the selected one and the reason for the selection.

Section 1 includes the research question, and the conceptual framework, which provides a background of the framework and establishes the based on the theory for the study. Section 1 also included the significance of the study which highlights strategies that benefit society. Section 2 provides an overall understanding of the research project and presents a plan for the study. Also included is the role of the researcher, participants and population sampling, ethical research, data collection, organization, and analysis, and reliability and validity.

Section 2: The Project

Section 2 includes a restatement of the purpose of this study; provides details on the reason behind the selected methodology, including access to participants; and outlines the researcher's bias. Also, it addresses the role of the researcher, participants, the research method and design, population and sampling, and ethical research. Further, it includes data collection, data analysis technique, reliability, and validity, and it concludes with a transition into Section 3, summarizing Section 2.

Purpose Statement

The purpose of this qualitative pragmatic research was to explore strategies IT managers in the healthcare industry use to protect their customers' PHI from cyberattacks when using telemedicine. The target population consisted of seven IT managers in the private healthcare industry within the United States who had experience with cybersecurity strategies implementation to protect PHI from cyberattacks when using telemedicine. The implications for positive social change rest on the potential to reduce PHI data exposure in telemedicine from cyberattacks, inadvertently accessed, shared, sent, and/or received. The reduction of data exposure can improves healthcare at a distance and has the potential to increase individuals' quality of life that otherwise would be at risk by the lack of cybersecurity on PHI used for patient care.

Role of the Researcher

Qualitative researchers play a key role in data collection. According to Clark and Veale (2018), the researcher's role is to gain insight into the participants' environment and experiences as the main data collection instrument. My role as the researcher in the data collection process was to be the primary data collection instrument. Participants were engaged to understand their environment and experiences. The researcher's familiarity with their geographical location, community, or professional contacts could influence the research results. According to Wadams and Park (2018), the researcher's relationship with their place of work, participants, and the area where they live may impact the outcome of the research. Wadams and Park (2018) suggested some strategies to mitigate researchers' bias: (a) explicitly documenting their worldviews/personal beliefs in field notes; (b) using open-ended questions, so the researcher's influence on data collection is limited; (c) peers reviewing data collected, analysis, and findings, which could establish internal validity by peers counteracting researchers' bias; (d) continuously asking analytical questions to bring insight on the topic; and (e) aligning their values/beliefs in relation to the study, enhancing validity of the data and giving the researcher deeper understating on participants' experiences.

My relationship with the topic extended to work experience. I had no prior knowledge of who the participants were; thus, no relationship with the participants was formulated for the study. Nevertheless, to mitigate bias that could influence the outcome of the study, open-ended questions were used, the study was reviewed by peers and mentors, and I maintained an analytical position throughout to reduce impacting the outcome of this study.

A researcher must maintain discretion during the research process. Researchers' ethical responsibility is to keep confidentiality and safeguard information trusted to them without disclosing it (Eagleson et al., 2017). According to L. Wood (2017), researchers' responsibility to protect participants and the data they provide, ensuring that ethical practice is followed and that participants are treated fairly, was established by the Belmont Report of 1979. The ethics standards in the Belmont Report protocol were adhered to across all phases of the study. Integrity is an essential part of my values. Integrity was maintained as a standard during the various stages of the study.

Researchers could inadvertently introduce bias to their research, based on their beliefs, values, and education received since childhood. To reduce researcher bias, researchers should disclose their values, worldviews, prejudices, and experiences they bring to the research study (Sutton & Austin, 2015). A fair and without-bias interview protocol was developed. All participants received an explanation of the process. Kaewkungwal and Adams (2019) said that the researcher's personal, professional, and economic worldviews could introduce bias into the research and recommended that researchers avoid introducing bias, understand and follow their organizations' board of ethics policy, consider potential risks to participants, and protect them. Therefore, to reduce bias, the Walden University Institutional Review Board (IRB) study number 07-26-24-0664321 policy was reviewed and understood.

Participants

IT managers such as CIOs, CISOs, and IS personnel in the private healthcare industry were key participants who possessed authority to impact policy changes. The criteria for which the participants were eligible and selected were a critical aspect of this study. McNair et al. (2016) and White and Hind (2015) used a broad criterion because it was challenging to obtain participants with limited parameters. Restricted or limited criteria could exclude participants (Martínez-Mesa et al., 2016). The following criteria were used to find participants who met the following requirements: IT managers in the private healthcare industry within the United States who had experience with cybersecurity strategies implementation to protect PHI from cyberattacks when using telemedicine. Those candidates who did not meet these criteria did not take part in the study.

Peticca-Harris et al. (2016) said that gaining access to participants is key to conducting research and added that gaining access to participants entails finding and securing participants for research. Peticca-Harris et al. stated that to gain access to participants, researchers must create rapport with gatekeepers as facilitators who enable access, monitor, and control activities with participants. Marks et al. (2017) used social media and a liaison to gain access to suitable participants. To gain access to participants, social media websites such as LinkedIn and members of associations such as Health IT and Health Information and Management Systems Society (HIMSS) were used. Cooper (2017) suggested that the use of a consent form protects participants because it specifies the anonymity and confidentiality of the participants. Before engaging in data collection from potential participants, I obtained approval from Walden's IRB, which I provided to potential participants with a consent form.

Developing a good working relationship with participants is essential in gaining their trust. Weller (2017) assured that rapport is fundamental to ethical research practice and involves communicating with participants and establishing a relationship prior to an interview. Dempsey et al. (2016) suggested that to build rapport with a participant, the researcher should practice active listening, make participants feel at ease, and share personal stories and invite participants to do so as well. Drabble et al. (2016) stated that cultivating rapport between the researcher and participants is vital to engaging participants in having a productive interview. Drabble et al. added that to build rapport, the researcher and participant can engage in small talk prior to the interview, discuss the interview objective, and talk about the interview afterwards, such as in the researcher responding to questions the participant may have. To establish rapport with participants, a relationship with participants was established by conversing via phone, exchanging emails, or making video calls. This process allowed participants to become familiar and comfortable with the research study, discuss the interview process, and receive answers to questions they might have.

Research Method and Design

The three main methods in research include qualitative, quantitative, and mixed methods. Researchers use qualitative methods to answer the research question(s), based on the participants' point of view and lived experiences (Hammarberg et al., 2016). The purpose of this study was to explore the successful strategies participants used to protect PHI in telemedicine.

Research Method

In research, there are two main categories, quantitative and qualitative; quantitative is precise in the use of numbers, and qualitative concentrates on people's lived encounters (Rutberg & Bouikidis, 2018). The combination of the two is referred to as mixed-method, which consists of numerical data and words describing data collection

(Rutberg & Bouikidis, 2018). I considered qualitative, quantitative, and mixed-methods, and I selected the qualitative research method. According to Aspers and Corte (2019), it is hard to describe the main essence of qualitative methodology; however, they defined qualitative methods as an explorative process in which a strategy is developed to obtain deeper understanding of the phenomenon being studied. Aspers and Corte added that qualitative methods are not scientific and are not as accurate as quantitative methods that use empirical data; therefore, qualitative methods are more susceptible to subjective analysis. Similarity, Mohajan (2018) stated that qualitative methods are a way in which people explain individuals' experiences and understand their environment. Qualitative methods involve logic, discourse analysis, open-ended questions, focus groups, pragmatic inquiry, ethonography, and grounded theory (Mohajan, 2018). Moreover, Park and Park (2016) suggested that the qualitative method is how researchers gain understanding and explore experiences that individuals have in common with a phenomenon or topic. Qualitative methods focus on applied discoveries and findings, such as the use of research question(s) and field study in natural settings (Park & Park, 2016).

Qualitative methods can be used to obtain deep insight from individuals' experiences. Pope (2020) said that the essence of qualitative methods is that the researcher focuses more on conducting research on participants and less on the subject; the researcher and participants develop a rapport, trust, and close relationship. Researchers use qualitative methods to gain a deep understanding of peoples' experiences and to provide insights into their actions or behaviors (Rosenthal, 2016). In addition, qualitative methods are useful to explore participants' personal view in researching a concept (Bhattacharyya & Pradhan, 2019). Likewise, Tahamtan et al. (2017) conducted a study that utilized the qualitative method to provide in-depth insight into the participant's experience in adopting smartphones. Likewise, Birt et al. (2016) used semistructured in-depth interviews in qualitative research to understand participants' experience with a medical issue. I chose the qualitative research method because it allowed me to use semistructured questions to explore the participants' experiences and gain insight on the strategies participants used to protect PHI in telemedicine, which was the emphasis of the study. Therefore, the qualitative method was the most appropriate approach to gain in-depth insight into strategies used by participants to protect PHI.

Quantitative methodology was considered; however, it was not chosen. Quantitative methods focus on quantifying data, testing a hypothesis, or theory. Park and Park (2016) described quantitative methods' attributes as structured, deductive, accurate and reliable, and objective. Park and Park stated that quantitative methods utilize hypothesis testing to attain research goals. Goertzen (2017) defined quantitative methods as focused on data collection and analysis that can be shown numerically. Goertzen added that quantitative methods use statistical analysis, can be measured and quantified, are objective, and involve the collection of data as numerical counts. McCarthy et al. (2017) agreed with Goertzen in that quantitative methods are objective, quantifiable, and measureable, and concurred that with quantitative methods, data analysis is based on statistical data. As discussed in this paragraph, quatitative methods are empirical in nature.

In quantitative methods, researchers have an empiral mindset, and they emphasize the significance of ideas such as objectivity, validity, or bias based on strict logic (Zyphur & Pierides, 2020). Bansal et al. (2018) suggested that many quantitative researchers have made their decision when they commence their study, making the data and their analysis acceptable to answer their research questions. Quantitative methods' nature of engaging in testing limits researchers' ability to explore phenomena (Else-Quest & Hyde, 2016). In this study, a theory or hypothesis was not tested, nor were quantitative data collected. This study was about gaining insight into participants' experiences and exploring effective strategies used to protect PHI. Because the emphasis of this study was exploring strategies IT managers use to protect customers' PHI from cyberattacks when using telemedicine, the quantitative method did not meet those needs. Therefore, it was not selected, as the quantitative method is an empirical process that concentrates on hypothesis testing.

The mixed-method approach was considered; however, it was not chosen. Mixed methods combine qualitative and quantitative methodologies (Dawadi et al., 2021). According to Palinkas et al. (2019), mixed methods is an approach that follows qualitative and quantitative concepts and is usally conducted by a team of researchers. Palinkas et al. elaborated that researchers collect and analyze data, integrate the findings, and reach a conclusion using qualitative and quantitative approaches simultaneously. Schoonenboom and Johnson (2017) confirmed Dawadi et al.'s (2021) statement that in mixed methods, researchers combine the quantitative and qualitative approaches, and they agreed with Palinkas et al. that in mixed methods, researchers apply quantitative and qualitative viewpoints to collect and analyze data and draw inferences from them, for accuracy, deep understanding, and validity.

Researchers find mixed methods valuable. Rutberg and Bouikidis (2018) claimed that with mixed methods, researchers are not limited to one approach to data collection, thus making the study more practical and enhancing validity by complementing each of the approaches (quantitative and qualitative). Molina-Azorin (2016) believed that for a mixed-methods approach to add value to research, it needs to integrate qualitative and quantitative methods. Similarly, Shannon-Baker (2016) expressed that with mixed methods, the researcher(s) can reach a deeper level of understanding of a phenomenon, an understanding that they would not acquire by using a single research method. Moreover, the quantitative methodology that is used in mixed methods contains empirical data used to predict variances and high and low values with data presented in graphs and plots (Zyphur & Pierides, 2020). A numerical or statistical type of data would not have added value to this study, because the focus of this study was to explore strategies and gain an in-depth understanding of how IT managers protect customers' PHI from cyberattacks when using telemedicine. Therefore, because the research study did not obtain numerical data, the quantitative approach was not used, eliminating the mixed-method possibility.

Research Design

The qualitative research method involves multiple design types: pragmatic inquiry, case study, ethnographic, grounded theory, narrative, and phenomenological design. Five designs were consisered: (a) pragmatic inquiry, (b) case study, (c) ethnographic, (d) narrative, and (e) phenomenological designs. A pragmatic inquiry design was chosen because it was the most appropriate design to address the research question, explore participants' practical experiences, and gain direct understanding on the process IT managers used in applying effective cybersecurity strategies to protect customers' PHI from cyberattacks when using telemedicine.

The case study was considered but not selected, because it is designed to explore complex problems that require deep understanding among a large pool of participants across multiple organizations (Harrison et al., 2017). Scuotto et al. (2016) used a case study design to conduct in-depth analysis to further theory development regarding activities, strategies, and methods in multiple organizations. Also, Ridder (2017) mentioned that a case study intensely scrutinizes issues in a "real-life" setting to understand events that occurred.

The ethnography design was considered as well but not selected. Ethnography designs focus on the study and definition of social groups and how they solve intricate issues (J. Wallace, 2019). Gable (2017) described ethnography design as the study of society's culture. Hanif (2015) used an ethnography design to study the significance of culture. Similarly, Isaksson et al. (2017) discussed ethnography in the context of the design and architecture of artifacts as a cultural study.

The narrative design was considered but not selected because this design's primary focus was social and human sciences, used as a way for people to express their life stories (Bruce et al., 2016). The focus of my study was not the participants' life stories. Hickson (2016) indicated that the narrative design is used by researchers who want to explore the way people's stories were created and placed. Clandinin et al. (2017) suggested that social science researchers use the terms *narrative* and *story* as interchangeable in this type of design. Clandinin et al. added that the way researchers conduct qualitative research with a narrative design is by living alongside the individual telling the story. This study did not include the use of living alongside participants or listening to their life stories, so the narrative design was not used.

The phenomenological research design was not selected because that design focuses on the description of individuals' daily life experiences. Limberg, Schuermann et al. (2018) stated that the phenomenological design's purpose is to gather individuals' life experiences and illustrate them. The focus of my study was not on individuals' life experiences through an event. The phenomenological is used widely in psychology research, and it focuses on individual experiences, how individuals perceived an event or issue (Larkin et al., 2019). Meshkinyazd et al. (2020) described the phenomenological approach as the daily "lived experience" of individuals that make research real or meaningful in their lives about the phenomenon. Consequently, since I did not study individuals' life experiences, the phenomenological design was not used.

Population and Sampling

The target population in this qualitative pragmatic research included IT managers working in the private sector supporting the healthcare industry, located in the United States. The IT managers roles comprise IT director, chief information officer (CIO), chief information security officer (CISO), network engineer/manager, ISSM, and telecomunications managers among other IS personnel. Martínez-Mesa et al. (2016)

described the target population as the overall group in which the eligible participants that have experienced the phenomenon or where the issue reside. Asiamah et al. (2017) said that defining a population's criteria that posses inclusive/exclusive attributes is the foundation to the sampling process. Ackerman et al. (2021) said that a good population representation is as good as the criteria established. I used an eligibility criteria during the sampling process, which yielded a high quality and precise sample group.

A purposeful sampling approach was used to identify individuals from the target population that possessed specific attributes included in the eligibility criteria. Bano et al. (2018) said that purposeful sampling is used in qualitative research to obtain the necessary information from a small number of sources. The power of purposeful sampling relies on that the more relevant the information the sample share, the least amount of participants are needed (Malterud et al., 2016). The purposeful sampling method established the sampling frame while accomplishing the research with all the participants. Griffith et al. (2016) referred to purposeful sampling as "information-rich" participants, which are not selected randomly. The purposeful sampling approach used is called expert sampling. The expert sampling approach relies on the subject matter experts experience and knowledge on a subject, to provide insight into the issue being studied (S. Khan et al., 2020). Utilizing the expert sampling approach, made it certain that participants met the defined elegibility criteria and the data that was collected was from experts in their cybersecurity specialty area. The homogeneous and snowball purposeful sampling strategies were considered. However, the homogeneous sampling strategy was not selected because it does not focuses on participants' expertise. Staller (2021) stated that homogeneous sampling focuses on cases with the same type of charatecristics such as cultural or economic background, and it is taylored towards focus groups. The snowball sampling strategy was considered; however, it was not selected. Snowball sampling focuses on participants refering other participants for the study, such as a network of friends (Curtis & Keeler, 2021), which may potentially introduced bias into the research. Therefore, the expert purposeful sampling method provided me with participants that have in-depth information and experience with cyberseucrity strategies to protect PHI in healthcare organizations, which based on their expertise potentially answered the research question.

The sample size or the number of participants has been contested for years in qualitative research, and in this case, it fluctuates. Moreover, to identify a valid sample size in qualitative research is challenging (Sim et al., 2018). The sample size is a critical aspect that could be affected by two main factors, the design of the study and the objective (Nanjundeswaraswamy & Divakar, 2021). Often, researchers need to specify a sample size to meet ethics research board requirements, but the sample size may fluctuate during data collection; qualitative researchers needs to continue collecting data to answer the research question until they reach data saturation (Gill, 2020). Boddy (2016) claimed evidence of data saturation in a qualitative study with a sample size of six to twelve in-depth interviews. Vasileiou et al. (2018) suggested that eight participants are suitable for exploratory research. Hagaman and Wutich (2017) conducted and affirmed that the sample size in qualitative research is based on data saturation, and added that data saturation has been reached between six and twelve interviews. Blaikie (2018) stated that the best qualitative researchers can do is to identify a sample size, to indicate a range based on previous research data. Therefore, since this is a qualitative pragmatic inquiry research and based on the information from the sources above, a sample size of seven interviews was used and deemed appropriate.

Data saturation describes the process when no new themes emerge from new data collection results, such as interviews. Hancock et al. (2016) stated that one had reached data saturation when new ideas are not emerging. Tran et al. (2016) agreed with Hancock et al. (2016) in that when researchers collect information from new participants, and there is little or no change from the data collected, data saturation has been reached. Likewise, Tran et al. (2017) indicated that data saturation occurs when the collection and analysis of data from new participants do not change the data results or introduce new themes. Boddy (2016) stated that data saturation take place when no new themes are found in the data from further interviews. Vasileiou et al. (2018) mentioned that in qualitative studies, the researcher often has to conduct additional data collection until no new themes emerge.

A participants' criteria is use to define characteristics that identified eligible participants from the population. The selection of elegible participants is crucial to yield quality data in the study. Lopes et al. (2020) used inclusive and exclusive criteria on a research study about reading challenges, to define the eligible participants. Asiamah et al. (2017) stated the eligibility criteria is the key to discover those potential participants that possess the desired attributes to provide quality information. E. S. Kim et al. (2017) states that broad and limited criteria could impact negatively the research study and the outcome. The eligibility criteria, described in the Participants section of this study, and included in the consent form is specific, not broad or limited to avoid risking generalization or applicability of the results, and is defined to select those participants that potentially answered the research question. The use of a eligibility criteria to select participants helped me prevent bias and ensure potential participants meet the required criteria to participate in the study.

Remote interviews were conducted using Microsoft Teams, a video call technology. An alternate comparable video call technology, such as Zoom was used if the participant was unable to use Microsoft Teams. The interviews were audio recorded with participant agreement. Participants were able to decide the interview location from which they feel safe, comfortable, and free to open-up. Oltmann (2016) said that interviews could be done from a place in which the participants feel protected. Mirick and Wladkowski (2019) stated that the use of “digital technologies” such as Skype to conduct interviews, provides the capability to observe for visual cues. Weller (2017) conducted research about the use of video calls in qualitative studies, and stated that participants liked it, had a pleasant experience, felt comfortable, and safe to open-up. Recently, we have been under a health hazard that we had to maintain social distancing; allowing participants to interview from a remote location potentially reducing stress and making them feel comfortable. Thus, video call technologies such as Microsoft Teams and similarities were an excellent alternative to on-site interviews.

Ethical Research

In this study, attention to ethical research was given by following The Belmont Report guidelines that protect participants' privacy and anonymity. Brear (2018) suggested that the consenting process is a fundamental principle in ethical research, and it provides participants with information about the study as well as risks and benefits they can encounter. In the U.S., ethical basis protections for research involving humans are established by the Belmont Report, which consist of three ethical principles: respect for persons, beneficence, and justice (Redman & Caplan, 2021). Respect for people is focused on individuals' participation according to their terms, which is achieved by the informed consent process, and assures participants' autonomy (L. Wood, 2017). Beneficence is focused on the risk participants may be exposed to vs. the benefits they could receive from the research, and it is achieved by the involvement of a Review Board or committee to weigh the risk vs. benefit ratio (Adashi et al., 2018). Justice is focused on the benefit for one group does not harm another (Veatch, 2020). In this study, respect for people was achieved using the informed consent form; beneficence, was achieved by the participants not being exposed to different/higher risk levels as of everyday life risk level. Justice was achieved by the participants being the same group that benefit from the study. Therefore, Walden's IRB was adhered to, which follows the Belmont Report.

The IRB ensured this research follows and meets ethical standards by reviewing and verifying it before the consent process starts. Lindsley (2019) expressed that the consent process is an ongoing communication providing participants with adequate information so they can keep making informed decisions. Additionally, participants were properly informed of their right to participate and withdraw their consent to participate at any stage of the study (Kaewkungwal & Adams, 2019). A fundamental aspect of the consent process is the consent form, which is a document that describes in simple terms the researcher's ethical role and responsibility, a statement about protecting participants identification, as well as indicating the presence of any risks and how it will be mitigated (Vitak et al., 2017). The consent form for this study includes: a) a statement that participants identification was protected/masked by a letter/number code, none of the participants' identity was disclosed to anyone outside the study's data transcript/analysis process; b) a brief explanation of the purpose of the study, c) a description of how the study is a benefit to the participants; d) a statement indicating the study does not present risks levels not already present on everyday life, and e) a statement indicating there is no incentive for participation in the study. Furthermore, the consent form indicates that participants can withdraw at any time during the study with no penalty for their discontinued participation, by formally notifying the Walden University's research participants advocate or me via email and stating their intentions to withdrawal from the study.

The consent process started once approval was received from the Walden University IRB. The consent form was emailed to participants, right after sending the LinkedIn invitation to participate. The participants replied consenting and included the statement "I consent" explicit on the reply. In turn, each participant was assured complete anonymity. The informed consent is designed as an ethical protection for participants taking part in research (Crutzen et al., 2019). Othman and Hamid (2018) explained that protecting and guaranteeing participants anonymity was essential to the wellbeing of participants and their withdrawal from their study. Likewise, Tulyakul and Meepring (2020) stated that confidentiality is key in the informed consent process and to protect participants' anonymity a code needs to be used. To protect participants' anonymity, a letter-number combination code was used. For example: *Participant One* was coded P1, *Participant Two* was coded P2, and so on, which masqueraded their identity. The consent replies received from participants were secured along with the rest of the raw data (interview recordings, logs, and others). Electronic files are kept in an encrypted or password-protected drive/vault, which is a secure container that I only have access to; data is kept for five years, then destroyed. In addition to that, when the transcript service was being used, a confidentiality and nondisclosure agreement was signed to protect all participants.

Data Collection

Instruments

In qualitative research there are many types of data collection instruments. but the researcher is the primary instrument. Data collection instruments in qualitative research refer to interviews, documents analysis (electronic or hardcopy), focus groups, observation, the researcher, and any devices used, such as recording devices and video cameras, among others (Twining et al., 2017). Clark and Veale (2018) stated that the researcher's analysis and interpretation of the data collected are crucial to the study, which is why the researcher is the primary data collection instrument. Likewise, Paradis et al. (2016) stated that the data collection strategy in qualitative research is critical and concurred with Clark and Veale (2018) that the researcher as the interviewer is the primary data collection instrument. Data was collected from IT managers by conducting semistructured interviews and reviewing publicly available documents such as policies and procedures, technical documents, and memorandums related to cybersecurity strategies to protect PHI from cyberattack when using telemedicine. Public-facing documents published by reputable sources such as those found in social media, blog postings, magazines, and professional organizations' websites, such as LinkedIn, IEEE, ISC2, and HIMSS, were used to further validate the research studies results.

During data collection, semistructured interview questions were used (see Appendix A). An interview protocol (see Appendix B) was used to stay focused on the topic and guide the interview process, standardizing it for all participants. Interview voice recordings were used to aid in maintaining accuracy. Taylor et al. (2017) developed an interview protocol using semistructured interviews as data collection, which included a list of questions that guided the interview process. Likewise, DeJonckheere and Vaughn (2019) utilized semistructured interviews and an interview protocol to conduct data collection. Furthermore, Rimando et al. (2015) utilized interviews as a data collection instrument for their study and added that recording devices could help capture details the researcher might miss by taking notes.

Member checking refers to the participants' view/verification of the data collected, such as interview data interpretation and analysis. Busetto et al. (2020) stated that member checking is obtaining participants feedback for accuracy of the researcher's analysis of the data collected. Thomas (2017) indicated that member checking validates researchers' findings against participants' statements. The study's validity was enhanced by using member checking. Candela (2019) indicated that member checking occurs when the researcher provides participants with a draft of the interview analysis, findings, or transcripts for review to ensure the researcher's accuracy of the data collected and analyzed. Participants reviewed a summary of the interview transcript, data analysis, and interpretation of the data collected to validate the data and enhance trustworthiness.

Data Collection Techniques

The primary data collection technique used was semistructured interviews with audio recordings to enhance data accuracy. The semistructured interviews included ten open-ended questions tailored towards addressing cybersecurity strategies to protect PHI from cyberattacks when using telemedicine. Once permission was obtained from Walden University IRB to collect data, LinkedIn social media site was used to reach out to potential participants. IT managers that met the criteria were provided with an informed consent form for participation. After reviewing the signed consent forms and identifying those that met all the participants' criteria, interviews were scheduled by using video call technology, Microsoft Teams, or a comparable technology to accommodate the participant, if Microsoft Teams is not feasible. Forero et al. (2018) utilized a semistructured interview data collection method because it provided a flexible and focused environment for participants to expand on the topic that has been studied. Seitz (2016) suggested that using a software application such as Skype to conduct interviews is convenient, less intrusive, and participants may feel more comfortable being interviewed in the privacy of their home or office, in a safe space. The research topic and purpose of the interview was explained. Additional clarification included the need for taking personal notes of thoughts/impressions, and with their permission. The interviews were audio recorded using a voice recorder smartphone app. The use of a smartphone to record the interviews audio is beneficial (S. Matlala & Matlala, 2018) to maintain accuracy. Recording the interview increased data collection accuracy (McInnes et al., 2017). Participants were reassured their name would be removed from the voice recording transcript, the interview would not be published, and they can withdraw at any time during the study.

The secondary data collection technique that was used is the review of publicly available documents with emphasis on PHI protection and cyberattacks; the topic being studied to complement the analysis of the data. Publicly available documents such as those published online, those found on public-facing websites, and those posted on social media websites were part of the analysis. Document analysis is one of the most used data collection techniques and it includes the review of reports, guidelines, and policies (Busetto et al., 2020). Document analysis adds value to a study while decreasing bias ethical concerns from the public worldviews (Morgan, 2022). Document analysis not only complements other types of evidence but also is an effective data collection technique in pragmatic inquiry research (Ulrich, 2020). The use of this technique increased this research credibility and supported the evidence from the semistructured interviews.

Data collection techniques such as semistructured interviews and document analysis have advantages and disadvantages. The main advantage is that interviews can be focused on answering research questions of the study (Gaikwad, 2017). The researcher has the freedom (within the interview protocol) to change the order of the questions while maintaining the direction of the interview (Dikko, 2016). Another advantage of the semistructured interview technique is the gain of deep insight from participants (Maramwidze-Merrison, 2016). A drawback to semistructured interviews is the coordination and challenges to meet with participants and agree on availability/schedule (Maramwidze-Merrison, 2016). The limitation of semistructured interviews when interviewing individuals is that the interviews tend to generate fewer opinions/ideas than in group semistructured interviews setting (Tausch & Menold, 2016). Another limitation with semistructured interviews when conducted by phone is that they could hinder the overall quality of the interview because of nonverbal cues and participants' reactions the researcher may miss (Shapka et al., 2016).

There are some advantages and disadvantages of using the revision of documents as a data collection technique. A significant advantage of document revision technique is that it can be used across multiple fields of studies and topics (L. M. Wood et al., 2020). Also, potentially rich data sources, especially for difficult subjects and historical value of the data (Chatfield, 2020). Documents vary in format; they can be printed or digital (Wilson et al., 2016). A crucial disadvantage of using the revision of documents as a data collection technique is the potential of introducing the documents' author's bias (Gaikwad, 2017). The reviewed document was a result of different research/inquiry and may not have pertinent information (Sherif, 2018).

Once the data was collected via semistructured interviews with audio recordings and analysis of documents, member checking was performed. Hays et al. (2016) agreed that member checking as a data collection strategy maintains quality in the research for which the participants provide data validation. Member checking not only provides credibility, reliability, and trustworthiness, but it also gives participants the chance to verify their contributions, such as thoughts and ideas (Simpson & Quigley, 2016). According to Smith and McGannon (2018), member checking is a crucial technique in acquiring credibility, controlling bias, and producing trustworthiness. A summary of the transcripts data interpretation/analysis was sent to the participants for verification and validation of the data collected, which in turn increased the study's credibility and reliability while reducing the researcher's bias.

Data Organization Techniques

Data organization is essential to facilitate analysis and query of the data. To organize and query the data, Excel was used as a data analysis tool to review audio recordings, documents, and transcripts. Data organization started with interview audio recordings, which were reviewed, analyzed, and organized by themes. The interview recordings were transcribed into Microsoft Word, and the responses captured on the transcripts were added into Excel. Using Excel, information from was entered, reviewed, and analyzed.

The raw data will be kept in a locked container for five years, then destroyed. According to Lin (2009), data must be kept from three to ten years, but the researcher's sponsoring organization dictates the period the data should be kept; Walden University's policy is five years. Phillippi and Lauderdale (2018) encouraged researchers to store field notes (even if not used) and treat and protect them as the rest of the data collected. Tsai et al. (2016) reiterated that field notes, interview transcripts, audio/video recording contain sensitive data (participants identification) and needs to be protected from disclosure. The electronic data will be stored in an encrypted or password-protected hard drive/flash drive. They will include interview recordings, any personal thought notes, and all related data collection material used. Lin (2009) stated that all raw data needs to be collected, including sensitive information (names, locations, etc.) about the participants that, if disclosed, could compromise their confidentiality.

Data Analysis Technique

The data analysis technique used was methodological triangulation to perform thematic analysis. The thematic analysis focuses on extracting emerging themes from the raw data (Castleberry & Nolen, 2018). P. Fusch et al. (2018) described methodological triangulation as a cross method or using one method with multiple data sources, such as interviews, observations, field notes, and document analysis, among others. The use of methodological triangulation (using different data collection sources) helped me confirm the results from the research (Bengtsson, 2016). Also, triangulation increases research trustworthiness, especially when using tools to analyze the data (Leech & Onwuegbuzie, 2008). Publicly available documents such as those found online related to cybersecurity strategies to protect PHI from cyberattacks when using telemedicine were reviewed.

Data analysis started after the data had been collected. The thematic data analysis process is broken down into six phases: (a) becoming acquainted with the data, (b) creating codes of the raw data, (c) searching themes, (d) reviewing themes, (e) defining and naming themes, and (f) generating a report (Nowell et al., 2017). After immersing myself in the data and listening to keywords that may constitute or become a theme, notes were made for coding emerging themes. Participants' responses were reviewed, and all recordings were listened to, including a read over the personal thoughts' notes, and use publicly available documents. During the data review for analysis, codes were created, noted repeating themes, and assigned a name before findings were presented.

There are specialized tools such as computer-assisted qualitative data analysis software (CAQDAS), NVIVO, and ATLAS. Also, there are familiar/common office programs like Microsoft (MS) Word and Excel, which can be used for data analysis as well, such as coding the data with conditional formatting (Gasigwa et al. (2022). Dhakal (2022) suggested that NVIVO is efficient, accurate, and a reliable tool. Excel was used to store interview responses, digital recordings, transcripts from MS Word, and publicly available documents, which were used for coding and identifying themes. Excel was a great tool that assisted with data analysis, as it helped create code for analysis of the data.

Once the interviews were transcribed, the data was revised and analyzed. The data was labeled by using the Microsoft Word functionality of highlighting and writing comments of the terms and phrases that aligned with the interview questions. Those labels became codes that were used to extract themes that emerged from the data. All themes were addressed and considered how they might bring insight to answer the research question. A focus on reviewing key themes identified in Excel software was found while reviewing the data from those repeating terms or patterns. Key themes were used to begin data interpretation.

Reliability and Validity

In qualitative studies, reliability and validity refer to the study's trustworthiness by enhancing dependability, credibility, transferability, and confirmability of the findings. Those criteria were established in 1985 and are used by most qualitative researchers to achieve reliability and validity in their studies (Connelly, 2016). Cypress (2017) argued that reliability and validity are essential to qualitative research to the point that it should be used constantly to meet the research requirements. Likewise, Colorafi and Evans (2016) suggested that attaining reliability and validity is vital to qualitative research. Hadi and Closs (2016) described member checking "as the single most important method" to establish reliability in qualitative research. Reliability denotes that the study process is consistent among all participants, and dependable that can be audited (Colorafi & Evans, 2016). Validity and reliability were accomplished by using triangulation, which means using a variety of data sources.

Dependability

Dependability refers to obtaining the same results so the study can be replicated. Crowe et al. (2015) stated that dependability is gathering enough information during data collection and analysis, so the research is consistent. Dependability could produce trustworthy findings by participants reviewing the data collected and data interpretation (McInnes et al., 2017). I provided the transcript analysis from data collection to participants to ensure the data was consistent with their responses and the data interpretation. Furthermore, Amankwaa (2016) suggested that dependability rests on demonstrating that the findings can be replicated.

Credibility

Credibility refers to internal validity, which in this qualitative study included the methodological triangulation technique, to ensure the data has true value to the study. FitzPatrick (2019) argued that researchers need to use a minimum of one triangulation technique to increase the credibility of the findings and reduce the researcher's bias. Likewise, Korstjens and Moser (2018) describe credibility as the equivalent of internal validity, which focuses on the truth-value. Furthermore, the researcher's consistency enhances credibility, but it must be verified by a triangulation technique of the data (Santiago-Delefosse et al., 2016). Similarly, Gunawan (2015) claimed that member checks are fundamental to obtaining credibility. By using methodological triangulation techniques, the research study will bring internal validation and increase its credibility.

Transferability

Transferability, also known as generalizability, refers to external validity and the relevance the results are to others outside the study. Moon et al. (2016) referred to transferability as a form of external validity in which one's study findings can be useful for future research. Bengtsson (2016) expressed transferability as in the way the findings apply to other situations, indicating that the accuracy of the sample would define how general the findings could be. Likewise, Leung (2015) suggested that transferability should use methodical sampling and triangulation. Moon et al. (2016) added that transferability might be fundamental to the application of research findings.

Transferability in this study was accomplished by using purposeful sampling and member checking, a triangulation technique.

Confirmability

Confirmability refers to the proof the researcher gives the readers that the study's results mirror the participants' perceptions, not the researcher's worldviews. Castleberry and Nolen (2018) stated that confirmability assures the findings come from the data, not from one's biases. Sarma (2015) argued that triangulation guarantees confirmability and diminishes the researcher's bias. Likewise, McInnes et al. (2017) indicated that one obtains confirmability when the findings truthfully echo the data provided by participants. McInnes et al. (2017) go on to say that by using multiple sources of triangulation, the researcher can accomplish confirmability. Consequently, by relying on the data participants bring to the study and using methodological triangulation, confirmability was obtained. In this study, confirmability was obtained through methodological triangulation (interview, member checking, and document revision) to ensure results emerge from the data.

Data Saturation

Data saturation is essential to the quality of the research. P. I. Fusch and Ness (2015) stated that if data saturation is not reached, it affects the quality of the study. Galvin (2015) conducted a study to find out when data saturation was reached using interviews as a data collection instrument. Although Galvin concluded that in twelve interviews, most of the data saturation occurred, new themes ceased emerging after the 30th interview. Nevertheless, P. I. Fusch and Ness (2015) suggested that if no new data appears or there is no more coding necessary, the researcher has reached data saturation. Similarly, Saunders et al. (2018) described data saturation when new data becomes redundant to the already collected data. Once the data being collected renders the same information or does not render latest information, data saturation was reached.

Transition and Summary

Section two focused on the role the researcher has with participants and included more details about the research method and described the research design used, to include defined data collection instruments, and the population. Also, section two included ethical considerations that were present during the research and interaction with participants to include their protection. Likewise, it included the role the participants have of checking/verifying the data to increase the reliability and validity of the study.

Section three covers the application to the professional practice of IT, which comprises of the presentation of the findings and the relevance to IT, the implications for social change, and the positive and tangible impact on society, individuals, and cultures. Also, section three contains recommendations for those that relate to the findings, as well as recommendations for future research. Some items addressed in section three include the researcher’s reflection and finalizing with a conclusion; appendices are also included in this section as well.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative pragmatic research was to explore the effective strategies that IT managers in the healthcare industry used to protect their customers' PHI from cyberattacks when using telemedicine. Data was collected using semistructured interviews from IT managers. Participants were recruited through social medial LinkedIn invitation. The data collected was obtained from seven IT managers responses to ten open-ended questions listed in the interview questions appendix (Appendix A) and data from five publicly available online documents in the United States were used to complement and strengthen the study's results. Those documents were identified with a letter and number combination (i.e., D1 - D5). Likewise, participants were assigned a letter-number combination to maintain participants' anonymity, such as P1, P2, P3, etc.

Most interviews were conducted via Microsoft Teams or phone, according to participants' availability. Excel was used to analyze the data collected, then, the data was sent for member-checking process to validate data analysis. During member checking, participants' responses were clarified. Their responses provided deep insights into answering the overarching research question. The findings showed that IT managers used many strategies to protect customers' PHI from cyberattacks. The thematic analysis conducted using Excel identified major themes that emerged throughout the data analysis of the research. Data collection evidence showed Risk Management Framework and Protection from Unauthorized Disclosure as the main themes and key strategies to protect customers' PHI. I was able to link those major themes back to the framework and literature review.

Presentation of Findings

The overarching research question was "*What effective strategies do IT managers in the Healthcare industry use to protect their customers' PHI from cyberattacks when using telemedicine?*" Data was collected data from seven IT managers, utilizing semistructured interview questions to gain deep insight into the topic studied, and incorporated publicly available online documents from Organizations such as, NIST, NIH, HHS, to increase data validation. This section includes tables and figures to aid with data visualization of the insight gathered from the IT managers and identifies each theme. Table 1 shows the publicly available documents that reinforce data validation.

Table 1

Publicly Available Documents

Document number	Title	Author
D1	*Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide*	National Institute of Standards and Technology (NIST)
D2	*Healthcare and Cybersecurity Taking a Zero Trust Approach*	National Institutes of Health (NIH)
D3	*Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*	Health and Human Services (HHS)
D4	*Privacy and Security Risk Factors Related to Telehealth Services – A Systematic Review*	National Institutes of Health (NIH)
D5	*Mitigating Cybersecurity Risk in Telehealth Smart Home Integration*	National Institute of Standards and Technology (NIST)

Table 2 below shows the number of references regarding the two main themes that emerged during data collection.

Table 2

Main Themes

Main themes	Participants		Document	
	No. of Participants	No. of references	No. of Documents	No. of references
Risk management	7	31	3	67
Protection from unauthorized disclosure	7	19	2	4
Cybersecurity awareness training	4	8	3	84
Privacy	3	6	5	104
Data-loss prevention	2	3	2	18

Theme 1: Risk Management

During the thematic analysis risk management emerged as the most mentioned theme; a key theme across the data collection thematic analysis, among all seven participants. Findings confirmed that risk management is an essential aspect for organizations that want to protect their resources/assets and procedures from cybersecurity attacks. All participants, apart from P2, stressed out that risk management plays a key role in multiple aspects of the strategies to protect customers' PHI from cyberattacks. Although P2 mentioned the use of risk management strategies, it did not consider them a key aspect in the strategies to protect customers' PHI from cyberattacks. P1 and P3 identified risk management as an essential framework in today's evolving threats. P3 added and P7 conveyed risk management strategies such as "*ensuring end-to-end device management and robust patching is the primary tool in preventing the cyberattacks.*" P2 and P5 emphasized patient awareness and involvement in addressing risk from the customers' perspective. P3, P4, and P6 utilized security, test, and evaluation strategies to protect PHI against cyberattacks. P3 factors in "*the history of reported breaches or detected breaches*" and verified their effectiveness, along with evaluating the security tools performance. P4 shared "*perform Pen Test to verify the performance of our security controls*". P6 reviews and compares the number of security incidents for security events that occurred over a year to assess their security posture. P2 stated the "*implementation of multi-factor authentication for providers as well as for all patients who have online accounts with the provider. This is one of the simplest and most powerful actions providers can take to boost cybersecurity and minimize the risk of cyberattacks*. Many participants mentioned the use of the NIST Framework as part of their strategies to protect PHI from cyberattacks. Some of the NIST framework aspects participants were referring to are the NIST guidelines and tools. P6 shared that the use of the NIST guidelines combined with cybersecurity tools framework provide PHI protection while supporting each other. Some cybersecurity strategies P3 pointed out to make them less vulnerable are vulnerability management and following the NIST traceable guidelines.

Publicly available documents confirmed the findings about the significance of implementing a risk management framework or processes to protect customers' PHI from cyberattacks. D1 provides HIPAA Security Rule guidance about risk assessment, risk management, and information security program activities. D1 emphasizes Theme 1 and validates P2 response and the importance of a HIPAA compliance cybersecurity program. D3 reaffirms the evolving cybersecurity threats the healthcare industry faces, states the essence of risk management, and explicitly addresses best practices. D3 describes threats and vulnerabilities, as well as offering solutions to the industry.

Thes findings align with the risk management theme found in the research, which describes risk management best practices, processes and actions taken to address risk in the organization to protect its resources. Arogundade et al. (2021) studied the risk management process to identify critical information, security risks, and control measures. Researchers like Pal and Mukhopadhyay (2018) measured how risk analysis and assessment identify attack types, and Muraguri et al. (2019) included the risk management theory in their research and included assessment, evaluation, and mitigation in their studies.

The IST conceptual framework showed a risk management theme exemplified by the risk management theory discussed by Hong et al. (2003). The risk management theory describes the risk management process in its entirety, evaluating, assessing, and controlling risk within an organization (Fikri et al., 2019). Poleto et al. (2021) said that when using telemedicine, risk management encompasses policies/procedures, setting up a baseline, assessing risk, and event notifications. These activities were found in the data collected from P4, P5, and P6, which indicated in their response to cyberattacks the first action taken would be to stop the attack or contain the incident.

Theme 2: Protection From Unauthorized Disclosure

Protection from unauthorized disclosure was the second main theme that emerged during the thematic analysis. This theme was found in the analysis eighteen times and similarly to the first theme, it was visible among all seven participants as well, except for

P1 and P5 that were the least to use this strategy related to this theme. This theme's importance resides on the ability for the Healthcare Industry to "*strike a balance between confidentiality, integrity, and availability*," as P6 shared. There are many strategies that can be applied to protect customers' PHI, but not all of them are adequate. P3 mentioned zero trust to minimize unauthorized disclosure, because zero trust is based on a least privileged principle. P4 said "*effectiveness vs. Baselines*" referring to factors and the industry standards; also, incorporating lessons learned into organization policies/documentation. Unauthorized disclosure could occur from internal or external sources, what is important is to keep protecting the data to the best of our abilities and resources, P7 accomplishes this by having physical security controls, inventory management, and robust patching. P7, like P6, employs CIA triad strategies to protect PHI from cyberattacks; P7 reinforced *"to ensure the confidentiality, integrity and availability (CIA) of data and systems is maintained".*

Publicly Available documents support the findings about the importance of protecting data from unauthorized access, thus protecting customers' PHI from cyberattacks. D2 addresses data protection from cyberattacks in the healthcare industry, focusing on Zero-Trust, a strategy that functions in the principle of never trust-always verify to protect the data. D2 strengthens Theme 2 by offering strategies applicable to the healthcare industry that IT managers and readers alike can use as guidance and implement as protection from unauthorized disclosure. Furthermore, P3 confirms the key aspects of Theme 2 and reinforces D1 statements regarding access control and the least privilege, which are necessary strategies to protect customers' PHI against cyberattacks.

P3 shared that "*Key one, is principle of least privilege, making sure the users have the least amount of privilege necessary to accomplish their job and not expose greater risk than is necessary*".

Theme 2, protection from unauthorized disclosure, is directly in line with the research. Bandari (2023) pointed out the criticality of this theme; Bandari wrote in his study regarding preventing unauthorized access, the use of access control strategies, and its effectiveness to protect data from unauthorized disclosure. Moreover, Bandari (2023) stated that access control is "one of the most effective tools" to prevent data breaches, which coincided with P3 assertions. Basil et al. (2022) studied the security concerns or issues of health information databases including telemedicine; in their research they stated that the implementation of access controls increases the protection from unauthorized disclosure and potentially prevents data breaches. Some key factors Basil et al. (2022) investigated were privacy and security breaches (i.e., using third-party software), which consequently impact data confidentiality. Confidentiality is a concern that P7, P6, and P2 shared; all three participants expressed the importance of this factor with this theme, protection from unauthorized disclosure, and suggested that cybersecurity program, policies, and systems maintenance along with HIPAA compliance, would reduce the risk of data breaches.

Likewise, Theme 2, protection from unauthorized disclosure, can be observed through the conceptual framework, security policy theory developed by Hong et al. (2003). The security policy theory addresses protection from unauthorized disclosure by establishing, implementing, and maintaining information security policies to meet organizational requirements. Zaini et al. (2020) supports this Theme through elements of the conceptual framework, security policy theory and contingency theory, such as access control (physical/network), system maintenance, and business continuity; agreeing with P6 in utilizing security policy theory elements to protect from unauthorized disclosure, but if an attack occurs, switch to a response mode and "*make sure that it's cut off*". Butt et al. (2023) discussed the use of security strategies to secure customers' data and protect it from unauthorized access, by focusing on data confidentiality applying security control mechanisms.

Theme 3: Cybersecurity Awareness and Education

The third theme that emerged was cybersecurity awareness and education. This theme was found in data analysis eight times. cybersecurity awareness and education theme consist of enhancing employees' understanding to recognize potential cyberattacks, thus reducing organizational risk (Pranggono & Arabo, 2021). Theme 3 extant among four of our participants (P1, P3, P4, and P6), which emphasized the significant role cybersecurity awareness and education plays for personnel. P1 mentioned that personnel that are professionally trained could lead to an insider threat issue. P3 shared that the training must be required and teach personnel to recognize PHI/PII, identify threats, and respond accordingly. P4 explained the types of threats experienced that users should be able to recognize, such as phishing attacks and social engineering. P6 said regarding education to end users "*providing them real examples of tangible things that they can do to help protect the people*". P2 and P3 excerpts about engaging customers in cybersecurity practices were unexpected and provided insight and a different point of view on strategies used to protect PHI. Normally, the focus is on the implementation of cyber awareness for organizations' employees, but very seldom is presented the idea of educating customers regarding cybersecurity practices, threats, and vulnerabilities, including risk and their acceptance. P2 shared to implement the practice of multifactor authentication for providers as well as for all patients, as part of the strategies to protect customers' PHI against cyberattacks. Another excerpt about engaging customers in cybersecurity practices was from P3, which commented on explaining customers and making sure they understand the potential cybersecurity risks that a telemedicine connection may pose. This suggests that although cybersecurity awareness and education theme appeared eight times, it maintains its relevancy and key to an organization's security posture.

Publicly available documents reinforced Theme 3, cybersecurity awareness and education. D4 identified cybersecurity awareness and education as a risk factor to telemedicine's privacy and security, making it a key aspect in the healthcare industry and requirement for the training to include telemedicine security related training. D3 strengthens this theme, cybersecurity awareness and education, by showing the impact and consequences of the lack cyber training could bring to an organization, such as lack of training in protecting PHI, resulting in loss of the PHI, which translates into monetary loss to organizations. Awareness and training, as D1 refers to Theme 3, demonstrates the intricacy of the cybersecurity awareness and education theme activities, such as developing, implementing, incorporating training reminders, as well as monitoring and evaluating the training plan.

Theme 3 was found in the literature on multiple articles that presented the importance of this theme. The literature regarded cybersecurity awareness as a factor in reducing organizational risk to cyberattacks (Pranggono & Arabo, 2021). Also, the literature showed impacts on the organization's cyber posture and increasing of the chances of cyberattacks due to gaps in cybersecurity awareness and education, in areas like social engineering (Chanti & Chithralekha, 2022) and phishing (Aldawood & Skinner, 2019). Niki et al. (2022) mentioned that a cyber awareness and education integrated approach is necessary in the healthcare industry. Niki et al. (2022) study identified cybersecurity awareness and education falling short among IT professionals and indicating the need of improvement and suggested the use of multiple methods from formal university training, simulator, to gamification to increase cyber posture in the organization.

Cybersecurity awareness and education, Theme 3, can be linked back to the IST conceptual framework through the control and audit theory. The control and audit theory focuses on information security control systems and audit procedures to measure the control's performance. Also, the control and audit theory increase an organization's cyber posture by implementing network control over assets and managing risk of the resources protecting them from internal threats. This includes cyber awareness training and education to complement access control (Bratu, n.d.).

The thematic analysis included three themes, cybersecurity awareness and education, privacy, and last data-loss prevention. These three themes were originally considered potential major themes from the research, but findings from data collection analysis identified them as themes due to the scarcity of their appearance in the data.

Theme 4: Privacy

The second theme that appeared was Privacy. This theme emerged seven times during data analysis. Privacy was mentioned among three participants in the study validating Privacy as a concern. P6 commented "*making sure no one can listen in on the conversation…where the clinician is sitting physically that means that needs to be private as well*". P2 discussed many strategies to protect customers' PHI from cyberattacks, which were focused on maintaining "*patient confidentiality and privacy for their information*". Similarly, P5 shared "*prevent exposure…by obfuscation*", "*consider the nature of the data and the legal aspects of how that data is supposed to be managed*" "Despite Privacy showing in the analysis little, the emphasis given by these participants worth noting it.

D4 emphasizes theme 4 by delineating privacy in Telehealth and points out three aspects, the environment that includes the lack of private spaces, which validates P6 concerns regarding the location where clinicians are physically sitting, a space where no one can listen to the conversation. The technological aspect, such as data security, uses mechanisms to protect and limit access to the data by encryption and authentication methods. And the operational aspect of privacy, involving access to technology and training of the users by educating the users to recognize privacy issues and respond accordingly, as well as protecting the data. D1 supports P5 earlier excerpts by stating the Health Insurance Portability and Accountability Act (HIPAA) security rules on protecting

PHI; requiring administrative, technical, and physical safeguards that must be in place to protect the privacy of PHI. Moreover, D1 refers to NIST special publications related to privacy in the NIST risk management framework.

The literature showed this fourth theme, privacy, which denotes the right to PHI protection (Alfawzan et al., 2022); privacy is about limiting what others are allowed to see, employing security mechanisms when using, sharing, and managing sensitive data to protect it (Basil et al., 2022). Bai et al. (2022) reiterated that telemedicine risk exposure of PHI have increased due to poor privacy practices/controls; this supports P5 excerpt when said "*prevent exposure*". We find the literature supporting this theme, Al-Muhtadi et al. (2019) indicated that Privacy is essential to telemedicine. Alqurashi et al. (2023) confirm privacy of PHI as one of the biggest concerns in telemedicine. The literature demonstrates a direct connection to this theme and exemplifies what was shared by the participants.

Theme 4, privacy, aligns with the IST framework Management System Theory, which establishes an information security management system that governs and safeguards information assets. Also, privacy aligns with the Security Policy Theory as well, which focuses on protecting PHI from internal/external threats by applying security policies and procedures across the organization to meet security requirements. Both theories support this theme in similar ways. The management system theory reinforces privacy using a system to control and safeguard information, PHI in this case. And the security policy theory supports this theme by implementing and maintaining security tools to enhance data protection using technical mechanisms such as having security policies in place.

Theme 5: Data-Loss Prevention

The least theme to make appearance was Data-Loss Prevention (DLP). This theme was the least mentioned by two participants during the analysis of the data collected, and it emerged twice during thematic analysis. Findings showed a connection to the DLP theme activities. DLP consists of the use of implemented countermeasures to prevent or reduce the potential of data being compromised by cyberattacks. DLP activities involve encryption, monitoring network and email for sensitive information, and blocking action mechanisms. P2 emphasized that "*monitoring for suspicious activity and ensuring data integrity*" protects PHI from cyberattacks, taking an initiative-taking approach and using automated tools for data protection. Likewise, P5 shared that the use of "*system hardening and encryption*" strategies help in the protection of PHI from cyberattacks, another initiative-taking and automated approach to data protection. Here we can appreciate two different participants with different strategies but with the same outcome: protecting PHI data through automation and an initiative-taking posture.

Publicly available documents such as D3 confirm Theme 4 by stressing DLP importance due to the cyberattacks that the healthcare industry has encountered such as phishing attacks, ransomware attacks, and data-loss due to internal and external threats. D3 encourages readers to use DLP tools to aid in the protection of data to detect and block PHI and PII leaving an organization. D2 stated that in the healthcare industry an integrated approach is required to protect data, utilizing Zero Trust combined with users' initiative-taking approach towards DLP, validating P2 and P5 excerpt of monitoring data and activities, and hardening and encrypting the systems and data.

The literature confirms the strategies found in this theme, even though the appearance of DLP was scarce. The findings align to the literature statements from Javaid et al., (2023) that used multifactor authentication to ensure the right access was granted to the right person. Herrera Montano et al. (2022) described how encryption in DLP protects PHI, in the healthcare industry, and added that an integrated approach including biometrics as a multifactor authentication method increases data protection. Grayson et al. (2023) study pointed out that DLP improves PHI protection by using encryption and multifactor authentication as shown by the findings. F. Khan et al. (2021) confirmed this theme by emphasizing data at rest and in-transit protection for PHI.

Findings showed the importance of authentication methods, such as multifactor authentication, training, security audits, and encryption for data in-transit, as well as securing data-at-rest, are factors found in the control and audit theory from the IST conceptual framework. The control and audit theory factors include information security controls and audit control, network monitoring to protect assets and resources, and cyber awareness training to make employees aware of threats.

Application to Professional Practice

The goal of this study was to explore cybersecurity strategies used to protect PHI against cyberattacks when using telemedicine. The strategies from this study's findings can benefit IT managers in the application of cybersecurity and risk management frameworks by utilizing an integrated data protection approach that includes security mechanisms, while keeping a balance between confidentiality, integrity, and availability (CIA) to protect PHI. Those strategies described in the presentation of the findings relate to the review of the literature and the analysis of the conceptual framework. This study results bring insight into the strategies IT managers use to protect PHI against cyberattacks and aspects of those strategies that could improve IT practice. The use of NIST cybersecurity and risk management frameworks is a critical aspect of any industry to define security controls policies and procedures to navigate the ever-evolving practice of IT, especially in the healthcare industry to help protect PHI.

Those two frameworks, which include security controls and mechanisms, combined with a balance of the CIA triad principles, produce an integrated approach to protect PHI against cyberattacks. Among the strategies found within the cybersecurity framework included the use of analytical tools to identify, assess, and mitigate risk. The security controls/mechanisms, such as encryption, multifactor authentication, network, and email monitoring, and blocking actions, were found to be critical in the protection of PHI against cyberattacks. The strategies found within the risk management framework encompassed policies, plans, and processes to evaluate the effectiveness and efficiency of systems to address their risks in organizations. Among the strategies found within the risk management framework included establishing vulnerability management, risk assessment, the periodic (i.e. annually) maintenance of policies by reviewing and updating the policies, such as cyber awareness training policies, security policies, and control policies, event notification, and incident response procedures; those activities reduce the risk of successful cyberattacks. This study's findings demonstrate real-world activities the healthcare industry experiences on any given day, and they shine insight into the strategies IT managers can utilize to protect PHI against cyberattacks. As well as extending the knowledge in this discipline by contributing to the cybersecurity body of knowledge, bringing in customers' worldviews, by engaging customers in cybersecurity practices such as cyber awareness training, risk management and acceptance.

Implications for Social Change

This study's implication for positive social change provides tangible improvements to IT managers and IT community, the healthcare industry, organizations, and society. The cybersecurity strategies included in this study are a practical guide that can be applied by IT managers and the IT community to reduce the risk of PHI exposure from cyberattacks, measuring the reduction in risk, by analyzing historical data showing the security measures have reduced the likelihood for PHI exposure. Tracking and measuring the detection and incident response times, noting how and what have reduced (i.e., time or numbers of incidents). Monitoring, tracking, and reporting compliance metrics such as monitoring of Data-Loss prevention events, data breaches and unauthorized access/disclosures, and tracking the number of threats that have been blocked.

The implication for positive social change at the organization's level, can be accomplished by implementing policies and encouraging a secure cyber posture, measuring the effectiveness of cyber awareness training, preparing employees in recognizing threats and responding to them. Also, by looking at the business side of organizations and demonstrating lower costs associated with downtimes and data breaches, as well as quantifying the reduction in downtime, loss of productivity (network outages), and gauging the effectiveness of the processes that are in placed requiring cyberattacks identification, response, and mitigation activities.

The implication for positive social change in society is palpable by the increase in the use of telemedicine (the technology) and broad implementation acceptance as a standard, decrease in cyber incidents reports, educating customers/the public, an improvement of individuals' quality of life, the availability of the technology and the potential of saving lives at remote locations where response time can make a difference between life and death, and this study that can be used as a guide to raise cybersecurity awareness in society/community and provide strategies on possible approaches to secure PHI.

Recommendations for Action

The intent of this qualitative pragmatic inquiry was to explore cybersecurity strategies IT managers use to protect PHI from cyberattacks when using telemedicine. This study's findings demonstrate that IT managers could benefit from the implementation of an integrated approach to data protection that includes cybersecurity strategies such as risk management and security mechanisms such as encryption and access control to protect sensitive data from unauthorized disclosure, reducing the risks of PHI exposure. Also, maintaining a balance between cybersecurity strategies and the CIA triad. This study's findings were supported by publicly available documents, scholarly research articles, and cybersecurity strategies shared by experienced IT managers in the U.S. that participated in the study.

IT and Cybersecurity are evolving. IT managers should be actively engaged in keeping abreast of modern technologies and ways to foster a learning environment applicable to end-users, IT staff, and customers. Starting with ensuring all personnel receive cyber awareness training and education baseline to recognize threats. Provide more in-depth training for IT staff according to their role. Also, make available relatable cyber awareness training for customers in their home environment to include mobile security. This study's findings showed the importance of cyber awareness training and education, its role in preventing unnecessary risk, and its consequences for reducing insider threats, which is a concern for any organization.

A way IT managers can accomplish acting on these strategies is dissemination of the information to the lowest level of personnel, using web announcements, posters, marketing materials or campaigns, tabletop exercises/training with role play, gamification, being creative, thinking outside the box, engaging employees and customers alike; knowing their audience to deliver an effective approach to the strategies that they want to use; not everyone's learning ability is the same.

Recommendations for Further Research

The findings from this pragmatic inquiry study determined that the cybersecurity strategies shared by the seven IT managers, who use them on daily basis and that participated in this study, were adequate to protect PHI from the ever-evolving threats in cybersecurity. Recommendations for further research consist of:

1. Amplify qualitative or mixed methods research approach on the cybersecurity topic to protect PHI/PII, considering Artificial Intelligence (AI) involvement, business, and benefits.
2. Conduct research focusing on data protection in transit with the use of mobile devices and how wireless technology improves or increases risk in an organization.
3. Research into customers' engagement into cybersecurity awareness training and education, the benefits it brings to the organization's cyber posture, and the impact on society.

Reflections

Looking back, this was a journey that I never thought of travelling on. This Doctor of IT (DIT) program was full of challenges that questioned my knowledge and experience in the subject on many occasions. I learned to view and discuss topics and issues through scholarly lenses; the impact this doctoral program was having over my life was permeating my personal life, I was suddenly more understanding, more open to others point of views, and responding accordingly. Also, in my professional life as well, carrying discussions, writing documents, or even a simple email contained an air of scholarly tone.

This DIT journey helped me grow on personal, educational, and professional levels. My study focused on exploring cybersecurity strategies to protect PHI from cyberattacks when using telemedicine; my experience with cybersecurity gave me the preconceived idea that data-loss prevention (DLP) would be a major topic/theme emergent during the thematic analysis. The lack of excerpts related to DLP found during thematic analysis took me by surprise given the study's focus on strategies to protect data.

Nevertheless, the experience of conducting this study and connecting with the study participants was a humble and educative experience. I am grateful for their participation, sharing their experiences brought into insight into the topic and data protection, as well as shining a light on a points seldomly looked at by the customer. The participants were happy I was looking into the subject due to the lack of research on the topic and that they were able to contribute by sharing their experiences.

Conclusion

Cyberattacks occur every day and each time they are more elaborate. It is crucial for IT managers/cybersecurity professionals to stay abreast of the innovative technologies at the fast pace they are emerging and to be initiative-taking in finding new ways to protect sensitive data, such as PHI, against cyberattacks. The use of the IST framework as a roadmap to protect PHI is an effective approach, given that not all cyberattacks are the same. This study showed that utilizing a combined/integrated approach addresses risks and threats from different perspectives, as well as established policies and processes for organizations to lower the risk of cyberattacks. Furthermore, creating and maintaining a balance between cybersecurity and the CIA triad was an important aspect for the operations of any organization.

References

Ackerman, B., Lesko, C. R., Siddique, J., Susukida, R., & Stuart, E. A. (2021). Generalizing randomized trial findings to a target population using complex survey population data. *Statistics in Medicine*, *40*(5), 1101–1120. https://doi.org/10.1002/sim.8822

Adashi, E. Y., Walters, L. B., & Menikoff, J. A. (2018). The Belmont Report at 40: Reckoning with time. *American Journal of Public Health*, *108*(10), 1345–1348. https://doi.org/10.2105/AJPH.2018.304580

Ahmed, M. A., Sindi, H. F., & Nour, M. (2022). Cybersecurity in hospitals: An evaluation model. *Journal of Cybersecurity and Privacy*, *2*(4), 853–861. https://doi.org/10.3390/jcp2040043

Akerblad, L., Seppanen-Jarvela, R., & Haapakoski, K. (2021). Integrative strategies in mixed methods research. *Journal of Mixed Methods Research*, *15*(2), 152–170. https://doi.org/10.1177/1558689820957125

Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. *Future Internet*, *12*(10), 1–39. https://doi.org/10.3390/fi12100168

Alabdulatif, A., Khalil, I., & Saidur Rahman, M. (2022). Security of blockchain and AI-empowered smart healthcare: Application-based analysis. *Applied Sciences*, *12*(21). https://doi.org/10.3390/app122111039

Alawonde, K. (2020). *Tailored information security strategies for financial services companies in Nigeria* [Doctoral dissertation, Walden University]. Walden University ScholarWorks. https://scholarworks.waldenu.edu/dissertations/8662/

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, *11*(3), Article 73. https://doi.org/10.3390/fi11030073

Alfawzan, N., Christen, M., Spitale, G., & Biller-Andorno, N. (2022). Privacy, data sharing, and data security policies of women's MHealth apps: Scoping review and content analysis. *JMIR MHealth and UHealth*, *10*(5), 1–14. https://doi.org/10.2196/33735

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences*, *11*(8), 1–38. https://doi.org/10.3390/app11083383

Aligarh, F., Sutopo, B., & Widarjo, W. (2023). The antecedents of cloud computing adoption and its consequences for MSMEs' performance: A model based on the Technology-Organization-Environment (TOE) framework. *Cogent Business & Management*, *10*(2), 1–17. https://doi.org/10.1080/23311975.2023.2220190

Al-Muhtadi, J., Shahzad, B., Saleem, K., Jameel, W., & Orgun, M. A. (2019). Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment. *Health Informatics Journal*, *25*(2), 315–329. https://doi.org/10.1177/1460458217706184

Alqurashi, H., Mohammed, R., AlGhanmi, A. S., & Alanazi, F. (2023). The perception of health care practitioners regarding telemedicine during COVID-19 in Saudi

Arabia: Mixed methods study. *JMIR Formative Research*, *7*, 1–16. https://doi.org/10.2196/47065

Alshammari, Z. (2020). What is data loss prevention? *ISSA Journal*, *18*(11), 23–28. http://www.issa.org/?page=ISSAJournal

Alsyouf, A., Lutfi, A., Alsubahi, N., Alhazmi, F. N., Al-Mugheed, K., Anshasi, R. J., Alharbi, N. I., & Albugami, M. (2023). The use of a technology acceptance model (TAM) to predict patients' usage of a personal health record system: The role of security, privacy, and usability. *International Journal of Environmental Research and Public Health*, *20*(2), 1–24. https://doi.org/10.3390/ijerph20021347

Amankwaa, L. (2016). Creating protocols for trustworthiness in qualitative research. *Journal of Cultural Diversity*, *23*(3), 121–127. Retrieved from Walden University Library databases. https://research.ebsco.com/c/4wdw3l/viewer/pdf/gd2rrhe6f5

Ansari, D. B., & Khaliq, M. (2022). A proposed multilayered framework for security and privacy in big data. *International Journal of Computer Applications*, *184*(3), 20–31. https://doi.org/10.5120/ijca2022921989

Arogundade, O. T., Folashade, M., Oluwafolake, O., Yetunde, A. C., & Igbe, T. (2021). Critical factors affecting the efficiency of information security risk management in business organization: An empirical study. *Covenant Journal of Informatics & Communication Technology*, *9*(1), 1–18. https://www.researchgate.net/publication/356603938

Asenahabi, B. M. (2019). Basics of research design: A guide to selecting appropriate research design. *International Journal of Contemporary Applied Researches*, *6*(5), 76–89. http://www.ijcar.net/

Asiamah, N., Mensah, H. K., & Oteng-Abayie, E. F. (2017). General, target, and accessible population: Demystifying the concepts for effective sampling. *The Qualitative Report*, *22*(6), 1607–1622. https://doi.org/10.46743/2160-3715/2017.2674

Aspers, P., & Corte, U. (2019). What is qualitative in qualitative research? *Qualitative Sociology*, *42*(2), 139–160. https://doi.org/10.1007/s11133-019-9413-7

Bai, P., Kumar, S., Kumar, K., Kaiwartya, O., Mahmud, M., & Lloret, J. (2022). GDPR compliant data storage and sharing in smart healthcare system: A Blockchain-based Solution. *Electronics*, *11*(20), 1-20. https://doi.org/10.3390/electronics11203311

Bandari, V. (2023). Enterprise data security measures: A comparative review of effectiveness and risks across different industries and organization types. *International Journal of Business Intelligence and Big Data Analytics*, *6*(1), 1–11. Retrieved from https://research.tensorgate.org/index.php/IJBIBDA/article/view/3

Bano, J., Jabeen, Z., & Qutoshi, S. B. (2018). Perceptions of teachers about the role of parents in developing reading habits of children to improve their academic performance in Schools. *Journal of Education and Educational Development*, *5*(1), 42. https://doi.org/10.22555/joeed.v5i1.1445

Bansal, P., Smith, W. K., & Vaara, E. (2018). New ways of seeing through qualitative research. *Academy of Management Journal*, *61*(4), 1189–1195. https://doi.org/10.5465/amj.2018.4004

Basil, N. N., Ambe, S., & Ekhator, C. (2022). Health records database and inherent security concerns: A review of the literature. *Cureus*. *14*(10), 1-6. https://doi.org/10.7759/cureus.30168

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *NursingPlus Open*, *2*, 8–14. https://doi.org/10.1016/j.npls.2016.01.001

Bhattacharyya, P., & Pradhan, R. K. (2019). Exploring cherishing: A qualitative approach. *The Qualitative Report*, *24*(7), 1511-1536. Retrieved from https://nsuworks.nova.edu/tqr/vol24/iss7/2

Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S., Levy, M., Kedia, S., Dasgupta, D., & Dobalian, A. (2020). Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. *Journal of Medical Systems*, *44*(5), 98. https://doi.org/10.1007/s10916-019-1507-y

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research*, *26*(13), 1802–1811. https://doi.org/10.1177/1049732316654870

Blaikie, N. (2018). Confounding issues related to determining sample size in qualitative research. *International Journal of Social Research Methodology*, *21*(5), 635–641. https://doi.org/10.1080/13645579.2018.1454644

Bloomfield, J., & Fisher, M. (2019). Quantitative research design. *Journal of the Australasian Rehabilitation Nurses' Association*, *22*(2), 27–30. https://doi.org/10.33235/jarna.22.2.27-30

Boddy, C. R. (2016). Sample size for qualitative research. *Qualitative Market Research: An International Journal*, *19*(4), 426–432. https://doi.org/10.1108/QMR-06-2016-0053

Bratu, I. I. (n.d.). Information security risk audit in organizations. 1-4. Retrieved from https://www.theibfr.com/

Brear, M. (2018). Ethical research practice or undue influence? symbolic power in community- and individual-level informed consent processes in community-based participatory research in swaziland. *Journal of Empirical Research on Human Research Ethics*, *13*(4), 311–322. https://doi.org/10.1177/1556264618761268

Bruce, A., Beuthin, R., Sheilds, L., Molzahn, A., & Schick-Makaroff, K. (2016). Narrative research evolving: Evolving through narrative research. *International Journal of Qualitative Methods*, *15*(1), 1–6. https://doi.org/10.1177/1609406916659292

Busetto, L., Wick, W., & Gumbinger, C. (2020). How to use and assess qualitative research methods. *Neurological Research and Practice*, *2*(1), 14. https://doi.org/10.1186/s42466-020-00059-z

Butt, U. A., Amin, R., Aldabbas, H., Mohan, S., Alouffi, B., & Ahmadian, A. (2023). Cloud-based email phishing attack using machine and deep learning algorithm.

Complex & Intelligen t Systems, *9*(3), 3043–3070. https://doi.org/10.1007/s40747-022-00760-3

Candela, A. (2019). Exploring the function of member checking. *The Qualitative Report*, *24*(3), 619–628. https://doi.org/10.46743/2160-3715/2019.3726

Cardile, D., Corallo, F., Cappadona, I., Ielo, A., Bramanti, P., Lo Buono, V., Ciurleo, R., & De Cola, M. C. (2023). Auditing the audits: A systematic review on different procedures in Telemedicine. *International Journal of Environmental Research and Public Health*, *20*(5), 1-17. https://doi.org/10.3390/ijerph20054484

Cartwright, A. J. (2023). The elephant in the room: Cybersecurity in healthcare. Journal of Clinical Monitoring and Computing. https://doi.org/10.1007/s10877-023-01013-5

Caster, M. (2020). Policies and procedures in providing competent customer service in urgent care centers. *Open Journal of Business and Management*, *8*(3), 1164-1192. https://doi.org/10.4236/ojbm.2020.83075

Castleberry, A., & Nolen, A. (2018). Thematic analysis of qualitative research data: Is it as easy as it sounds? *Currents in Pharmacy Teaching and Learning*, *10*(6), 807–815. https://doi.org/10.1016/j.cptl.2018.03.019

Chai, K. Y., & Zolkipli, M. F. (2021). Review on Confidentiality, Integrity and Availability in Information Security. *Journal of ICT In Education*, *8*(2), 34–42. https://doi.org/10.37134/jictie.vol8.2.4.2021

Chanti, S., & Chithralekha, T. (2022). A literature review on classification of phishing attacks. *International Journal of Advanced Technology and Engineering Exploration*, *9*(89), 446–476. https://doi.org/10.19101/IJATEE.2021.875031

Chatfield, S. L. (2020). Recommendations for secondary analysis of qualitative data. *The Qualitative Report*, *25*(3), 833-842. Retrieved from https://nsuworks.nova.edu/tqr/vol25/iss3/17

Chellaiyan, V. G., Nirupama, A. Y., & Taneja, N. (2019). Telemedicine in India: Where do we stand? *Journal of Family Medicine and Primary Care*, *8*(6), 1872–1876. https://doi.org/10.4103/jfmpc.jfmpc_264_19

Chua, J. A. (2021). Cybersecurity in the Healthcare Industry. *The Journal of Medical Practice Management: MPM*, *36*(4), 229-231. https://www.proquest.com/scholarly-journals/cybersecurity-healthcare-industry/docview/2504871270/se-2

Clandinin, D. J., Cave, M. T., & Berendonk, C. (2017). Narrative inquiry: A relational research methodology for medical education. *Medical Education*, *51*(1), 89–96. https://doi.org/10.1111/medu.13136

Clark, K. R., & Veale, B. L. (2018). Strategies to enhance data collection and analysis in qualitative research. *Radiologic Technology*, *89*(5), 482–485. Retrieved from Walden University Library databases. https://research.ebsco.com/c/4wdw3l/viewer/pdf/cvnpfpuvmz

Colorafi, K. J., & Evans, B. (2016). Qualitative descriptive methods in health science research. *Health Environments Research & Design Journal*, *9*(4), 16–25. https://doi.org/10.1177/1937586715614171

Connelly, L. M. (2016). Trustworthiness in qualitative research. *MedSurg Nursing*, *25*(6), 435–436. Retrieved from http://www.medsurgnursing.net/Cooper, P. (2017). Organizational security threats related to portable data storage devices: Qualitative exploratory inquiry (Doctoral dissertation, University of Phoenix). Retrieved from ProQuest (Accession No. 1886131060)

Crowe, M., Inder, M., & Porter, R. (2015). Conducting qualitative research in mental health: Thematic and content analyses. *Australian & New Zealand Journal of Psychiatry*, *49*(7), 616–623. https://doi.org/10.1177/0004867415582053

Crutzen, R., Ygram Peters, G.-J., & Mondschein, C. (2019). Why and how we should care about the General Data Protection Regulation. *Psychology & Health*, *34*(11), 1347–1357. https://doi.org/10.1080/08870446.2019.1606222

Curtis, A. C., & Keeler, C. (2021). Sampling design in Nursing research. *American Journal of Nursing*, *121*(3), 53–57. https://doi.org/10.1097/01.NAJ.0000737304.14564.51

Cypress, B. S. (2017). Rigor or reliability and validity in qualitative research: Perspectives, strategies, reconceptualization, and recommendations. *Dimensions of Critical Care Nursing*, *36*(4), 253–263. https://doi.org/10.1097/DCC.0000000000000253

Das, S. D., & Bala, P. K. (2023). What drives MLOps adoption? An analysis using the TOE framework. *Journal of Decision Systems*, 1–37. https://doi.org/10.1080/12460125.2023.2214306

Dawadi, S., Shrestha, S., & Giri, R. A. (2021). Mixed-methods research: a discussion on its types, challenges, and criticisms. *Journal of Practical Studies in Education*, *2*(2), 25-36. https://doi.org/10.46809/jpse.v2i2.20

DeJonckheere, M., & Vaughn, L. M. (2019). Semistructured interviewing in primary care research: A balance of relationship and rigour. *Family Medicine and Community Health*, *7*(2), 1-8. https://doi.org/10.1136/fmch-2018-000057

Dempsey, L., Dowling, M., Larkin, P., & Murphy, K. (2016). Sensitive interviewing in qualitative research: Sensitive interviewing. *Research in Nursing & Health*, *39*(6), 480–490. https://doi.org/10.1002/nur.21743

De Oliveira, I. A. M., Méxas, M. P., Machado, E. M. M., & Drumond, G. M. (2021). Information security governance in the electricity industry. *Brazilian Journal of Operations & Production Management*, *19*(1), 1–17. https://doi.org/10.14488/BJOPM.2021.045

Dey, J. (2023). State-of-the-art session key generation on priority-based adaptive neural machine (PANM) in telemedicine. *Neural Computing and Applications*, *35*(13), 9517–9533. https://doi.org/10.1007/s00521-022-08169-2

Dhakal, K. (2022). NVivo. *Journal of the Medical Library Association : JMLA*, *110*(2), 270–272. https://doi.org/10.5195/jmla.2022.1271

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security*, *92*, 1-21. https://doi.org/10.1016/j.cose.2020.101747

Dikko, M. (2016). Establishing construct validity and reliability: Pilot testing of a qualitative interview for research in Takaful (Islamic Insurance). *The Qualitative Report*, *21*(3), 521–528. https://nsuworks.nova.edu/tqr

Drabble, L., Trocki, K., Salcedo, B., Walker, P., & Korcha, R. (2016). Conducting qualitative interviews by telephone: Lessons learned from a study of alcohol use among sexual minority and heterosexual women. *Qualitative Social Work*, *15*(1), 118–133. https://doi.org/10.1177/1473325015585613

Eagleson, R., Altamirano-Diaz, L., McInnis, A., Welisch, E., De Jesus, S., Prapavessis, H., Rombeek, M., Seabrook, J. A., Park, T., & Norozi, K. (2017). Implementation of clinical research trials using web-based and mobile devices: Challenges and solutions. *BMC Medical Research Methodology*, *17*(1), 1–8. https://doi.org/10.1186/s12874-017-0324-6

El Komy, M. H. M., Chiricozzi, A., Van De Kerkhof, P., Armstrong, A., Diamei, V., Hsu, C., Gelfand, J., & Navarini, A. A. (2023). Telemedicine and psoriasis: A review based on statements of the telemedicine working group of the International Psoriasis Council. *JEADV Clinical Practice*, *2*(1), 19–31. https://doi.org/10.1002/jvc2.93

Else-Quest, N. M., & Hyde, J. S. (2016). Intersectionality in quantitative psychological research: I. Theoretical and epistemological issues. *Psychology of Women Quarterly*, *40*(2), 155–170. https://doi.org/10.1177/0361684316629797

ENISA. (n.d.). Cramm. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html

Erceg, A. (2019). Information security: Threat from employees. *Tehnicki Glasnik*, *13*(2), 123–128. https://doi.org/10.31803/tg-20180717222848

Fikri, M. A., Putra, F. A., Suryanto, Y., & Ramli, K. (2019). Risk assessment using NIST SP 800-30 Revision 1 and ISO 27005 combination technique in profit-based organization: Case study of ZZZ information system application in ABC agency. *Procedia Computer Science*, *161*, 1206–1215. https://doi.org/10.1016/j.procs.2019.11.234

FitzPatrick, B. (2019). Validity in qualitative health education research. *Currents in Pharmacy Teaching and Learning*, *11*(2), 211–217. https://doi.org/10.1016/j.cptl.2018.11.014

Forero, R., Nahidi, S., De Costa, J., Mohsin, M., Fitzgerald, G., Gibson, N., McCarthy, S., & Aboagye-Sarfo, P. (2018). Application of four-dimension criteria to assess rigour of qualitative research in emergency medicine. *BMC Health Services Research*, *18*(1), 1–11. https://doi.org/10.1186/s12913-018-2915-2

Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security*, 100, 1-7. https://doi.org/10.1016/j.cose.2020.102080

Fusch, P., Fusch, G., & Ness, L. (2018). Denzin's paradigm shift: Revisiting triangulation in qualitative research. *Journal of Social Change*, *10*, 19–32. https://doi.org/10.5590/JOSC.2018.10.1.02

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, *20*(9), 1408–1416. Retrieved from https://nsuworks.nova.edu/tqr/

Gable, E. (2017). Swedish Design: An ethnography by Keith M. Murphy. Ithaca, NY: Cornell University Press, 2015. *Visual Anthropology Review*, *33*(1), 98–100. https://doi.org/10.1111/var.12127

Gaikwad, P. (2017). Including rigor and artistry in case study as a strategic qualitative methodology. *The Qualitative Report*, *22*(13), 3431–3446. Retrieved from https://nsuworks.nova.edu/tqr/vol22/iss13/4

Galvin, R. (2015). How many interviews are enough? Do qualitative interviews in building energy consumption research produce reliable knowledge? *Journal of Building Engineering*, *1*, 2–12. https://doi.org/10.1016/j.jobe.2014.12.001

Gasigwa, T., Maniraho, J. F., & Habimana, O. (2022). Effectiveness of Excel software Integration in Teaching and Learning Statistics on Students' Performance in Selected Kicukiro District Upper Secondary Schools in Rwanda. *Journal of Research Innovation and Implications in Education*, *6*(3), 194–200. www.jriiejournal.com/JRIIE-6-3-021

Gerardo, V., & Fajar, A. N. (2022). Academic IS risk Management using OCTAVE Allegro in Educational Institution. *Journal of Information Systems and Informatics*, *4*(3), 687–708. https://doi.org/10.51519/journalisi.v4i3.319

Gill, S. L. (2020). Qualitative sampling methods. *Journal of Human Lactation*, 36(4), 579–581. https://doi.org/10.1177/0890334420949218

Goertzen, M. (2017). Chapter 3: Introduction to Quantitative Research and Data. *Library Technology Reports*, *53*(4), 12–18. https://journals.ala.org/index.php/ltr/article/view/6325

Grayson, N., Pulivarti, R., Hodges, B., Littlefield, K., Miller, J., Peloquin, C., Snyder, J., Wang, S., & Williams, R. (2023). Mitigating privacy and cybersecurity risks affecting telehealth remote patient monitoring ecosystems. *Computer*, *56*(9), 50–61. https://doi.org/10.1109/MC.2023.3253044

Greener, S. (2018). Research limitations: The need for honesty and common sense. *Interactive Learning Environments*, *26*(5), 567–568. https://doi.org/10.1080/10494820.2018.1486785

Griffith, D. A., Morris, E. S., & Thakar, V. (2016). Spatial autocorrelation and qualitative sampling: The case of snowball type sampling designs. *Annals of the American Association of Geographers*, *106*(4), 773–787. https://doi.org/10.1080/24694452.2016.1164580

Gul, I. (2019). *Exploring the application security measures in hive to secure data in column* (Doctoral dissertation, Colorado Technical University). Available from ProQuest Dissertations & Theses Global. (Order No. 10844071).

https://www.proquest.com/openview/f29652d0ec43cc8ca99e86bf5ac85d2e/1?pq-origsite=gscholar&cbl=18750

Gunawan, J. (2015). Ensuring trustworthiness in qualitative research. *Belitung Nursing Journal*, *1*(1), 10–11. https://doi.org/10.33546/bnj.4

Hadi, M. A., & Closs, S. J. (2016). Ensuring rigour and trustworthiness of qualitative research in clinical pharmacy. International Journal of Clinical Pharmacy, 38, 641–646. https://doi.org/10.1007/s11096-015-0237-6

Hagaman, A., & Wutich, A. (2017). How many interviews are enough to identify metathemes in multisited and cross-cultural research? Another perspective on Guest, Bunce, and Johnson's (2006) landmark study. *Field Methods*, *29*(1), 23–41. https://doi.org/10.1177/1525822X16640447

Haleem, A., Javaid, M., Singh, R. P., & Suman, R. (2021). Telemedicine for healthcare: Capabilities, features, barriers, and applications. *Sensors International*, *2*(1), 1-12. https://doi.org/10.1016/j.sintl.2021.100117

Hammarberg, K., Kirkman, M., & de Lacey, S. (2016). Qualitative research methods: When to use them and how to judge them. *Human Reproduction*, *31*(3), 498–501. https://doi.org/10.1093/humrep/dev334

Hancock, M. E., Amankwaa, L., Revell, M. A., & Mueller, D. (2016). Focus group data saturation: A new approach to data analysis. *Qualitative Report*, *21*(11), 2124–2130. https://nsuworks.nova.edu/tqr

Hanif, I. (2015). Management control system design: An interpretive ethnography. *Procedia - Social and Behavioral Sciences*, *211*, 119–126. https://doi.org/10.1016/j.sbspro.2015.11.018

Harrison, H., Birks, M., Franklin, R., & Mills, J. (2017). Case study research: Foundations and methodological orientations. *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, *17*(1), 1-17. Retrieved from http://www.qualitative-research.net/

Hayashi, P., Abib, G., & Hoppen, N. (2019). Validity in qualitative research: A processual approach. *The Qualitative Report*. doi:10.46743/2160-3715/2019.3443

Hays, D. G., Wood, C., Dahl, H., & Kirk-Jenkins, A. (2016). Methodological rigor in Journal of Counseling & Development qualitative research articles: A 15-Year review. *Journal of Counseling & Development*, *94*(2), 172–183. https://doi.org/10.1002/jcad.12074

Herrera Montano, I., García Aranda, J. J., Ramos Diaz, J., Molina Cardín, S., De La Torre Díez, I., & Rodrigues, J. J. P. C. (2022). Survey of techniques on data leakage protection and methods to address the insider threat. *Cluster Computing*, *25*(6), 4289–4302. https://doi.org/10.1007/s10586-022-03668-2

Hickson, H. (2016). Becoming a critical narrativist: Using critical reflection and narrative inquiry as research methodology. *Qualitative Social Work: Research and Practice*, *15*(3), 380–391. https://doi.org/10.1177/1473325015617344

Hong, K. S., Chi, Y. P., Chao, L., & Tang, J. H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, *11*(5), 243–248. https://doi.org/10.1108/09685220310500153

Houston, R. (2019). *Thriving cybersecurity professionals: Building a resilient workforce and psychological safety in the federal government* (Capstone Projects). Retrieved from https://repository.upenn.edu/mapp_capstone/172

Hussain, M., Al-Haiqi, A., Zaidan, A. A., Zaidan, B. B., Kiah, M., Iqbal, S., Iqbal, S., & Abdulnabi, M. (2018). A security framework for mHealth apps on Android platform. *Computers & Security*, *75*, 191–217. https://doi.org/10.1016/j.cose.2018.02.003

Iqbal, Y., Tahir, S., Tahir, H., Khan, F., Saeed, S., Almuhaideb, A. M., & Syed, A. M. (2022). A novel homomorphic approach for preserving privacy of patient data in Telemedicine. *Sensors*, *22*(12), 1–19. https://doi.org/10.3390/s22124432

Isaksson, A., Borjesson, E., Gunn, M., Andersson, C., & Ehrnberger, K. (2017). Norm critical design and ethnography: Possibilities, objectives and stakeholders. *Sociological Research Online*, *22*(4), 232–252. https://doi.org/10.1177/1360780417743168

Iwaya, L. H., Ahmad, A., & Babar, M. A. (2020). Security and privacy for mHealth and uHealth systems: A systematic mapping study. *IEEE Access*, *8*, 150081–150112. https://doi.org/10.1109/ACCESS.2020.3015962

Jalali, M. S., Landman, A., & Gordon, W. J. (2021). Telemedicine, privacy, and information security in the age of COVID-19. *Journal of the American Medical Informatics Association*, *28*(3), 671–672. https://doi.org/10.1093/jamia/ocaa310

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, *1*, 1–13. https://doi.org/10.1016/j.csa.2023.100016

Jin, M. X., Kim, S. Y., Miller, L. J., Behari, G., & Correa, R. (2020). Telemedicine: Current impact on the future. *Cureus*, *12*(8), 1–5. https://doi.org/10.7759/cureus.9891

Kaewkungwal, J., & Adams, P. (2019). Ethical consideration of the research proposal and the informed-consent process: An online survey of researchers and ethics committee members in Thailand. *Accountability in Research*, 1-27. https://doi.org/10.1080/08989621.2019.1608190

Kelly, L. M., & Cordeiro, M. (2020). Three principles of pragmatism for research on organizational processes. *Methodological Innovations*, *13*(2), 1-10. https://doi.org/10.1177/2059799120937242

Khan, F., Kim, J. H., Mathiassen, L., & Moore, R. (2021). Data breach management: An integrated risk model. *Information & Management*, *58*(1), 1–12. https://doi.org/10.1016/j.im.2020.103392

Khan, R. A., Akbar, M. A., Rafi, S., Almagrabi, A. O., & Alzahrani, M. (2023). Evaluation of requirement engineering best practices for secure software development in GSD: An ISM Analysis [Preprint]. Preprints. https://doi.org/10.22541/au.167416698.89030964/v1

Khan, S., Mubarik, M., Kusi-Sarpong, S., Zaman, S., & Alam Kazmi, S. H. (2020). Social sustainable supply chains in the food industry: A perspective of an emerging economy. *Corporate Social Responsibility and Environmental Management*, *28*(1), 1–15. https://doi.org/10.1002/csr.2057

Kim, D., Choi, J., & Han, K. (2020). Risk management-based security evaluation model for telemedicine systems. *BMC Medical Informatics and Decision Making*, *20*(1), 1-14. https://doi.org/10.1186/s12911-020-01145-7

Kim, E. S., Bruinooge, S. S., Roberts, S., Ison, G., Lin, N. U., Gore, L., Uldrick, T. S., Lichtman, S. M., Roach, N., Beaver, J. A., Sridhara, R., Hesketh, P. J., Denicoff, A. M., Garrett-Mayer, E., Rubin, E., Multani, P., Prowell, T. M., Schenkel, C., Kozak, M., … Schilsky, R. L. (2017). Broadening eligibility criteria to make clinical trials more representative: American society of clinical oncology and friends of cancer research joint research statement. *Journal of Clinical Oncology*, *35*(33), 3737–3744. https://doi.org/10.1200/JCO.2017.73.7916

Kim, Y., & Kim, B. (2021). The Effective Factors on Continuity of Corporate Information Security Management: Based on TOE Framework. Information, 12(11), 1–12. https://doi.org/10.3390/info12110446

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2022). Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management

Systems: A Case Study in IT Consulting Industry. *Sustainability*, *14*(3), 1–19. https://doi.org/10.3390/su14031269

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, *24*(1), 120–124. https://doi.org/10.1080/13814788.2017.1375092

Lang, U. (2018). Securing complex cyber-physical medical device landscapes. *Information Systems Security Association.* 14-46. https://www.issa.org

Larkin, M., Shaw, R., & Flowers, P. (2019). Multiperspectival designs and processes in interpretative phenomenological analysis research. *Qualitative Research in Psychology*, *16*(2), 182–198. https://doi.org/10.1080/14780887.2018.1540655

Leech, N. L., & Onwuegbuzie, A. J. (2008). Qualitative data analysis: A compendium of techniques and a framework for selection for school psychology research and beyond. *School Psychology Quarterly*, *23*(4), 587–604. https://doi.org/10.1037/1045-3830.23.4.587

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care*, *4*(3), 324-327. https://doi.org/10.4103/2249-4863.161306

Limberg, D., Schuermann, H., Fox, J., & Robinson, E. (2018). A phenomenological investigation of altruism from the perspective of counsellors in Scotland. *Counselling and Psychotherapy Research*, *18*(1), 49–58. https://doi.org/10.1002/capr.12150

Lin, L.-C. (2009). Data management and security in qualitative research. *Dimensions of Critical Care Nursing*, *28*(3), 132–137. https://journals.lww.com/dccnjournal/toc/2009/05000

Lindsley, K. A. (2019). Improving quality of the informed consent process: Developing an easy-to-read, multimodal, patient-centered format in a real-world setting. *Patient Education and Counseling*, *102*(5), 944–951. https://doi.org/10.1016/j.pec.2018.12.022

Lopes, J. A., Gomes, C., Oliveira, C. R., & Elliott, J. G. (2020). Research studies on dyslexia: Participant inclusion and exclusion criteria. *European Journal of Special Needs Education*, *35*(5), 587–602. https://doi.org/10.1080/08856257.2020.1732108

Malodia, S., Dhir, A., Mishra, M., & Bhatti, Z. A. (2021). Future of e-Government: An integrated conceptual framework. *Technological Forecasting and Social Change*, *173*, 1–17. https://doi.org/10.1016/j.techfore.2021.121102

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

Maramwidze-Merrison, E. (2016). Innovative methodologies in qualitative research: Social media window for accessing organisational elites for interviews. *The Electronic Journal of Business Research Methods*, *14*(2), 157-167. https://www.ejbrm.com

Marks, A., Wilkes, L., Blythe, S., & Griffiths, R. (2017). A novice researcher's reflection on recruiting participants for qualitative research. *Nurse Researcher*, *25*(2), 34–38. https://doi.org/10.7748/nr.2017.e1510

Martínez-Mesa, J., González-Chica, D. A., Duquia, R. P., Bonamigo, R. R., & Bastos, J. L. (2016). Sampling: how to select participants in my research study? *Anais Brasileiros de Dermatologia*, *91*(3), 326–330. https://doi.org/10.1590/abd1806-4841.20165254

Matlala, S., & Matlala, M. (2018). The use of a smartphone to facilitate qualitative research in South Africa. *The Qualitative Report*, *23*(10), 2264-2275. https://nsuworks.nova.edu/tqr/vol23/iss10/3

McCarthy, C. J., Whittaker, T. A., Boyle, L. H., & Eyal, M. (2017). Quantitative approaches to group research: Suggestions for best practices. *The Journal for Specialists in Group Work*, *42*(1), 3–16. https://doi.org/10.1080/01933922.2016.1264520

McInnes, S., Peters, K., Bonney, A., & Halcomb, E. (2017). An exemplar of naturalistic inquiry in general practice research. *Nurse Researcher*, *24*(3), 36–41. https://doi.org/10.7748/nr.2017.e1509

McNair, A. G. K., MacKichan, F., Donovan, J. L., Brookes, S. T., Avery, K. N. L., Griffin, S. M., Crosby, T., & Blazeby, J. M. (2016). What surgeons tell patients and what patients want to know before major cancer surgery: A qualitative study. *BMC Cancer*, *16*(1), 1–8. https://doi.org/10.1186/s12885-016-2292-3

Meshkinyazd, A., Heydari, A., & Fayyazi bordbar, M. (2020). Lived experiences of caregivers with patients borderline personality disorder: A phenomenological study. *International Journal of Community Based Nursing & Midwifery*, *8*(2), 177-188. https://doi.org/10.30476/ijcbnm.2020.83358.1154

Mirick, R. G., & Wladkowski, S. P. (2019). Skype in qualitative interviews: Participant and researcher perspectives. *The Qualitative Report*, *24*(12), 3061-3072. https://nsuworks.nova.edu/tqr/vol24/iss12/9

Mohajan, H. K. (2018). Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment and People*, 7(1), 23-48. https://doi.org/10.26458/jedep.v7i1.571

Molina-Azorin, J. F. (2016). Mixed methods research: An opportunity to improve our studies and our research skills. *European Journal of Management and Business Economics*, *25*(2), 37–38. https://doi.org/10.1016/j.redeen.2016.05.001

Moon, K., Brewer, T. D., Januchowski-Hartley, S. R., Adams, V. M., & Blackman, D. A. (2016). A guideline to improve qualitative social science publishing in ecology and conservation journals. *Ecology and Society*, *21*(3), 1–20. https://doi.org/10.5751/ES-08663-210317

Moreno-Ligero, M., Moral-Munoz, J. A., Salazar, A., & Failde, I. (2023). mHealth intervention for improving pain, quality of Life, and functional disability in patients with chronic pain: Systematic review. JMIR mHealth and uHealth, 11(1), 1–25. https://doi.org/10.2196/40844

Morgan, H. (2022). Conducting a qualitative document analysis. *The Qualitative Report*, *27*(1), 64–77. https://doi.org/10.46743/2160-3715/2022.5044

Mseke, E. P., Jessup, B., & Barnett, T. (2023). A systematic review of the preferences of rural and remote youth for mental health service access: Telehealth versus face-to-face consultation. *Australian Journal of Rural Health*, 1-15. https://doi.org/10.1111/ajr.12961

Muraguri, N., Mwalili, T., & Mose, T. (2019). Factors influencing cybersecurity readiness in deposit taking savings and credit cooperatives: A case study of Nairobi County. *International Academic Journal of Information Systems and Technology*, *2*(1), 157–182. http://www.iajournals.org/articles/iajist_v2_i1_157_182.pdf

Nanjundeswaraswamy, T. S., & Divakar, S. (2021). Determination of sample size and sampling methods in applied research. *Proceedings on Engineering Sciences*, *3*(1), 25–32. https://doi.org/10.24874/PES03.01.003

National Institute of Standards and Technology. NIST. (n.d.). *PHI—Glossary*. U.S. Department of Commerce, Computer Security Resource Center. https://csrc.nist.gov/glossary/term/phi

Ngenye, L., & Kreps, G. (2020). A Review of Qualitative Methods in Health Communication Research. *The Qualitative Report*, *25*(3), 631–645. https://doi.org/10.46743/2160-3715/2020.4488

Ngongo, B., Ochola, P., Ndegwa, J., & Katuse, P. (2019). The technological, organizational and environmental determinants of adoption of mobile health applications (m-health) by hospitals in Kenya. *PLOS ONE*, *14*(12), 1-25. https://doi.org/10.1371/journal.pone.0225167

Nie, J. X., Heidebrecht, C., Zettler, A., Pearce, J., Cunha, R., Quan, S., Mansfield, E., & Tang, T. (2023). The perceived ease of use and perceived usefulness of a web-based interprofessional communication and collaboration platform in the hospital setting: Interview study with health care providers. *JMIR Human Factors*, *10*, 1–14. https://doi.org/10.2196/39051

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, *21*(15), 5119. https://doi.org/10.3390/s21155119

Niki, O., Saira, G., Arvind, S., & Mike, D. (2022). Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that. *Digital Health*, *8*, 1-3. https://doi.org/10.1177/20552076221104665

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, *16*(1), 1–13. https://doi.org/10.1177/1609406917733847

Obitade, P. O. (2019). Big data analytics: A link between knowledge management capabilities and superior cyber protection. *Journal of Big Data*, *6*(1), 1–28. https://doi.org/10.1186/s40537-019-0229-9

Ogbonna, L. (2020). *Technical strategies database managers use to protect systems from security breaches.* (Doctoral dissertation). https://scholarworks.waldenu.edu/dissertations/

Oltmann, S. (2016). Qualitative interviews: A methodological discussion of the interviewer and respondent contexts. *Forum: Qualitative Social Research*, *17*(2), 1-16. http://www.qualitative-research.net/

Othman, Z., & Hamid, F. (2018). Dealing with un(expected) ethical dilemma: Experience from the field. *The Qualitative Report*, *23*(4), 733-741. https://nsuworks.nova.edu/tqr/vol23/iss4/1

Pal, S., & Mukhopadhyay, A. (2018). Cyber risk quantification and mitigation framework for healthcare using machine learning. *Proceedings of the 24th Americas Conference on Information Systems*, New Orleans, 1-10. https://aisel.aisnet.org/amcis2018/Security/Presentations/23/

Palinkas, L. A., Mendon, S. J., & Hamilton, A. B. (2019). Innovations in mixed methods evaluations. *Annual Review of Public Health*, *40*(1), 423–442. https://doi.org/10.1146/annurev-publhealth-040218-044215

Paradis, E., O'Brien, B., Nimmon, L., Bandiera, G., & Martimianakis, M. A. (2016). Design: Selection of data collection methods. *Journal of Graduate Medical Education*, *8*(2), 263–264. https://doi.org/10.4300/JGME-D-16-00098.1

Park, J., & Park, M. (2016). Qualitative versus quantitative research methods: Discovery or justification? *Journal of Marketing Thought*, *3*(1), 1–7. https://doi.org/10.15577/jmt.2016.03.01.1

Perez-Gonzalez, D., Preciado, S. T., & Solana-Gonzalez, P. (2019). Organizational practices as antecedents of the information security management performance: An empirical investigation. *Information Technology & People*, *32*(5), 1262–1275. https://doi.org/10.1108/ITP-06-2018-0261

Peticca-Harris, A., deGama, N., & Elias, S. (2016). A dynamic process model for finding informants and gaining access in qualitative research. *Organizational Research Methods*, *19*(3), 376–401. https://doi.org/10.1177/1094428116629218

Phillippi, J., & Lauderdale, J. (2018). A guide to field notes for qualitative research: Context and conversation. *Qualitative Health Research*, *28*(3), 381–388. https://doi.org/10.1177/1049732317697102

Pino Gavidia, L. A., & Adu, J. (2022). Critical Narrative Inquiry: An Examination of a Methodological Approach. *International Journal of Qualitative Methods*, *21*, 1–5. https://doi.org/10.1177/16094069221081594

Poleto, T., Silva, M. M., Clemente, T. R. N., De Gusmão, A. P. H., Araújo, A. P. D. B., & Costa, A. P. C. S. (2021). A risk assessment framework proposal based on Bow-Tie analysis for medical image diagnosis sharing within Telemedicine. *Sensors*, *21*(7), 2426. https://doi.org/10.3390/s21072426

Polukhina, E. (2022). Ethnographic Case-Study Design for Discovering Identities in Russian Post-Industrial Neighbourhoods. *The Qualitative Report*, 27(5), 1221–1238. https://doi.org/10.46743/2160-3715/2022.5381

Pope, E. M. (2020). From participants to co-researchers: Methodological alterations to a qualitative case study. *The Qualitative Report*, *25*(10), 3749-3761. Retrieved from https://nsuworks.nova.edu/tqr/vol25/iss10/15

Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2), 1-6. https://doi.org/10.1002/itl2.247

Ramanadhan, S., Revette, A. C., Lee, R. M., & Aveling, E. L. (2021). Pragmatic approaches to analyzing qualitative data for implementation science: An introduction. *Implementation Science Communications*, *2*(1), 70. https://doi.org/10.1186/s43058-021-00174-1

Redman, B. K., & Caplan, A. L. (2021). Should the regulation of research misconduct be integrated with the ethics framework promulgated in The Belmont Report? *Ethics & Human Research*, *43*(1), 37–41. https://doi.org/10.1002/eahr.500078

Ridder, H. G. (2017). The theory contribution of case study research designs. *Business Research*, *10*(2), 281–305. https://doi.org/10.1007/s40685-017-0045-z

Rimando, M., Brace, A., Namageyo-Funa, A., Parr, T., Sealy, D.-A., Davis, T., Martinez, L., & Christiana, R. (2015). Data collection challenges and recommendations for early career researchers. *The Qualitative Report*, *20*(12), 2025–2036. https://nsuworks.nova.edu/tqr

Rivers, L. (2020). Strategies for reducing the risk of data breach within the internet cloud. [Doctoral dissertation, Walden University]. Walden University Library Databases. https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=11074&context=dissertations/

Rosenthal, M. (2016). Qualitative research methods: Why, when, and how to conduct interviews and focus groups in pharmacy research. *Currents in Pharmacy Teaching and Learning*, *8*(4), 509–516. https://doi.org/10.1016/j.cptl.2016.03.021

Rothstein, M. A., Wilbanks, J. T., Beskow, L. M., Brelsford, K. M., Brothers, K. B., Doerr, M., Evans, B. J., Hammack-Aviran, C. M., McGowan, M. L., & Tovino, S. A. (2020). Unregulated health research using mobile devices: Ethical considerations and policy recommendations. *Journal of Law, Medicine & Ethics*, *48*(S1), 196–226. https://doi.org/10.1177/1073110520917047

Rutberg, S., & Bouikidis, C. D. (2018). Focusing on the fundamentals: A simplistic differentiation between qualitative and quantitative research. *Nephrology Nursing Journal*, *45*(2), 209–213. https://www.academia.edu/download/122272598/20181009143525article2.pdf

Salsabilla, A., Azzahra, A. B., Syafitri, R. I., Supadmi, W., & Suwantika, A. A. (2021). Cost-Effectiveness of Telemedicine in Asia: A scoping review. *Journal of Multidisciplinary Healthcare*, *14*(1), 3587–3596. https://doi.org/10.2147/JMDH.S332579

Santiago-Delefosse, M., Gavin, A., Bruchez, C., Roux, P., & Stephen, S. L. (2016). Quality of qualitative research in the health sciences: Analysis of the common criteria present in 58 assessment guidelines by expert users. *Social Science & Medicine*, *148*, 142–151. https://doi.org/10.1016/j.socscimed.2015.11.007

Sardi, A., Rizzi, A., Sorano, E., & Guerrieri, A. (2020). Cyber risk in health facilities: A systematic literature review. *Sustainability*, *12*(17), 7002. https://doi.org/10.3390/su12177002

Sarma, S. K. (2015). Qualitative research: Examining the misconceptions. *South Asian Journal of Management*, *22*(3), 176–191. https://www.sajm-amdisa.org/images/stories/pdf/sajmvol.22.3-abstract.pdf

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2018). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity*, *52*(4), 1893–1907. https://doi.org/10.1007/s11135-017-0574-8

Schoonenboom, J., & Johnson, R. B. (2017). How to construct a mixed methods research design. *Kolner Zeitschrift Fur Soziologie Und Sozialpsychologie*, *69*(S2), 107–131. https://doi.org/10.1007/s11577-017-0454-1

Scuotto, V., Ferraris, A., & Bresciani, S. (2016). Internet of things: Applications and challenges in smart cities: A case study of IBM smart city projects. *Business Process Management Journal*, *22*(2), 357–367. https://doi.org/10.1108/BPMJ-05-2015-0074

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020). Healthcare data breaches: Insights and implications. *Healthcare*, *8*(2), Article 2. https://doi.org/10.3390/healthcare8020133

Seitz, S. (2016). Pixilated partnerships, overcoming obstacles in qualitative interviews via Skype: A research note. *Qualitative Research*, *16*(2), 229–235. https://doi.org/10.1177/1468794115577011

Sendelj, R., & Ognjanovic, I. (2022). *Cybersecurity Challenges in Healthcare.* In J. Mantas, A. Hasman, & R. Haux (Eds.), Studies in Health Technology and Informatics. IOS Press. https://doi.org/10.3233/SHTI220951

Sethuraman, S. C., Vijayakumar, V., & Walczak, S. (2020). Cyber attacks on healthcare devices using unmanned aerial vehicles. *Journal of Medical Systems*, *44*(1), 29. https://doi.org/10.1007/s10916-019-1489-9

Shahbaznezhad, H., Kolini, F., & Rashidirad, M. (2021). Employees' behavior in phishing attacks: What individual, organizational, and technological factors matter? *Journal of Computer Information Systems*, *61*(6), 539–550. https://doi.org/10.1080/08874417.2020.1812134

Shahbodin, F., Azni, A. H., Ali, T., & Mohd, C. K. N. C. K. (2019). Lightweight cryptography techniques for mHealth cybersecurity. Proceedings of the 2019 Asia Pacific Information Technology Conference on - APIT 2019, 44–50. https://doi.org/10.1145/3314527.3314536

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, *124*, 1-8. https://doi.org/10.1016/j.cose.2022.102974

Shannon-Baker, P. (2016). Making paradigms meaningful in mixed methods research. *Journal of Mixed Methods Research*, *10*(4), 319–334. https://doi.org/10.1177/1558689815575861

Shapka, J. D., Domene, J. F., Khan, S., & Yang, L. M. (2016). Online versus in-person interviews with adolescents: An exploration of data equivalence. *Computers in Human Behavior*, *58*, 361–367. https://doi.org/10.1016/j.chb.2016.01.016

Sherif, V. (2018). Evaluating preexisting qualitative research data for secondary analysis. *Forum: Qualitative Social Research*, *19*(2), 1–22. https://doi.org/10.17169/fqs-19.2.2821

Sim, J., Saunders, B., Waterfield, J., & Kingstone, T. (2018). Can sample size in qualitative research be determined a priori? *International Journal of Social Research Methodology*, *21*(5), 619–634. https://doi.org/10.1080/13645579.2018.1454643

Simpson, A., & Quigley, C. F. (2016). Member checking process with adolescent students: Not just reading a transcript. *The Qualitative Report*, *21*(2), 376–392. https://nsuworks.nova.edu/tqr

Sindhuja, P. N. (2021). The impact of information security initiatives on supply chain robustness and performance: an empirical study. *Information and Computer Security*, *29*(2), 365-391. https://doi.org/10.1108/ICS-07-2020-0128

Smith, B., & McGannon, K. R. (2018). Developing rigor in qualitative research: Problems and opportunities within sport and exercise psychology. *International*

Review of Sport and Exercise Psychology, *11*(1), 101–121. https://doi.org/10.1080/1750984X.2017.1317357

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Soomro, Z., Shah, M., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Staller, K. M. (2021). Big enough? Sampling in qualitative inquiry. *Qualitative Social Work*, *20*(4), 897–904. https://doi.org/10.1177/14733250211024516

Sutton, J., & Austin, Z. (2015). Qualitative research: Data collection, analysis, and management. *Canadian Journal of Hospital Pharmacy*, *68*(3). https://doi.org/10.4212/cjhp.v68i3.1456

Tahamtan, I., Pajouhanfar, S., Sedghi, S., Azad, M., & Roudbari, M. (2017). Factors affecting smartphone adoption for accessing information in medical settings. *Health Information & Libraries Journal*, *34*(2), 134–145. https://doi.org/10.1111/hir.12174

Tanoh, C. N., Mostafa, A., Lazo, A., Lyons, T., Straub, J. A., & Dean, I. (2022). Effectiveness of information security governance in the U.S. banking industry: Towards a resilient business perspective. Retrieved from Walden University Library databases. https://www.proquest.com/dissertations-theses/effectiveness-information-security-governance-u-s/docview/2654124325/se-2?accountid=14872

Tausch, A. P., & Menold, N. (2016). Methodological aspects of focus groups in health research: Results of qualitative interviews with focus group moderators. *Global Qualitative Nursing Research*, *3*, 1-12. https://doi.org/10.1177/2333393616630466

Taylor, M. J., Fornusek, C., Ruys, A. J., Bijak, M., & Bauman, A. E. (2017). The Vienna FES interview protocol – A mixed-methods protocol to elucidate the opinions of various individuals responsible for the provision of FES exercise. *European Journal of Translational Myology*, *27*(3). https://doi.org/10.4081/ejtm.2017.6604

Tejay, G. P. S., & Mohammed, Z. A. (2023). Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. *Information & Management*, *60*(3), 1–20. https://doi.org/10.1016/j.im.2022.103751

Theofanidis, D., & Fountouki, A. (2019). Limitations and delimitations in the research process. *Perioperative Nursing*, *7*(3), 155–163. https://doi.org/10.5281/ZENODO.2552022

Thomas, D. R. (2017). Feedback from research participants: are member checks useful in qualitative research? *Qualitative Research in Psychology*, *14*(1), 23–41. https://doi.org/10.1080/14780887.2016.1219435

Tran, V. T., Porcher, R., Falissard, B., & Ravaud, P. (2016). Point of data saturation was assessed using resampling methods in a survey with open-ended questions. *Journal of Clinical Epidemiology*, *80*, 88–96. https://doi.org/10.1016/j.jclinepi.2016.07.014

Tran, V. T., Porcher, R., Tran, V. C., & Ravaud, P. (2017). Predicting data saturation in qualitative surveys with mathematical models from ecological research. *Journal of Clinical Epidemiology*, *82*, 71-78. https://doi.org/10.1016/j.jclinepi.2016.10.001

Tsai, A. C., Kohrt, B. A., Matthews, L. T., Betancourt, T. S., Lee, J. K., Papachristos, A. V., Weiser, S. D., & Dworkin, S. L. (2016). Promises and pitfalls of data sharing in qualitative research. *Social Science & Medicine*, *169*, 191–198. https://doi.org/10.1016/j.socscimed.2016.08.004

Tu, C. Z., Adkins, J., & Zhao, G. Y. (2019). A review of information systems security management: An integrated framework. MWAIS 2019 Proceedings. 15. Retrieved from https://aisel.aisnet.org/mwais2019/15

Tulyakul, P., & Meepring, S. (2020). Ethical issues of informed consent: Students as participants in faculty research. *Global Journal of Health Science*, *12*(3), 86. https://doi.org/10.5539/gjhs.v12n3p86

Twining, P., Heller, R., Nussbaum, M., & Tsai, C. C. (2017). Some guidance on conducting and reporting qualitative studies. *Computers & Education*, *106*, 1–16. https://doi.org/10.1016/j.compedu.2016.12.002

Ullah, F., Qayyum, S., Thaheem, M. J., Al-Turjman, F., & Sepasgozar, S. M. E. (2021). Risk management in sustainable smart cities governance: A TOE framework. *Technological Forecasting and Social Change*, *167*, 1–22. https://doi.org/10.1016/j.techfore.2021.120743

Ulrich, T. A. (2020). Qualitative Studies and Textual Document Research in the United States: Conducting Research in National Archives. *The Qualitative Report*, *25*(2), 359–378. https://doi.org/10.46743/2160-3715/2020.4173

Vasileiou, K., Barnett, J., Thorpe, S., & Young, T. (2018). Characterising and justifying sample size sufficiency in interview-based studies: systematic analysis of qualitative health research over a 15-year period. *BMC Medical Research Methodology*, *18*(148), 1-18. https://doi.org/10.1186/s12874-018-0594-7

Veatch, R. M. (2020). Reconciling lists of principles in bioethics. *The Journal of Medicine and Philosophy: A Forum for Bioethics and Philosophy of Medicine*, *45*(4–5), 540–559. https://doi.org/10.1093/jmp/jhaa017

Vitak, J., Proferes, N., Shilton, K., & Ashktorab, Z. (2017). Ethics regulation in social computing research: Examining the role of institutional review boards. *Journal of Empirical Research on Human Research Ethics*, *12*(5), 372–382. https://doi.org/10.1177/1556264617725200

Wadams, M., & Park, T. (2018). Qualitative rcesearch in correctional settings: Researcher bias, western ideological influences, and social justice. *Journal of Forensic Nursing*, *14*(2), 72–79. https://doi.org/10.1097/JFN.0000000000000199

Wage and Hour Division. (n.d.). *Southeast Region*. U.S. Department of Labor, Wage and Hour Division. https://www.dol.gov/whd/programs/dbra/seast.htm

Wallace, J. (2019). Ethics and inscription in social robot design. A visual ethnography. *Paladyn, Journal of Behavioral Robotics*, *10*(1), 66–76. https://doi.org/10.1515/pjbr-2019-0003

Wallace, S., Green, K. Y., Johnson, C. M., Cooper, J. T., & Gilstrap, C. M. (2020). An extended TOE framework for cybersecurity adoption decisions. *Communications of the Association for Information Systems*, *47*(51), 338–363. https://doi.org/10.17705/1CAIS.04716

Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in Digital Health*, *4*(1), 1-20. https://doi.org/10.3389/fdgth.2022.862221

Weller, S. (2017). Using internet video calls in qualitative (longitudinal) interviews: Some implications for rapport. *International Journal of Social Research Methodology*, *20*(6), 613–625. https://doi.org/10.1080/13645579.2016.1269505

White, D., & Hind, D. (2015). Projection of participant recruitment to primary care research: A qualitative study. *Trials*, *16*(1), 473. https://doi.org/10.1186/s13063-015-1002-9

Wilson, A. D., Onwuegbuzie, A. J., & Manning, L. P. (2016). Using paired depth interviews to collect qualitative data. *The Qualitative Report*, *21*(9), 1549–1573. https://nsuworks.nova.edu/tqr/vol21/iss9/1

Wood, L. (2017). The ethical implications of community-based research: A call to rethink current review board requirements. *International Journal of Qualitative Methods*, *16*(1), 1-7. https://doi.org/10.1177/1609406917748276

Wood, L. M., Sebar, B., & Vecchio, N. (2020). Application of rigour and credibility in qualitative document analysis: Lessons learnt from a case study. *The Qualitative Report*, *25*(2), 456-470. https://nsuworks.nova.edu/tqr/vol25/iss2/11

Wu, Y. C., Sun, R., & Wu, Y. J. (2020). Smart City Development in Taiwan: From the Perspective of the Information Security Policy. *Sustainability*, *12*(7), 1-18. https://doi.org/10.3390/su12072916

Yang, J., Luo, B., Zhao, C., & Zhang, H. (2022). Artificial intelligence healthcare service resources adoption by medical institutions based on TOE framework. *Digital Health*, *8*, 205520762211260. https://doi.org/10.1177/20552076221126034

Yang, T. H., Ku, C. Y., & Liu, M. N. (2016). An integrated system for information security management with the unified framework. *Journal of Risk Research*, *19*(1), 21-41. https://doi.org/10.1080/13669877.2014.940593

You, Y., Cho, I., & Lee, K. (2016). An advanced approach to security measurement system. *Journal of Supercomputing*, *72*(9), 3443–3454. https://doi.org/10.1007/s11227-015-1585-7

Zaini, M. K., Masrek, M. N., & Sani, M. K. J. A. (2020). The impact of information security management practices on organisational agility. *Information & Computer Security*, *28*(5), 681–700. https://doi.org/10.1108/ICS-02-2020-0020

Zaini, M. K., Masrek, M. N., Sani, M. K. J. A., & Anwar, N. (2018). Theoretical modeling of information security: Organizational agility model based on integrated system theory and resource based view. *International Journal of Academic Research in Progressive Education and Development*, *7*(3), 390–400. https://www.hrmars.com

Zin, K. S. L. T., Kim, S., Kim, H.-S., & Feyissa, I. F. (2023). A study on technology acceptance of digital healthcare among older Korean adults using extended TAM

(Extended Technology Acceptance Model). *Administrative Sciences*, *13*(2), 1–18. https://doi.org/10.3390/admsci13020042

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

Zyphur, M. J., & Pierides, D. C. (2020). Making quantitative research work: From positivist dogma to actual social scientific inquiry. *Journal of Business Ethics*, *167*(1), 49–62. https://doi.org/10.1007/s10551-019-04189-6

Appendix A: Interview Questions

1. What types of cyber-attacks have you experienced against customers' PHI when using Telemedicine?
2. What security policies do you use to protect customers' PHI against cyber-attacks when using Telemedicine?
3. How does the implementation of those security policies protect customers' PHI against cyber-attacks when using Telemedicine?
4. What does security policies maintenance do for customers' PHI against cyber-attacks when using Telemedicine?
5. What strategies do you use to minimize the risk of cyber-attacks when using Telemedicine?
6. How do you manage those strategies to mitigate the risk of cyber-attacks to protect customers' PHI when using Telemedicine?
7. How do you measure the performance of the security controls implemented to protect customers' PHI against cyber-attacks when using Telemedicine?
8. What factors do you consider when auditing the strategies for protecting customers' PHI against cyber-attacks when using Telemedicine?
9. What strategies do you use to protect customers' PHI against cyber-attacks when using Telemedicine?
10. How do you respond to cyber-attacks against customers’ PHI when using Telemedicine?

Appendix B: Interview Protocol

1. The interview protocol will start with thanking the participant for taking the time to meet with me.
2. Followed by introducing myself and explaining the purpose of the study, as well as my role as the researcher.
3. I will confirm that I received email reply with participant’s consent after he/she had previously received the consent form that included the study purpose, nature, and open-ended questions.
4. The participant will be reminded that their participation is voluntary, and he or she can withdraw at any time during the research by sending me an email indicating so.
5. Describe the interview process and the different types of questions.
6. I will let the participant know before the interview starts and with his/her permission, that I will audio record the interview with a smartphone voice recording app, and I will be taking notes to facilitate data accuracy.
7. Also, in the event the interview is transcribed by a professional service, they will have to sign a non-disclosure agreement. So, their identity will not be disclosed.
8. Verify if the participant has any questions before beginning the interview. If not, I will start recording and the interview. If he/she has questions, I will answer them before beginning the interview questions.

9. Let the participant know that I will contact him/her back following up on the interview questions to verify I have captured the information accurately.
10. Then, I will wrap up the interview and ask if there are any questions. Then, thank the participant for participating in this study.