2022

Analyzing Secure Access Strategies to Protect Clinical-Information Systems in the Healthcare Industry

Manjit S. Kang
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Manjit Kang

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. Gail Miles, Committee Chairperson, Information Technology Faculty
Dr. Jon McKeeby, Committee Member, Information Technology Faculty
Dr. Jodine Burchell, University Reviewer, Information Technology Faculty

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

Walden University
2022

Abstract

Analyzing Secure Access Strategies to Protect Clinical-Information Systems in the Healthcare industry

by

Manjit Kang

MS in Information Technology, Walden University (2015)

MS in Computer Science/Engineering, CSU (1998)

MS in Applied Mathematics, CSU (1995)

MS in Mathematics, India (1990)

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

January 2022

Abstract

Securing patient health records within cloud-based health records is a critical security challenge for hospitals and healthcare organizations. Some information technology (IT) leaders working in the U.S. healthcare industry or hospitals are concerned with their patient cloud-based health records due to data breaches in their healthcare systems. Grounded in the task technology fit theory, the purpose of this qualitative pragmatic inquiry study was to explore strategies healthcare information leaders use to implement security procedures to protect patient health records on private cloud-based clinical information systems (CIS). The participants were six IT managers in metropolitan San Francisco Bay healthcare facilities. The data was analyzed using thematic analysis, and four themes emerged: the importance of security procedures and policies, security awareness, cyber security response strategy, and user training. A key recommendation to healthcare IT security personnel is to team up with their cloud-based application security administrators to review current security procedures to ensure their security protocols can mitigate cyber-attacks on their network application servers. The implication for positive social change is to offer hospitals the ability to protect healthcare systems with security procedures and provides patients with assurances that their information is secure.

Analyzing Secure Access Strategies to Protect Clinical-Information Systems in the Healthcare Industry

by

Manjit Kang

MS in Information Technology, Walden University (2015)

MS in Computer Science/Engineering, CSU (1998)

MS in Applied Mathematics, CSU (1995)

MS in Mathematics, India (1990)

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

January, 2022

Table of Contents

List of Tables

Section 1: Foundation of the Study

Background of the Problem

The primary cause of data breaches in private cloud-based clinical information systems (CIS) in healthcare organizations has not been adequately identified (Kruse et al., 2017). The healthcare industry and healthcare providers had 1096 data breaches in their CIS or online electronics healthcare systems (EHRs) due to unsecured network systems (Bai et al., 2017). Bai et al.(2017) also reported that 33 healthcare industries were breached more than three times, which affected millions of patients' private records as well as their health insurance information. CIS systems are part of EHRs. Healthcare industries in the United States are transferring paper-based records to electronics-based records for over 10 years (Akhu-Zaheya et al., 2018). However, after the Affordable Care Act passed in 2010, healthcare industry began transferring paper-based patient records to a web-based EHRs system, which led to a quicker transfer of data (Lanford & Quadagno, 2016). The healthcare industry CIS systems are not adequately secured due to lack of proper utilization of usernames and passwords, which leads to data breaches problems like patient identity theft or patient privacy loss data (Kruse et al., 2017).

Many healthcare industries have experienced cloud-based patient record data breaches in the last 5 years. Studies on healthcare industry electronics data breaches indicate that 29 million patient records were compromised from 2010 to 2013 (Bhuyan et al., 2016). The study also showed that data breaches had increased significantly from 12% in two thousand ten to 27 % in 2010 to 2013 (Bhuyan et al., 2016). Many healthcare industries indicated that patient's EHRs were at high risk of a security breach (Bhuyan et al., 2016). Papoutsi et al. (2015) conducted a survey that showed growing data security breach incidents during the two thousand ten's impacted patients and the general public's opinion. The study showed that 79% of participants expressed some level of concern related to the safety of their information stored in U.S. healthcare industry EHRs (Papoutsi et al., 2015).

Problem Statement

The private cloud-based CIS in healthcare organizations had many data breaches in the past 10 years (McLeod & Dolezel, 2018). Banja (2020) reported that more than 300, 000 patient records of the Touchstone healthcare services database were compromised due to an unsecured CIS cloud-based system. The general IT problem is that health care network frameworks of some healthcare industries have security exposures that affect private cloud-based CIS systems in protecting patient data. The specific IT problem is that some healthcare information technology (IT) leaders lack strategies to implement secure procedures to protect patient health records on the private cloud-based CIS systems.

Purpose Statement

The purpose of this qualitative pragmatic qualitative inquiry study was to explore strategies of the healthcare IT leaders to implement secure procedures to protect patient health records on the private cloud-based CIS systems. The study's target population consisted of CIO, CISO, or IT managers, who protect patient health records using strategies to secure private cloud-based CIS systems. The geographical location of this study was healthcare industry located in San Francisco, California. The findings of this study may impact positive social change by protecting patient healthcare records. Finally, this study may be used to identify and close security gaps, as well as alleviating the security concerns of both patients and administrators using the above system.

Nature of the Study

A qualitative pragmatic qualitative inquiry study methodology provides researchers the ability to isolate the specific strategies (Waibel et al., 2015). Rresearchers use the qualitative methodology to prepare in-depth analysis report about the phenomenon in research study as they happen in their current environment (Alase, 2017). I used qualitative methodology to explore strategies of the healthcare industry IT leaders to implement secure procedures to protect patient health records on the private cloud-based CIS systems and appropriate for this study. I used a qualitative method to evaluate the implementation of information technology strategies used in healthcare industries to help minimize private cloud-based CIS application servers from data breaches such as cybercrime hacking, theft of mobile devices, insider accidents, or malicious insiders. A quantitative research study method is used to focus on data measurement, and collects the data through surveys, multiple-choice questions, or polls (Ludo, 2019). A quantitative research study was not appropriate because it is used to understand strategies – not measuring them. Mixed-methods research is a combination of quantitative and qualitative research design methods (Jacquelynn, 2018). As mentioned above, a quantitative research approach was not appropriate for this study. The mixed-methods research was also not suitable for this research study. I used a multiple qualitative methods to interview IT professional managers or administrators to investigate strategies in CIS system applications.

This pragmatic qualitative inquiry study design was appropriate for this study. Palinkas et al. (2015) suggested that many researchers have used purposeful sampling technique in pragmatic qualitative inquiry study design for the identification and selection of information-rich cases target participants needed for their research study. John (2015) defined case study as research that explores different information technology security strategies requiring direct interaction with the information technology managers or experts, who create and implement strategies to understand from their experiences. Phenomenology is used to analyze the commonly shared features of participants that experienced an unusual phenomenon (Gentles et al., 2015). Phenomenological research was not appropriate for this study because the focus is to understand the strategies,- not behavior. An ethnographic research design between participants and users and based on social connections between them (Steven, 2015). Steven (2015) further explained that the critical focus is the writing and reporting of service provider IT professional and user participant experiences (Steven, 2015). Since there is no direct interaction between the CIS system IT professionals and public users, ethnography was also not an appropriate choice in this research study. The pragmatic qualitative inquiry approach was a suitable choice in this research study because it aligned with the research question.

Research Question

The research question for this study was: What strategies do healthcare IT leaders use to implement secure access procedures to protect patient health records on the private cloud-based CIS systems?

Interview Questions

The research participants for this interview were IT security managers, who are responsible for the healthcare industry's private cloud-based CIS or EHRs systems

- What procedure have you used in the past to eliminate non-public cloud-based CIS or EHRs system data breaches?
- What, if any, general complaints from patients are related to the management or use of the CIS or EHRs data system?
- What type of private cloud-based CIS or EHRs system application training did you provide to staff or users in the past?
- Are you comfortable supporting a private cloud-based CIS or EHRs system? If not, what are your concerns?
- What are security risks you have seen related to a protected cloud-based CIS or EHRs system used in your healthcare industry?
- Have you discovered security loopholes in your healthcare industry network? If so, how were they remedied?
- Do you have a budget to implement new security procedures? If so, it adequate. If not, what should be done about it?

- Does your healthcare industry have IT security staff members who have the knowledge to implement new security procedures? How does this impact your ability to keep the system safe?

- Would more funding security tools help your organization prevent data breaches, or other measures are needed to minimize breaches? Why or why not?

- What measures are needed to minimize breaches?

Conceptual Framework

Goodhue and Thompson developed the task-technology fit (TTF) theory in 1995. The authors suggest a correlation between user performances and how well the technology matches the tasks performed by the user. Goodhue and Thompson (1995) said that TTF consisted of quality, authorization, compatibility, and location ability, project scheduling user training, user connection, and system reliability different factors. TTF focuses on technology attributes used in information technology systems. TTF connects with the tasks and characteristics associated with an information software technology system (Chen et al., 2015). Based on the healthcare industry IT managers and patient concerns of cloud-based application systems, I used TTF theory mapped the user tasks with web-based software technology, and it accomplishes the requirements of ongoing healthcare industry business strategies.

The TTF theory was a suitable framework for understanding information security breaches and strategies to address them. The TTF can be used to examine how a software technology solution can affect the team or individual user performance (Goodhue &

Thompson, 1995). The TTF is perfect for calculating a group or specific user's confidence regarding how technology solution satisfies user task needs, which could impact user performance (Zigurs & Buckland, 1998). Alharbi et al. (2016) reported that the hardware and software computing services using TTF provided to healthcare organization users or customers based on their demands to complete their business tasks called Infrastructure application as services (IaaS) cloud services. Since healthcare industry user tasks mapped to the technical aspects of CIS/EHRs systems, the TTF theory was appropriate for this research study.

Assumptions, Limitations, Delimitations

Assumptions

Assumptions are a researcher's practical expectations in their research study (Theofanidis & Fountouki, 2018). One of the premises was that this study complied with participating healthcare industries' rules, regulations, and policies. I assumed that I would not have any issues getting access to the contact information of potential participants. I also expected many people who work in the California healthcare industry to agree to participate in my study.

Limitations

The limitations are the restrictions of a research study that can impact the qualitative study results. The limitations were factors such as unrestricted shortage, conditions, or less geographical location that might affect research study EHRs web application systems (Theofanidis & Fountouki, 2018). Brennan et al. (2017) explained that limitation reporting was vital as it provides the reference to other researchers to consider in their study. The main limitation of this study was that it confined to the geographic area of the San Francisco Bay Area, which includes only three healthcare industries. Since potential participants were from the same geographic region limited issues that healthcare industry in other areas face. The number of healthcare industries and the location of healthcare industry were limitations of my research study.

Delimitations

The delimitations are the researcher's research study boundaries (Theofanidis & Fountouki, 2018). Researchers should ensure that the delimitations conditions align with their study's purpose. The first delimitation was that only IT managers interviewed not technical contractors or consultants working in that healthcare industry. The second delimitation was that this study focuses on only the healthcare industry's CIOs, CISO, or IT managers, because they were responsible for managing the procedure to secure their cloud-based CIS systems.

The Significance of the Study

The significance of this research study was to explore IT strategies that may help health insurance's IT professionals minimize cloud-based CIS data breaches by using a multiple qualitative case study approach for two healthcare industry located in San Francisco, California. My primary goal was to identify the security strategies of healthcare industry IT leaders used to secure access procedures to protect private cloud-based CIS/EHRs systems. There is always a need for more information when trying to secure the network and I explored gaps or flaws in best security practices. By identifying weaknesses or gaps within security strategies, I attempted to determine the best procedures and practices. This study may provide valued to IT managers to help them implement new data security strategies focusing mainly on the US healthcare field, which will comply with US government laws and policies.

I identified the best security strategies that could be used by the health organization's IT managers to secure their cloud-based CIS systems by identifying gaps in current IT strategies. By using proper processes, these IT managers could provide network security through validation to protect patient records in their online cloud-based CIS systems. The implications for positive social change from this study are helping health community members to feel more secure and comfortable using online private cloud base CIS application systems. This research study may be used by IT managers, to avoid individual cloud-based CIS system data breaches.

A Review of the Professional and Academic Literature

My goal for this study was to explore strategies of the healthcare industry information technology (IT) leaders to implement secure procedures to protect patient health records on the private cloud-based CIS systems

The Literature Search Strategy

The research topic keywords that I used to find the proper academic peer-reviewed references are task technology fit Theory, TTF, clinical information systems security risks, analysis of current healthcare industry CIS system security data breaches, risk management strategy, optimally secured system requirements, mobile device user access security, HIPAA and governance with government laws, Cloud-based CIS security risks, clinical information systems (CIS) systematic review, and CIS healthcare industry data breaches reviews.

I searched databases including Academic Search Complete, EBSCO, Google Scholar, ProQuest Central, and Science Direct by using relevant research topic keywords, as mentioned above. I collected, reviewed, and categorize around 125 references; I selected all 125 these references related to this doctoral study research. More than 97% are from peer-reviewed academic articles, verified by the Ulrich Periodical Directory through Walden University web application system. All of these articles published within the past 5 years.

The literature review focused on the causes of the private cloud-based Clinical Information Systems (CIS) in health care organizations' data breaches. The CIS systems are part of Electronics healthcare records systems (EHRs).

A Review of TTF Theory

This research uses TTF as the foundation of the study. Goodhue and Thompson developed the TTF theory in 1995, which provides a framework model that adjusts a measure of user performance depending upon user tasks with technology. Goodhue and Thompson (1995) identified TTF as a measure of performance using (a) task characteristics (b) technology characteristics as input and produce the output, (c) performance impacts, and (d) utilization. Goodhue (1998) explained that TTF consisted of quality, authorization, compatibility, and location ability, project scheduling user training, user connection, and system reliability different factors; those were the major required factors for secure access procedures of CIS/EHRs systems and were directly relevant to my research study question. Every factor listed above has a set of questions measured on scale 1-5 ranging from *strongly disagree to agree strongly* (Goodhue & Thompson, 1995). The data gathered from these questions and their answers would be excellent indicator of job performance and the TTF is used in a wide array of IT systems for analysis (Goodhue & Thompson, 1995). Wu and Chen (2017) suggested that TTF was used to examine the reasons for participant's acceptance of new technologies. Williams (2018) used the upgraded version of TTF theory in his doctoral information technology study to explore the challenges in video game development strategies. Miko (2017) also used the modified version of TTF theory in his doctoral information technology study to reduce technical debt by collaborating strategies. The TTF has matched the capabilities of technology with the requirements of the task by measuring the degree to which the technology would assist an individual in performing a task (Wu & Chen, 2017). The TTF maps the user tasks with the capabilities of technology to implementing secure procedure strategies for cloud-based application systems.

The information technology solution aligned with user task properties helps the managers or users see the expected results in micros seconds, which is the foundation of TTF (Dang et al., 2018). The capability of information systems networking technology matched with user requirements should increase the individual performance quality and efficiency (Gebauer et al., 2005). Zigurs and Buckland (1998) expanded the ideas of TTF theory to include a group of information systems or a group of particular users in the companies. They further studied the connection between specific teams' use of technology, the selection of the technology, and performance impact degree. The TTF theory process matches with security procedures used to implement the IT strategies in securing cloud-based CIS systems.

The TTF theory posits that when user task characteristics match software application technology, more users will be able to use that software application technology. The TTF uses task and technology characteristics as input to a diverse range of business information systems and produces the information system outputs based on those application systems algorithms (Gebauer et al., 2005). Gebauer et al. (2005) suggested that TTF as a three-way communication between the following processes:

- Managerial tasks such as operationalized by non-routineness, interdependence, and time-criticality;
- Computer information systems have different attributes functionality, user interface, and adaptability; and
- Information systems use contexts such as operationalized by distraction, quality of network connection, previous experience, and mobility.

TTF theory suggests that cloud-based application system users feel more comfortable when client task characteristics map with software application technology.

TTF Theory Application

Many researchers have used TTF theory to select specific technology out of other available technologies depending upon business requirements to support user tasks. Erskine et al. (2019) used TTF theory to identify individual user characteristics for an experiment designed to model geospatial decision-making performance with and without the aid of data visualized using heat maps. The TTF applies to qualitative, quantitative, or mixed-mode research studies involving information system applications across the different parts of the world to provide solutions to business or public related problems (Dang et al., 2018; Erskine et al., 2019).

According to TTF theory, decision-making time, accuracy, and satisfaction are measures of decision-performance. The user task characteristics are influencing the previously stated measurements and technical aspects that impact their decision- making and TTF provides the foundation for their conceptual framework (Erskine et al., 2019). Erskine et al. (2019) suggested that the TTF inputs were personal innovativeness, self-efficacy, intrinsic motivation, relative advantage, and geospatial reasoning ability produced the output of Individual characteristics. They further explained decision-making satisfaction, time, and accuracy were decision performance indicators or measures, which can be the output of the conceptual framework. With the use of TTF theory, many organizations in healthcare industry providing online cloud-based software technology services and user output response increased (Dang et al., 2018). The software technology is used to organize the data accurately, which makes the user use that application comfortably, and the user satisfaction level goes up (Dang et al., 2018). The TTF is the measure to which a cloud-based technology may assist the group or user in the performance of tasks to implement secure access procedures of CIS cloud-based systems.

When IT managers use software technology solutions with TTF, EHRs application systems study showed that user performance and satisfaction increases (Dang et al., 2018). Dang et al.'s (2018) results showed that TTF significantly affects user acceptance of using cloud-based online application systems. Ratna et al. (2018) explained that technology characteristics and task characteristics played a significant effect on TTF, which supports that the more value of the technical aspects task characteristics and produces a better output of the TTF theory. Ratna et al. (2018) further explained that the use of software application systems matched with user tasks to support the company or healthcare industry work environment, the more users will utilize that technology solution in their businesses. Ratna et al. (2018) suggested that customer or user acceptance measured by perceived ease of use, perceived usefulness, the intention toward the usage of the new technology, and attitude towards usage of the latest technology as four different factors. Wu and Chen (2017) used the TTF model to calculate how data technology leads to an increase in the output by testing the match between technology characteristics and task characteristics. They further explained that a specific user or employee' experience with the information application system helped them with the adaption behavior of that technology. With the proper mapping of the TTF theory to the cloud-based online application, the system helps the users operate the online application comfortably.

The TTF theory was strong foundation for my research study by supporting strategies to protect CIS/EHRs application systems. Wu and Chen (2017) used the TTF model as part of the structure in a survey to a unified model integrating the TTF and massive open online courses (MOOCs), which features student engagement with other online student users. They reported that their survey results showed that their framework integrating the technology acceptance model (TAM) and the TTF models produced a complete understanding of the behavior of the MOOCs system. The TTF plays an essential role in analyzing the various theories and technology models to develop an integrated cloud-based online e-payment system known as the single platform e-payment system (Lai, 2017). The TTF plays a critical role to establish a private cloud-based online application system to provide customer or user support depending upon organization business requirements

TTF Theory Implementation Strategies

Patients, as well as healthcare industry staff members, are worried about the patient's private information; if a healthcare industries' online system is not compliant with health insurance portability and accountability act (HIPPA). Aldosari (2017) noted that it was a significant challenge for doctors or IT managers to secure the health records systems from hackers due to lack of user training or not using updated secure medication communication hardware and software technology. This type of network security problem happens when user data entry is not configured on network devices properly with proper sufficient firewall, router configuration, or encryption issues between server and client devices (Aldosari, 2017).

TTF Theory Relation to CIS systems Security Risks

The lack of private cloud-based EHR/ CIS system applications user training is one of the causes for healthcare industry patient record data breaches. Goodhue and Thompson (1998) showed that user training is an important part of TTF, which outputs good results of user acceptance of application software technology. The user training and user communication are an essential part of TTF theory (Dang et al., 2018). The lack of professional security training to IT managers and user training to healthcare industry staff members can cause the data breaches of patent records on cloud-based EHRs/CISs systems (Chen & Benusa, 2017). Many patients worry about their healthcare privacy records when they use an online cloud-based CIS/EHRs system to make a doctor's appointment or get other medical services from the healthcare industry (Bhuyan et al., 2016). Dental offices, healthcare industry , medical clinics, long-term care facilities, or other medical service providers with one to 200 employees were facing HIPAA information security (InfoSec) compliance challenges due to security gaps on their online medical EHRs systems (Chen & Benusa, 2017).

Williams (2018) used the updated version of TTF as the conceptual framework in his doctoral information technology study to explore the challenges in video game development strategies. Weak user credentials and lack of user training are some of the causes of the cloud-based EHRs/CIS application system data breaches. Goodhue and

Thompson (1998) defined TTF consisting of system user credential authorization accessing data or user credentials. Khan and Latiful-Hoque (2016) further reported that weak user credentials were the causes of the average number of breached records, which were 29,199 in Arabian Cluster, 19,788 in Australia, 22,902 in Brazil, 20,456 in Canada, 21,695 in France, 20,456 in Germany, 24,103 in India, 18,983 in Italy, 28,798 in Japan, 21,695 in the United Kingdom, and 19,214 in the United States. Comparison of the cost of each data breach record in different industries, the value for the healthcare industry was ranked top in the list (Khan & Latiful-Hoque, 2016). Rathert et al. (2017) reported that user training part of TTF is not enough to protect the patient's records from data breaches. The cloud-based EHRs/CISs application system security procedure should improve user security and better communication between healthcare industry employees, patients, or other users (Rathert et al., 2017).   IT leader's lack of skills in securing cloud-based CIS/EHRs systems leads to patient record data breaches (Edwards et al., 2016).

TTF Theory Relation to Remote Access to the Application Software System

The misconfiguration and lack of security of the cloud-based online EHRs/CISs application systems are the leading causes of patient records data breaches. The system misconfiguration and remote access are the two factors to the cloud-based software application based on the TTF significant features such as user device location, user connection, and system security reliability (Dang et al., 2018). Khan and Latiful-Hoque (2016) mentioned that the leading causes of the data breaches were remote access to cloud-based application systems and misconfiguration of them mobile devices as well as application servers located at remote data centers. Many security loopholes were possible in Wireless Mesh Networks (WMNs) due to low cost, quick implementation, and easy maintenance (Sgora et al., 2016). Sgora et al. (2016) also noted that WMNs had more chances of networking security vulnerabilities to healthcare server applications and user end devices, including desktops, laptops, mobile devices, or medical data storage X-rays machines. Many healthcare data breaches occurred in 2010-2015 due to server-client network security open ports or firewalls that were not configured correctly either on server application systems or user devices (Sgora et al., 2016). The user devices mobile laptops or smartphones connected with the wireless network using TTF to access a cloud-based clinical information application server system that had more chance of patient privacy data breaches as part of user security risks (Alharbi et al., 2016). The hardware and software computing services using TTF provided to healthcare organization users or customers based on their demands to complete their business tasks called infrastructure application as services (IaaS) cloud services (Alharbi et al., 2016). The cloud consisting of computing technology IT resources located at different locations of the same company or organization was called private cloud (Alharbi et al., 2016).

The combination of public and private clouds was called a hybrid cloud. The primary objective was to secure the end to end IoT mobile devices with user authorization and authentication login process, device identification with user information, tracking, and monitoring user’s networking activities as part of Infrastructure application as services (IaaS) (Thota et al., 2018). Many healthcare service provider organizations or healthcare industries could reduce their IT services cost by using cloud-based IT services (Mehraeen et al., 2016). Still, it could increase their security risks related to application systems uptime, patient privacy concerns, or patient data security (Alharbi et al., 2016). Some networking router or gateway provided a communication environment that is part of TTF to receive or transmit data from a networking device located in one city to another city that could cause security risks (Ratna et al., 2018). The proper security configuration of the cloud-based online EHRs/CISs application systems can help the IT managers to reduce the healthcare industry data breaches.

TTF Theory Relation to Social Engineering

The lack of security updates and security protection procedures on the cloud-based online social engineering applications systems are the leading causes of user's private records data breaches (Bai et al., 2017). The lack of system security and networking protection procedures of the cloud-based software technology application based on TTF's significant features such as user device location, user connection, and system security reliability (Dang et al., 2018). Dang et al. (2018) further explained that if the healthcare information technology offers threat protection on their network following the features of TTF by offering user training programs before users start using the online application, it would help the users avoid social engineering attacks. Albladi and Weir (2018) reported that social engineering is the leading cause of increasing the cloud-based application system security risks and user's private information. They found that the social engineering part of technology usage is the leading cause of data breaches cloud-based healthcare application systems. There was a need for a faster centralized safe and protected network of many Internet of things (IoT) devices used in private or public cloud-based electronics healthcare records systems (Thota et al., 2018). Poorly managed cloud-based CIS/EHRs application systems security could be at risk when users are responding to social engineering messages that come from other users on the network using IoT devices following the guidelines of TTF.

Importance of TTF Theory as a foundation for this research

A conceptual framework is a framework system in which there are concepts, theories, assumptions and limitations, expectations, and outputs. Singh (2017) defined a conceptual framework as a visual diagram or written product, one that “explains, either graphically or in narrative form, the main things to be studied such as the key factors, concepts, or variables associated with the purpose statement of the study.

TTF theory is being used as a foundation to explore strategies used by executive CIO, CISO, or IT Managers to protect patient health records on the private cloud-based CIS systems as well as to minimize the security exposures of network frameworks used in some healthcare industries health care systems. The TTF theory is an essential part of the research study’s foundation. The tenets of TTF provide a method to match the capabilities of technology with the requirements of the task by measuring the degree to which the technology would assist an individual in performing a task (Erskine et al., 2019). Erskine et al. (2019) reported that they had significant advantages of using business task characteristics and technical characteristics that impact their decision-making to choose TTF theory. The TTF theory is suitable for this research to explore information technology security strategies in securing access procedures in current healthcare industry cloud-based CIS/EHRs online systems in California.

The TTF theory focuses on technology attributes used in information technology systems and connects with the tasks and characteristics associated with an information software technology system (Chen et al., 2015). Goodhue and Thompson (1995) developed the TTF theory that used task and technology characteristics as input parameters and produced performance-impact and utilization as an output. Chen et al. (2015) adopted the theory for connecting mobile business environments task attributes with technical characteristics of emerging mobile technology. TTF is appropriate for this research study because it provides a high mapping of healthcare industry business tasks to IT strategies in implementing secure access procedures to protect-cloud based CIS/EHRs online systems used in healthcare industry.

In this study, the TTF theory can set a framework for mapping healthcare industry business tasks to IT strategies in implementing secure access procedures to protect-cloud based CIS/EHRs online systems. Malley et al. (2015)'s study showed that healthcare industry information technology managers divided teams in a way to minimize challenges related to private cloud-based CIS/EHRs. These CIS or EHRs IT managers had a lack of integrated care management software and care plans in private cloud-based CIS, poor practice registry functionality and interoperability, and inadequate ease of tracking patient data in the CIS systems for some time (Malley et al., 2015). Singh (2017) showed that the survey study showed that the healthcare industry information technology team faced many challenges, such as lack of knowledge about the cloud-based CIS/ EHRs online application systems. Based on the above review, this is a significant challenge or problem for healthcare industry IT managers, and it aligns with my research question.

The principles of TTF provide a procedure for a detailed understanding of comprehending EHRs companies' usability processes using TTF, which do not reach the proper level of EHRs company's best practices (Ratwani et al., 2016). User satisfaction, which is part of TTF, consists of many components such as user's EHRs systems satisfaction, user satisfaction with usefulness, easy to learn system level, user comfort level, and overall satisfaction (Abouelmehdi et al., 2018). The TTF based on the availability of the CIS or EHRs technology resources such as computers & networks infrastructure resources and user training, which is equivalent to task characteristics and technology characteristics of the TTF theory. The TTF defined use and usefulness: as utilization, use of frequency of the system, and list of tasks processed by the system. TTF produces the output as performances of usability and the ability to learn the system for users and managers.

The security gateways or network security devices access procedures help the healthcare industry to protect their cloud-based CIS/EHRs systems used. The security gateways validate the cloud-based CIS/EHRs application system user's credentials using mobile devices (Verba et al., 2017). The security gateways are part of Platform as a Service (PaaS) gateway used to store the specific driver database information to check which application to apply for networking routing tasks (Alharbi et al., 2016). The managers, patients, doctors, nurses, or other healthcare industry employees are the users of cloud-based CIS/EHRs application systems and their access level permissions based on their employment status or level using the TTF input-output features (Wu & Chen, 2017). The patient or healthcare industry user identity, user profile, and group management functionality were part of the cloud-based EHRs application system, which communicated with other software applications within the same method to manage a large number of user credentials, groups, and patterns with the use of updated version TTF (Chard et al., 2016). The different forms of the patient record application system such as healthcare industry employee, billing, insurance, accounting, inventory, etc. communicated with each other in different domains crossed organizational boundaries security risks, which could be challenging for company managers by using Single-Sign-On (SSO) user access the hardware as well as software application resources (Chard et al., 2016). The cloud-based CIS/EHRs application system is a web-based user interface that helped the IT managers, healthcare industry employees, or patients.

The healthcare industry CIS/EHRs application system organizes the health records database and the data received from bio-medical scanning devices to do the patient's test or patient lab test depending upon the doctor's recommendation with the use of TTF theory (Wu & Chen, 2017). The healthcare industry with the modern architecture of cloud services provided a high-throughput neuro-informatics user acceptance framework with updated version to do automated brain MRI segmentation and remote calculation by using analytical tools with cloud Web-based user interfaces (Mori et al., 2016). Some EHRs application systems software as a Service (SaaS) and many security risks are associated when one application access data from other application systems as part of distributed systems. The cloud-based server-client model provided large or faster output by using distributed servers using TTF located at different geographical locations (Wang & Lin, 2019). Many healthcare service provider organizations have adopted Software as a Service (SaaS) cloud service model to provide Information technology services to their company employees and customers (Van de Weerd et al, 2016). The cloud-based CIS/EHRs application system using TTF could have many security risks when one application access the data from an application running on medical machines used in the healthcare industry to do the patient's medical testing (Wang & Lin, 2019). The above-mentioned procedures are part of the IT strategies to implement security access procedures of the healthcare industry's CIS/EHRs application system and related to my research question.

The user's task mapped to a private cloud-based CIS technology system with TTF is an important factor in preparing access procedures strategies of private cloud-based EHRs application systems. The cloud-based EHRs application systems included Software as a Service (SaaS) using the TTF theory (Wang & Lin, 2019). The healthcare industry or medical service provider organizations can choose one or more cloud service types based on their business needs (Alharbi et al., 2016). The healthcare industry's information technology professional managers can use proper strategies to divide tasks among separate departments such as patient's services, doctors, nurses, healthcare industry management, system administration, billing department, or insurance agencies. The healthcare industry healthcare insurer’s information technology professional manager, CIO, has used needed strategies to divide tasks among different departments (Blijleven et al., 2017).

The information security TTF framework includes an organization’s functional user, location devices, and their interaction with the private cloud-based CIS servers (Wang & Lin, 2019). According to Chen and Benusa (2017), the healthcare industry healthcare’s CIO needs to adequately plan for an information security strategy, which is also compliant with company security policy as well as government data laws (Chen & Benusa, 2017). The user training will ensure that users feel more comfortable using the CIS web application system (Chaturvedi et al., 2019). The TTF theory, with the user’s task mapped to a private cloud-based CIS technology system, aligns with the research question.

Chen and Benusa (2017) showed that the healthcare industry information technology team faced many challenges related to HIPAA, including lack of integrated care management software and care plans in EHRs, poor practice registry functionality and interoperability, and inadequate ease of tracking patient data in the EHRs for some. Wang and Lin (2019) found that there was a significant security improvement in sharing, reading, and updating information with the use of CIS/ EHRs) online application systems. They used the TTF theory to improve patient access for better communication, patient engagement, and user’s self-management confidence in EHRs cloud-based systems (Wu & Chen, 2017). Rathert et al. (2017) recommended that the IT security manager or system administrator should use the security mentioned above technique to create role-based access to the EHRs systems and notify the users to logout from the networks when they were not using it. These security techniques would help to avoid patient record data breaches in the future.

The TTF theory divided into domains based on the user's workgroup, user application task characteristics, and locations of client devices communicating with CISs/ EHRs web application server to provide services to the clients (Salleh et al., 2016). The EHRs web-based system using TTF can have multiple electronic medical record owners as well as EHRs users, and there can be a Microsoft windows server active directory for each user group such as patients, nurses, doctors, or others depending upon the healthcare industry business operating policies (Salleh et al., 2016). Wang J et al. (2020) mentioned that technical communication using TTF provided the structure between users from their client devices with EMR web application servers to perform their business activities. Salleh et al. (2016) further explained how mobile CIS/EHRs web application users, such as nurses, pharmacists, and doctors are using online medical web applications by using their proper credentials to log in to the system to provide their services to the clients. The cloud-based public health records web-based systems used in the healthcare industry using a server-client model had risks associated with moving the infrastructure and sensitive patient data from healthcare industry to the cloud, posing severe security and privacy risks (Van de Weerd et al., 2016).   Rasmi et al. (2018) mentioned that users' private login or their other personal information is at risk using, when they use cloud-based EHRs application systems. EHRs application system data security is at high risk when a cloud-based system is not secured using firewalls and proper data encryption between clients to the server.

The security strategies for EHRs application systems plays an important role in securing access procedures to protect patient health records, data accuracy, and user satisfactions are measures of IT managers' decision-performance. Koczkodaj et al. (2019) explained that 29 million private patient health records were compromised between 2010 and the end of 2013. Smith (2015) further found that the Department of Health & Human Services (HHS) reported data breaches involving 500 or more patient records covered under the Health Insurance Portability and Accountability Act (HIPAA). Koczkodaj et al. (2019) also found that there are many information security risks or gaps in current EMR web application models that should resolve in the future. Users, such as patients, can make appointments, reschedule, or cancel appointments online by using the HHS EHRs web application.

Some cloud-based EHRs application systems have many data security risks and patients do not comfortable using those application systems. Smith (2015) found that because current models have data security risk gaps, patients do not feel comfortable using the healthcare industry’s online EHR web application since many healthcare industry records hacked in the past. Koczkodaj et al. (2019) showed that there is a gap in US healthcare industry CIOs and IT managers when using strategies to implement secure access procedures to protect patient health records on the private cloud-based CIS systems. The healthcare industry’s Chief Information Officer should adequately plan for information security strategy and be compliant with company security policy as well as government laws (Chen & Benusa, 2017). The CIS/ EHRs security risk management strategy should include testing all the systems and applications, which follow the company's business security policies as well as government laws (Bahga & Madisetti, 2015). The proper testing and user training can be helpful to the community giving patients easy access to their records, having them feel more comfortable using the EHR the web application system from anywhere by using the Internet. The user's task mapped to the CIS/EHRs technology system with a qualitative research method is supported by TTF.

Contrasting Theories

Cloud-based Big Data Model Theory

Many healthcare service provider healthcare industries use cloud-based technology clinical information application systems aligned with business functions (Angappa et al., 2018). There is a gap between healthcare industry service support functions and CIS application systems. Some studies have shown a difference between organizations that adopt information technology systems in their health care businesses (Evans et al., 2017). Many companies, including health care service providers, collected public data by using cloud-based big data services and used that information to complete their business-related tasks (Zuchowski et al., 2016). Zuchowski et al. (2016) used a method called internal crowdsourcing, which was different from external crowdsourcing and different management application access level at varying levels of company employees. Zuchowski et al. (2016) examined 74 peer-reviewed articles in the internal crowdsourcing research area with proper academic literature review, and they identified some areas with conflicting finding. Since this cloud-based big data model theory shows that there is gap between healthcare industry service support functions and CIS application systems, so my study is more aligned with TTF theory as compare to Big Data theory, so I have chosen TTF theory for my study.

Person-centered care (PCC) model theory

Healthcare organizations have used healthcare improvement application systems with “Structure,” “Process,” and “Outcome” categories to form a group person-centered care (PCC) model sectors (Santana et al., 2018). Santana et al. (2018) developed person-centered care (PCC) model for faster communication between healthcare industry and patients. Many companies, organizations, and medical service application systems were considering using person-centered care (PCC) model for speedier communication between patients and health services providers (Santana et al., 2018). Santana et al. (2018) designed and utilized a PCC model framework with the cooperation of patients, healthcare industry staff, medical doctors, and healthcare management teams, and using a case study research method. Some medical organization have used PCC model framework in their system applications.

The person-centered care (PCC) model used in the United States consists of healthcare adopted business terms, patients or users’ medical care process, relationship application model of customer care, and client- servers patient records systems (Santana et al., 2018). Many health care providers’ online health record systems have used PPC resources to guide women to have better maternal outcomes results (Howell et al., 2018). The healthcare cloud-based application systems (EHRs) have played an important role in providing improved healthcare quality services to patients in healthcare industry (Degenholtz et al., 2016). The cloud-based application systems used in many medical service provider organizations in communication between patients, doctors, nurses, or healthcare industry managers (Degenholtz et al., 2016). Therefore, person-centered care (PCC) framework could be another option for healthcare industry for quality improvement, data transfer, and compliance with government laws, online structured clinical documentation, and procedure used in medication to their patients. This theory deals with large datasets that consist of public and private databases located in different states of the United States and this theory causes security risks to the patient private data, which is not a helpful framework in my research study.

Analysis of Potential Themes/Phenomenon: Security Strategies for EHRs

A major responsibility of IT managers is to use a set of procedures securing the cloud-based EHRs/CISs application systems to provide services to healthcare industry employees, patients, or other users. IT managers can ask their support team to follow the EHRs/CISs application systems security checklist (Day et al., 2019). Day et al. (2019) further suggested that the IT managers collect and analyze the security information reports needed to secure their EHRs application systems. Many healthcare industry or medical offices are using the cloud-based CISs /EHRs healthcare application systems to provide medical services to patients at a faster speed (Lopez & Sekaran, 2016). Manogaran et al. (2017) reported that securing online healthcare application system helps healthcare industry decrease the patient cost, a quick patient appointment with doctors, patient medical treatment, patient re-admission process, patient online prescription, consultation with doctors, or and response between doctor and patient at a faster rate with the use of technology virtual meeting such as Zoom meeting.

The end to end encryption is one way to secure the data from the source client application system to another destination server application system. Huang et al.(2018) mentioned that many healthcare industry ' EHRs are stored on untrusted cloud-based servers. They recommended using the encryption strategies algorithm such as attribute-based encryption on client-based application system before submitting user data to the server-side application system.   Nagasubramanian et al. (2020) explained that the loss of patient's confidential data could cause a severe security risk of the healthcare industry EHRs' cloud-based application system. They provided the solution to this problem to use the keyless signature infrastructure to ensure the digital signature security and authentication process during data transfer from source to destination cloud-based application system. They have suggested using blockchain technology to encrypt user data, which takes 50% less time, file size , and 20% cost less associated in transferring data from one machine to another compared to other conventional data storage techniques. If needed, Based on the research, healthcare industry IT leaders should use the end-end encryption data in their cloud-based EHRs/CISs application systems when the user submits the data from the client device to the server application system.

Data transfer can be vulnerable during data transfer from one system to another such that of the middleman downloading or copying the patient's confidential data if it is not encrypted. Thota et al.(2018) recommended using an efficient centralized, secure architecture to secure IoT based devices used by healthcare industry EHRs application systems users doctors, nurses, and lab technicians to transfer patient data from their mobile devices cloud-based EHRs/CISs server system. They reported that collected patient data should be secured on healthcare industry's network using https protocol from sensor based devices connected with the patient and then transferred to other system located on cloud-based application system. This data could be reviewed by healthcare industry staff or doctors to monitor patient's current condition and later provide medical treatment based on their observation of the data. They further suggested identifying and tracking the sensor-based devices using authentication and authorization secure procedure in transferring the data one device to another in cloud-based EHRs application systems. Rawal et al. (2018) reported that infrastructure, network services, and software applications cloud services are part of many the healthcare industry EHRs/CISs application systems. They also reported that many mobile devices had a finite rate of failure, and the hackers used intrusion with complex and a sophisticated procedure, which causes the security failure rates to up in cloud-based EHRs application systems. They further suggested to the IT managers to use https or ssh in their cloud-based application to transfer data from one device to another in order to avoid security risks in their application system.

Many researchers suggested that healthcare industry healthcare technology or information security managers should backup their cloud-based application data on their local sites. Otherwise, hackers can launch ransomware attacks and ask healthcare industry organizations for ransom’s fee to retrieve healthcare industry patient data. Ido et al. (2019) recommended that medical service providers should backup their patient health records data on their local sites from the cloud-based application servers. They also found that Japan healthcare industry ' IT managers backup more than 11 million patients with more than 420 million data items in 2018; more than 900 facilities were Miyagi Medical and Welfare Information Network (MMWIN) users number of patients consenting to share their clinical information reached 90,000. This type of backup data became an excellent resource for future research. Bachiri et al.(2018) explained the security risk associated with the pregnant women privacy data collected from mobile devices using healthcare industry EHRs application system. They suggested that healthcare industry could backup the patient data on their servers to resolve ransomware problems.

The EHRs cloud-based application network vulnerabilities can open access to patient health records for cyber-attacks, which causes healthcare industry patient privacy data at high risk, and healthcare industry could spend billions of dollars as fines to compliance with federal government laws. Tieu et al. (2017) said that many patients accessed their online health record application to make their appointment and communicate with their doctors to get their medical services. They also reported that cloud-based application system vulnerability, lack of user system training, and weak user passwords could put patient health records data at high risk. They suggested that healthcare industry managers monitor online application user activities, do internal network security audits, and provide user training to all users of the EHRs cloud-based application system. Once users complete and pass the training, they can use healthcare industry EHRs application system to perform the online medical services activities.

Moosavi et al. (2016) explained that the following are security access challenges to access cloud-based EHRs application system from IoT devices and other mobile user devices:

- The healthcare industry IT managers develop access procedures to eliminate the gap between the cloud-based service provider and users.
- The data synchronization procedures used to integrate the healthcare online application system and other parts of the network application could be on the private or public cloud-based on the IT manager’s choice.
- The secure access procedure should develop faster communication between cloud-based EHRs and user devices.
- Service-oriented architecture (SOA) improves communication between different parts of the network devices and user devices.
- The advanced authentication and authorization process must to secure the healthcare industry resources and patient’s private information. The implementation of the Advanced Encryption Standard (AES) algorithm helps IT managers to secure the healthcare industry resources, user’s confidential information, and IoT device information.
- The access to data center processes is developed to use the triple-layer authentication such as login credentials, use of the biometric device, and system-generated passcode sent to user’s mobile phone system

- The proper user training process helps the IT managers and application system users feel comfortable using that the EHRs application system.

Issues of implementing security strategies

Many healthcare industry employees such as doctors or nurses use their mobile devices to response to patient calls at work, which makes patient's private information is at high risk on healthcare industry staff's mobile devices. Many mobile device users are not familiar with how online applications are installed on their mobile devices or the risk associated with the user's private data (Muzammal et al., 2018). Many doctors, nurses, and other healthcare industry staff are using smartphones to access CISs/EMRs application systems to provide their healthcare services to the patents (Abouelmehdi et al., 2018). Muzammal et al. (2018) reported that many users did not pay attention to granting permissions and user's private data policies. This practice led to distribute user's data on many other network servers without the user's knowledge (Muzammal et al., 2018). When users manage these healthcare applications on their smartphone, the user data gets exposed to the network devices on the mobile network, and many users became victim of identity theft. Abouelmehdi et al. (2018) mentioned security challenge issues of those medical IT managers to secure the medical professional's mobile devices to protect patient's private information. Abouelmehdi et al. (2018) explained that security strategy compliance with Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) could help the IT managers protect patient's information data accessed or updated from doctors' mobile devices.

Many healthcare industry staff members use wireless wearable sensor devices connected with patents to monitor their conditions 24 hours to send or receive their medical information from medical records with the use of cloud-based EHRs systems (Bao et al., 2017). Some wireless wearable sensors used body sensor networks (BSNs) environment by using cryptographic key management processes, but data transmission is not secure due to the complexity of mobile systems (Bao et al., 2017). Bao et al. (2017) suggested a data partitioning and scrambling algorithm as an add-on security mechanism could help protect data transmission from the user wearable device to cloud-based EHRs application system

A major responsibility of IT managers is to create access procedures to secure the EHRs by using the several processes or strategies. The user knowledge of user credential information such as username and password and user authentication processes are essential (Jayabalan & O'Daniel, 2019). A study by Simpao et al. (2018) showed that many healthcare industry and other clinical offices lack identifiable user credentials knowledge and did not used strong password strategies on their onsite computer systems, Some of the systems did not have the login credential at the operating system level (Simpao et al.,2018). Ramani et al. (2018) suggested that strong credential strategy, biometric tool authorization, and token-based authorization were a critical requirement of the EHRs application systems used in healthcare industry. Many student use generic login credentials for their EHRs system to complete their assigned tasks were the cause of the data breach in their organization (Simpao et al., 2018).

IT managers or security administrators have the responsibility to monitor, detect security vulnerabilities, and protect user data in the EHRs application system. Adamu et al. (2020) explained that weak authentication, cross-site scripting, SQL injection, and cross-site request forgery are the EHRs application system security vulnerabilities. They suggested that networking detection and monitoring tools can reduce the security vulnerabilities in the EHRs application system. Farhadi et al. (2018) reported that many IT managers did not configure EHRs application system properly at the user access level, which leads to patient record data breaches in medical offices. Some healthcare industry or clinical offices used the open-source EHRs application systems in their organization to reduce cost, but open-source application system runs many applications in the background and provided remote access to that EHRs application (Farhadi et al., 2018.). Based on this research, the security configuration tools of the EHRs application can help the IT managers to close unwanted applications or ports on those network systems.

The use of anti-malware services is an important part of the access procedure to secure the cloud-based EHRs application system. Information technology managers should run antivirus and anti-malware services to reduce the malware attacks on the EHRs system (Muzammal et al., 2018). The malware could infect the healthcare industry EHRs application server, and it may cause the EHRs server not available to the users (Cottrell et al., 2018). Cottrell et al. (2018) suggested that IT managers could use antimalware services on the EHRs application server to avoid this type of attack.

User training is an essential part of the EHRs application system to protect patient records in healthcare industry. The lack of EHRs application system user training, government policies, patient payment system, user task distribution, or resource allocation could cause security gaps in the healthcare industry network application system (Tutty et al., 2019). Tutty et al. (2019) suggested that proper or certified EHRs application user training could help the healthcare industry to reduce the data breaches in their application system. Cottrell et al. (2018) also reported that proper user training could help the healthcare industry or medical offices to reduce the hacker's attack on the EHRs application system.

Literature Gap

The purpose of the pragmatic qualitative inquiry study is to evaluate strategies to protect patient health records on the private cloud-based CIS systems as well as to minimize the security exposures of network frameworks used in some healthcare industry ' health care systems. Peer-reviewed articles and literature have identified that there is a gap in academic writing in regards to finding the security exposures of network frameworks in United States healthcare industry , which cause many data breaches in healthcare industry and cost billions of dollars in payments of lawsuits in the past (Khan & Latiful-Hoque,2016). Aldosari (2017) noted that it was a significant challenge for doctors or IT managers to secure the health records systems from hackers due to lack of user training or not using updated secure medical communication hardware and software technology. This type of network security problem happened due to user data entry being done through improperly configured network devices properly with firewall, router configuration, or encryption issues between server and client devices (Aldosari, 2017). There was little research completed to find the security risks associated with EHRs application systems and a lot of study needs to be done to find the security risks and evaluate strategies used by healthcare industry IT managers to secure CIS/EHRs cloud-based systems from hackers or data breaches (Aldosari, 2017).

User training is not enough to protect the patient records from data breaches. Still, EHRs procedures should improve for better communication between healthcare industry employees, patients, or other users of the private cloud-based EHRs systems (Aldosari, 2017). Rathert et al. (2017) showed that there was a significant security improvement in sharing, reading, and updating information with the use of CIS/ EHRs) online application systems. It helped patient access function for better communication, patient engagement, and user's self-management confidence in EHRs cloud-based systems. The IT security manager or system administrator should use the security techniques of the researchers to create role-based access to the EHRs systems and notify the users to logout from the networks when they are not using it. So this type of security technique would help avoid patient record data breaches in the future. Some healthcare industry's information technology (IT) leaders lacked the strategic experience to implement secure access procedures to protect patient health records on the private cloud-based CIS systems. It demonstrated a literature gap and should be explored or researched.

Transition and Summary

This section provides an introduction to how IT managers should implement secure access procedures to protect CIS patient health records. The private cloud-based CIS systems should minimize the security exposures of network frameworks used in some healthcare industry 's health care systems. The purpose of the pragmatic qualitative inquiry study is to evaluate strategies to protect patient health records on the private cloud-based CIS systems as well as to minimize the security exposures of network frameworks used in some healthcare industry ’ health care systems.

For section 2 and 3, I worked on the various components of doctoral study section 2 such as my role as researcher, the qualitative research study participant role, research design & method, population sampling process, ethical research rules and guidelines, interview data collection & organization process, testing and reliability of interview data. Finally, I present my findings.

Section 2: The Project

Purpose Statement

The purpose of this qualitative pragmatic qualitative inquiry study was to explore strategies of the healthcare industry IT leaders to implement secure procedures to protect patient health records on the private cloud-based CIS systems. The study's target population consisted of CIO, CISO, or IT managers, from the healthcare industry using strategies to secure private cloud-based CIS systems. The geographical location of this study was healthcare industries located in San Francisco, California. The findings of this study may impact positive social change by improving strategies to protect patient healthcare records. Finally, this study assisted in identifying and closing security gaps, as well as alleviating the security concerns of both patients and administrators.

Role of the Researcher

For this pragmatic qualitative inquiry study, my role the data instrument was to develop, design, and make a plan to perform the study, collect the participant's interview responses, analyze the findings or data, and present the result in a non-biased way. The primary data collection was through the interviews with participants with a selected number of qualitative questions to support the research question without bias.

The methodological triangulation was used to verify the finding of this pragmatic qualitative inquiry research study and with themes such as strategies that healthcare industry IT leaders use to implement secure access procedures to protect patient health records. I used industry documents for methodological triangulation related to IT leaders' strategies in the healthcare industry to implement secure access procedures to protect patient health records. (Råheim et al. (2016) reported that the bias in a researcher's finding could be an ethical issue which researchers should avoid at all cost. Each researcher should avoid bias and prepare the study results with participant's exact responses (Bero, 2017). Bero (2017) suggested that biased study would have different effects than an unbiased study. The biased data could create potential threats to the validity of the researcher's finding of the research (Olteanu et al., 2019). Bero (2017) said that every researcher should not use bias in their participant's data collection and analysis process of the research study. Berry (2016) reported that the researcher must understand the relationship with participants, interview question answers, and how to collect the data without bias. As a researcher, I was an observer and interviewer, who record each participant's response without bias, collect the interview data, and conclude the data analysis in a qualitative research study by using a software application and then reported the finding based on the data analysis.

I have worked in the hardware, software, and information technology industry for many years as a consultant. I used, managed, configured, and provided training of cloud-based application CISs/EHRs system for many years, including software application used in healthcare industry or medical offices to provide services to their customers. I did not have any relationship with the participants of the study. The researcher should follow the ethical conduct rules in their target qualitative research study and communication with the participants (Cumyn et al., 2019). I followed ethical conduct rules when I communicated with participants, asked participants interview questions, collected participants' data, and do the data analysis.

I followed the rules of the *Belmont Report*. The *Belmont report* includes a list of the ethics rules, guidelines, concepts, or theories for securing participants during the research study interview process (Brothers et al., 2019). The fundamentals rules and guidelines of *Belmont report* are: respect, justice, and beneficence. I understand the importance of the *Belmont Report* rules in detail as a researcher. I ensured that all the participants were treated with respect, justice, and beneficence using the Belmont report criteria before, during, and after the research study was completed. I completed the Protecting Human Research Participants Research web-based training from the National Institute of Health (NIH) Office (Appendix A).

I followed the Walden University IRB guidelines when conducting interviews with target qualitative research study participants. I notified the participants about the distinct characteristics in detail of my research study. I informed them about the process of the study, their role in this study, the objective of this study, and how the results will be used and produce by using proper consent form. The participants also made their independent decision to answer my questions in this study. Once an appointment with the participant was confirmed, I asked interview questions to each participant in the interview and record their answers following the interview protocol. The participant's identity and interview data was kept confidential. The above protocol was used to communicate, set up appointments during and after the interview with participants.

Participants

I used a pragmatic qualitative inquiry study methodology. Audrey et al. (2016) found that the specific participant selection process is a significant component in the data collection process relevant to the participant's interview related to the research study. I selected qualified participants from available eligible CIO, CISO, or IT managers from the healthcare industry using strategies to secure private cloud-based CIS systems. The scientists or researchers should use the criteria to select a participant pool that supported the research question because using the standard process to choose the participants may produce the wrong results (VonBastian et al., 2016). CIO or senior IT managers play a vital role in preparing strategies to secure access procedures to protect software online application systems (Morris, 2018).

This qualitative research study participant's selection criteria were based on my research question, which was "What strategies do healthcare IT leaders use to implement secure access procedures to protect patient health records on the private cloud-based CIS systems?" Requirements for participation in the study included:

- At least 1 year of IT online cloud-based application experience
- CIO, CISO, or IT managers with more than one year of experience in the healthcare system
- Based in the Northern California area of the United States; and
- Have a management working knowledge of using strategies to implement secure access procedures to protect patient health records application systems

The relationship between researcher and interview participants was critical and based on trust level and research study validity. Cheng et al. (2017) suggested that the scientist's or researcher's ability to create trust with the participants depends on the communication methodology between them and step by a step interview process with participants. I followed the interview protocol to promote trust and mitigate bias.

I chose participants using LinkedIn or social media, online healthcare associations to identify participants that meet my research study criteria and healthcare industry using private cloud-based EHRs/CISs in the metropolitan San Francisco Bay area and other parts of Northern California within 400 miles radius from San Jose, California. I recruited qualified participants from available eligible CIO, CISO, or IT managers from the healthcare industry. These qualified potential participants used strategies to *secure private cloud-based CIS systems.* Shaharudin et al. (2017) explained that census sampling worked great with a smaller population for the research study. I selected participants for my research study using the census sampling approach, and my target participant's population was small.

After IRB approved my study, I recruited potential participants in the healthcare industry on LinkedIn, other social media, and healthcare associations who met the participant criteria and can provide answers to my research question. Spacey et al. (2020) reported that proper strategy to communicate with potential participants using social media could help the researcher to resolve their problems. Email is an excellent approach to communicate and recruit potential participants from the above list. I contacted eligible participants to participate in this study through email.

I explained the purpose of my research study to the participants. Angappa et al. (2018) described how to initiate the initial contact by writing an email letter addressed to senior IT management of the organization with the purpose of the study and how it may help that organization to secure their online application systems. Wilkes et al. (2017) explained that participant selection procedure or method should be according to comfortable level and human network of the participants. Neville et al. (2016) also suggested that the internet is a great source to connect with participants or recruit the participants for a qualitative research study such as healthcare IT professional managers' discussion forums, LinkedIn, or Facebook. I used the online resources social media to recruit the qualified healthcare IT managers as participants in the healthcare industry for this research study.

Tolich (2019) explained that the researcher can inform the participants about the procedure and risks involved in the research study (Tolich, 2019). I gained potential participants' consent and notified them about the process and purpose of the interview. I also informed them about the importance of their participation in the research study. I emailed the consent form to potential participants to set up the interview with them. After signing the consent form, I arranged an interview with the participant. The interviews with the participants were Zoom audio conference meeting by using Zoom or other internet tools available and allowed by the healthcare industry. Since I was using purposeful homogeneous sampling method, I found potential participants in the healthcare industry on LinkedIn, other social media, and healthcare associations who meet the participant criteria and can provide answers to my research question. I interviewed all those participants who agreed and met the interview protocol criteria .

Research Method and Design

A pragmatic qualitative inquiry study methodology provides researchers the ability to isolate the specific strategies (Waibel et al., 2015). The credibility, dependability, confirmability, and transferability were essential factors of the research study's procedures (Waibel et al., 2015). The research method and design of this study was a pragmatic qualitative inquiry technique to evaluate IT strategies used in the healthcare industry to help minimize private cloud-based CIS application servers from data breaches such as cybercrime hacking, theft of mobile devices, insider accidents, or malicious insiders.

Research Method

I chose a qualitative method to evaluate IT strategies used in the healthcare industry to help minimize private cloud-based CIS application servers from data breaches such as cybercrime hacking, theft of mobile devices, insider accidents, or malicious insiders. Kahn et al. (2016) reported that many EHRs system data have been used in qualitative research and found out those EHRs systems with different settings produced different results to prospective randomized trials data. Garg et al. (2015) suggested using the qualitative research method to evaluate the security risks associated with EHRs cloud-based systems. A quantitative research study method focuses on data measurement and collected through surveys, multiple-choice questions, or polls (Ludo, 2019). Quantitative research was a method used to identify numerical data based on reliable measurements from survey results (Queirós et al., 2017). Eyisi (2016) explained that the quantitative approach based on a phone or online survey related to problem-solving skillset resulted in arithmetical data, which could be used in data analysis. A quantitative research study was not appropriate for this study because the focus is to understand the strategies – not measure them. Mixed-methods research is a combination of quantitative and qualitative research design methods (Jacquelynn, 2018). Since a quantitative research approach was not appropriate for this study, mixed-methods research is also not suitable for this research study. I used a multiple qualitative case study design method to interview IT security managers to investigate strategies in CIS system applications.

Research Design

A pragmatic qualitative inquiry design provides researchers the ability to isolate the specific strategies (Waibel et al., 2015).The pragmatic qualitative inquiry design method was appropriate for this study. Examining different *information technology* security strategies required direct interaction with the IT managers, CIOs, or CSOs creating and implementing those strategies to understand their experiences. Khorram Niaki and Nonino (2017) collected 16 different business model operating companies using pragmatic qualitative inquiry research methodology and a theoretical replication approach. Aschemann-Witzel et al. (2017) analyzed 26 regular and definite consumer food waste initiatives using a pragmatic qualitative inquiry study method.

Phenomenology is another design method and is used to analyze the commonly shared features of participants that experienced an unusual phenomenon (Gentles et al., 2015). Crowther et al. (2017) argued that the phenomenological literature review crafted stories were compatible with the philosophical methodology. The phenomenology was a collection of stories or ideas that were not appropriate in examining engagement procedures as part of the qualitative research study (Ash & Simpson, 2016). Thus, phenomenological research was not suitable for this study because the focus is to understand the strategies- not IT professional's behavior or stories. Steven (2015) explained that the social connections were the bases for an ethnographic research design between participants and users. Garthwaite (2016) reported that the ethnographic research was time-consuming in making social connections or interactions in connecting users, customers, or potential participants to discuss their background, education, or experience. Chatti et al. (2017) showed how different people made their decisions depending upon their expertise and ethical responsibilities in ethnographic research design. There was no direct interaction between the CIS system IT professionals and public users. Therefore, ethnography was also not an appropriate choice in this research study. The pragmatic qualitative inquiry study approach was a suitable choice in this research study because it aligned with the research question, and I used one-to-one interviews with IT managers working in the healthcare industry *using interview questions (Appendix C).*

Population and Sampling

Population

The population of this study included the information technology managers, CIOs, CSOs, or Information security managers working in healthcare industry in northern California. These managers were developing and using security strategies to secure patient health records on the private cloud-based CIS systems. The participants used in this research pragmatic qualitative inquiry study were located in the San Francisco Bay area and other parts of California. The study's participants had the experience, education, and knowledge as noted in the criteria in securing and management of cloud-based CISs application systems.

The senior information technology managers met the following criteria to participate in this research study:

- At least one year of information technology online cloud-based software application experience
- CIO, CISO, or IT managers with more than one year of experience in the healthcare system and their offices located in the Northern California area of the United States
- Had a management working knowledge of using strategies to implement secure access procedures to protect patient health records application systems

These criteria allowed me to collect data to answer my research question: What strategies do healthcare industry IT leaders use to implement secure access procedures to protect patient health records on the private cloud-based CIS systems?

I interviewed the potential participants by using an interview protocol (Appendix C). I interviewed the participant, which was ½ to 1 hour. A follow-up meeting was set up for member-checking. I collected the interview data with the participant in the proper process using an interview protocol (Appendix C). I planned to conduct a virtual interview meeting with the potential participants. Arquilla and Guzdial (2020) suggested that researchers should use virtual conferencing with participant interviews for their research study. I provided the participant interview a comfortable virtual environment Zoom meeting environment such as, and we used audio recording depending upon the participant's personal choice. I did the audio recording, which complied with Walden university guidelines. I had a Zoom interview meeting with participants in a closed room environment, so participants felt comfortable and relaxed during the interview process.

Sampling

I used the purposeful homogenous sampling method in this qualitative research study. Allahyari et al. (2020) reported that they had used the purposeful sampling method to identify and recruit the participants samples in their qualitative research study. They have further explained that their focus was on a specific population, which answered the researcher's research question.   Hunter et al. (2019) reported that researchers could use purposeful sampling in the study when the participant's population more as compared to other populations in that organization or community. I used a purposeful homogenous sampling approach to identify potential information technology managers' qualification criteria. I asked the IT managers, network or security managers, CIOs, or other customer service department managers that meet my study's population criteria. I sat up interviews with all who meet the study's population criteria and agree to participate. The participants can be IT professionals working on securing their CISs or EHRs cloud-based application systems. I interviewed those participants in my research study target population. Kissam et al. (2018) used the census-taking strategy to sample from US federal, state, or local government agencies based on collected population census data. My expectation was that 5 participants allowed me to meet data saturation. Otherwise, I kept adding participants to my list until data saturation reached.

Many researchers found that sampling can be a difficult task for their research study, and it takes a lot of time to complete the sampling task. Naderifar et al. (2017) explained that qualitative research study data was a systematic procedure of participant's experience and their internal feeling information data, which can be participant's answers related to the researcher's research questions. They have further reported that most data were output from an interview with participants, research study focus group, interview notes, or other participant's data. Farley (2020) also explained that sometimes researchers could increase the sample size to reach a saturation point in their qualitative study. I used the LinkedIn social media to find network or security managers, CIOs, or other IT managers as potential participants. My minimum sample size was a total of five participants for my study. If the number falls short and I had not reached data saturation, I would participants to the list to meet the data saturation. I reached data saturation after interviewing total of participants for my study.

Ethical Research

I performed the qualitative research study honestly and ethically. I used the interview protocol procedure (Appendix C) to guide the interviews with potential participants. In a study by Gong et al. (2018), the participants could not participate in their study without signing the pharmaceutical company consent form. They reported that monitoring the procedure, realignment of the medical and technical education universities process to communicate with the research study participants can restore the patient-centric models and informed consent trust with interview participants. Lim and Greenwood (2017) suggested that the researcher should use ethical criteria to communicate with participants. Researchers can build an ethical relationship with qualitative study participants to help create trust between the researcher and participants (Lim & Greenwood, 2017). Walumbwa et al. (2017) suggested that ethical conduct, peer justice, and justice environment were the essential mechanisms to help researchers and participant groups learn from each other. I contacted each potential participant according to this study's selection criteria. Each participant signed the informed consent form (Appendix A) to participate voluntarily in this study. The informed consent form (Appendix A) consisted of the purpose of this research, what I did in this research, the time required, risks, benefits, compensation, confidentiality, participation, and withdrawal of my contact information, statement of consent, and signature of the participant. I explained the purpose of the study to each participant at the beginning of each interview and also explained both my and their responsibility in the participant interview. Participation in the survey was voluntary. Participants could decline to participate in this process and can withdraw by advising the researcher, and no questions asked.

There was no risk to the participants because I did l not choose potential participant who might have any relationship with me. I explained that the interview will be a half-hour in length and then a 30-minute follow-up session for member -checking. I also explained to each participant the benefits of this study to them and their healthcare industry in closing security gaps in their network and resolving other security concerns. If participants had a question about their rights, they can contact a Walden representative at irb@mail.waldenu.edu. Surmiak (2018) found that 42 researchers worked with unprotected groups and participants in their research study, which was against the study's ethical laws. He further reported some accidental data breaches related to participant's privacy information, and it is the researcher's responsibility to keep the participant's private data confidential. As a researcher, I kept the participant's information hidden in a secure place. I analyzed the data and included the results in the next Section 3.

The Belmont report guidelines were the basics of the participant's privacy rights, trust, and respect. I followed the Belmont report's policies and kept the participant's interview data confidential, which is a critical factor in ethical research. According to the Belmont report, I followed the participant’s respect, trust, or privacy rights rules. The Belmont report includes a list of the ethics rules, guidelines, concepts, or theories for securing participants during the research study interview process (Brothers et al., 2019).

Ethics was an essential part of the research study for the researcher. Ethics plays a significant role in doctoral students becoming good scholars (Berg, 2016). He further reported that the literature review research into the ethical practice research study showed that scholarship included in each step of the doctoral research study based on the Belmont report protocol provides equal participant involvement, moral activities, or fairness to the participants. I ensured that I treat all the participants with respect by using the Belmont report rules before, during, and after the research study. I completed the Protecting Human Research Participants Research web-based training from the National Institute of Health (NIH) Office (Appendix A). I kept the participant's interview questions with each participant's recorded response anonymously using a coding strategy for each participant and store on a password-protected flash drive.

Furthermore, I kept the flash drive in my locked cabinet for five years. After five years, I destroyed the entire participant's recorded data and their corresponding consent forms. I also destroyed all the data on the flash drive and finally destroy the flash drive by putting in water for one hour and break it up with the hammer.

Data Collection

Instruments

I was the primary data collection instrument for this research study. Cutland et al. (2017) explained that data collection instruments could be the researcher's interview question, the participant's report form, or diary card information. The authors further explained that data collection could be a participant's name and contact information, interview date, participant’s job responsibility, or customer support to application system users. Mahabir et al. (2017) reported that many researchers using web-based tools or virtual meeting tools with their research participants in chatroom or message boards as a data collection instrument strategy.

I ensured that data collected from the participants’ interviews were kept confidential using the NVivo coding method to keep the participant data confidential. I mitigated bias using an interview protocol (Appendix C). I used ethical and methodological semi-structured qualitative interview strategies. Bryant-Waugh et al. (2019) reported a semi-structured interview strategy is an excellent investigator-based assessment tool to interview target participants to get maximum reliability. Dadzie et al. (2018) explained that the open-ended semi-structured interview approach produced reliable results during an interview with participant sustainability/energy efficiency professionals, building services engineers, project managers, facility managers, and architects. The unstructured and structured methods were the semi-structured interview procedure (Dadzie et al., 2018). They further explained that the open-ended questions approach allows flexibility and creativity during the interview process with target participants to answer the research question.

I developed nine open-ended interview questions (Appendix C). I asked follow-up questions based on their answers when appropriate. I followed the interview protocol (Appendix C) to explore healthcare industry information technology (IT) leaders or managers' strategies to implement security procedures to protect patient health records on the private cloud-based CIS systems. I prepared the interview questions in a simple language based on the research study question (Appendix C). The interviews were more successful in a relaxed environment, and they answered freely based on their experience and knowledge. Shankman et al. (2018) found that interviews with participants' feedback increased reliability and validity. The authors further explained that data collected from a virtual face-to-face meeting could use audio recordings to help the researcher do in-depth data analysis. Healthcare industry or medical service providers' online documents, old archival information, or healthcare industry website document can be part of data collection to perform methodological triangulation. I collected data from a virtual face-to-face Zoom meeting with potential participants and did the Zoom meeting recording with their permission, and it helped me do in-depth data analysis. I used the healthcare industry information technology documents and data to triangulate data related to securing online cloud-based application to protect patient privacy electronic health records.

Kallio et al. (2016) found that semi-structured interviews were a standard data collection method in qualitative research pragmatic qualitative inquiry research study, and good quality of interview procedures or protocols impact the research study findings. The authors further concluded that a qualitative semi-structured interview guide helps the objectivity and trustworthiness of studies and makes the results more believable. I used the Walden University guidelines using an informed consent form (Appendix A) and interview protocol (Appendix C) using a semi-structured interview process during an interview with the participants in the data collection procedure. I developed the qualitative interview process and set the interview protocol (Appendix C). The interview data's verification and reporting will be the last of the data collection instrument, and I reported the results in section 3 of my research study.

Member-checking helps the researcher get feedback from participants, which improves the qualitative research reliability. The member-checking process provides the knowledge exchange between researcher and participants (Naidu & Prose, 2018). The authors further suggested that member-checks could improve the validity in some research studies, not all studies and explained that member-checking commonly used methods to validate the researcher’s data collection and analysis. The researchers used member-checking to improve their research study's credibility, accuracy, and validity (Madill & Sullivan, 2018). The researcher can use an organized method to validate the participant interview data (Madill & Sullivan, 2018). I used a member-checking strategy to verify the data collection information from the participants. Once I completed the formal interview with all participants, I first interpreted the data collected. I sat up the second interview with each participant to share my interpretation of the first interview data with that specific participant to correct any misinterpretation of the interview. I did an audio Zoom meeting with each participant and follow-up virtual sessions were based on each participant’s availability. If some of the participants were not available for a follow-up session in a virtual Zoom meeting, a phone meeting was scheduled in that case. The reliability and validity of interview data and the member-checking strategy process were essential steps of my research study. The data triangulation method helps the researcher collect the data different resources and grab other research study measurements, which increased the study's validity. Fusch et al. (2018) explained that the data triangulation method could collect data from different sources and catch distinct measurement points of the research study. They also defined that data triangulation as inter-related and ongoing points people, time, and space, which expands the research study's confidence. Since many other researchers used data triangulation in their research study, I collected data from the participant Zoom interview and healthcare industry data and documents, which are related with healthcare industry. This process supported the finding of my study, which is to explore healthcare industry information technology (IT) leaders' strategies to implement secure procedures to protect patient health records on the private cloud-based CIS systems. It further increased the reliability and validity of the study. Andreadis & Kartsounidou (2020) explained that member-checking and data triangulation helped the researcher identify their decision and hypothesis to make the data interpretation. I used member-checking and data triangulation strategies to allow me to identify themes through data interpretation. These strategies helped me improve data validity and reliability.

Data Collection Technique

I identified potential participants in the healthcare industry using purposeful sampling technique. I used LinkedIn social media to recruit participants and email them my research study’s purpose.   After I got their approval, I emailed them an informed consent form (Appendix A) to read, understand, and sign it. When I received their signed consent form, I contacted them about their virtual interview date and time availability. The researcher should have needed skill sets and values in pragmatic qualitative inquiry study training and develop the interview protocol (Yin, 2017). Yin (2017) suggested that researchers can be successful by focusing on the interview research question with relevant questions when interviewing the participants.

I followed the following steps for data collection by using the interview protocol explained in Appendix C:

- I got the approval from Walden University IRB department
- I contacted the potential participants to ask for their participation through social media, and if they agree, I sent them the informed consent form (Appendix A).
- I contacted each of the participants to schedule an interview date and time once I received the signed consent form.
- I sent an email to confirm the virtual interview meeting date and time with Zoom link information, interview procedure explained in appendix A, keep the information confidential, participant's right to withdrawal from the interview, participant's right to answer or not any question.
- I got each participant's permission to record the Zoom video interview meeting, and I wrote the notes during the Zoom virtual interview meeting
- I conducted a Zoom interview meeting starting with the introduction; discuss the interview protocol (Appendix C), an overview of the research study topic or question, member-checking process.
- I thanked each participant and conclude the Zoom interview meeting.
- I used that member-checking with participants for data reliability and validation
- I ensured that Zoom interview data files stored on a local hard drive with a password-protected locked room.

I used the following strategies to make the interview process with participant enjoyable and successful:

- I asked sequential and probing questions, as mentioned in the interview protocol (Appendix C). When participants answer that question, I listened with my full attention or focus and allowing them to answer the question with their thoughts or examples.
- I stayed neutral with no bias during each question and the participant's response to that question. I provided a flexible interview environment so that the participant and I felt comfortable during the interview.
- Since we have 30-60 minutes for questions and answers, I monitored each question's time and gently ask the participant to move to the next question if less time is left for other questions.
- I motivated them to use an open conversation style during the interview question-answer session.

Based on the consent form (Appendix A), I shared their rights with each participant, the purpose of this research, the process, the time required, risks, benefits, compensation, confidentiality, participation, and withdrawal. Loss et al. (2020) suggested that semi-standardized interview processes help the researcher set up interviews with participants, provide flexibility in asking interview questions, and offer interview data collection flexible technique based on the interview protocol procedure. Loss et al. (2020) further recommended that the Zoom interview meeting be video or audio recorded, including the transcript captioning and later shared with the interview participants. Thomas (2017) also suggested that member–checking process or technique could improve the accuracy, validity, and credibility of the research study. I completed the member-checking procedure with each participant. I sent the interview interpretation to each participant before the follow-up meeting. I sat up the follow up meeting to request a specific date and time. Qualitative researchers used data triangulation in their research study to improve reliability. I collected data and documents from appropriate secondary sources in the healthcare industry. I also included an analysis of documents as a secondary data collection method. This process provided strong support for my study's finding to provide a second data source to be used in methodological triangulation collect data on healthcare industry information technology (IT) leaders' strategies to implement security procedures to protect patient health records on the private cloud-based CIS systems. It further increased the reliability and validity of the study. As explained above, I used the methodological triangulation method, working with participants, and collecting data and documents from healthcare industry secondary sources.

Data Organization Techniques

Data organization is a consistent process and helps the researcher to manage the participant interview data and other data collected from the organization documents. Broman and Woo (2018) explained that the data organization process should be consistent, and it can help the researchers manage the interview data easier later in the process. I used interview notes, Zoom video recording, research log information, and analyzing participant's organization online documentation to improve my data reliability and validity of the research study. The data collected from the participant's interview with the researcher should be consistent. The consistent data process could reduce many data problems later in the research study process (Broman & Woo, 2018). The research study log can heled the researcher for the confirmatory, reliability, or verification of data, and it can be part of data organization strategies. The research log is used to track the changes during each research study (Broman & Woo, 2018). Arndt et al. (2017) reported that the researcher developed a research log to record an event or interview data to test the interview research protocol and actions taken in the researcher's interview with the participant. I recorded the whole process and my notes with no bias or thoughts about how the interviews conclude with participants. Arndt et al. (2017) also reported that research log information could minimize bias in the research study.

It was essential to secure the interview data, which complied with Walden University IRB ethical research protocol. It was necessary to ensure the confidentiality of the participant's information and interview data collected in the research study related to the participant's identity information (Bender et al., 2017). I ensured that the participant's personal and interview data kept confidential and stored with a password-protected file on a local storage drive. I followed the guidelines of the San Francisco bay area 3 local healthcare industry ' communication ethical alphanumeric code for their employees' communication and protect their employee's or participant's privacy information stored on the password-protected file. I created, developed, or updated each participant's name with my assigned secret code in a separate folder. I recorded the participant's virtual

Zoom meeting and shared the interpretation of the data later, if needed. I secured this data on a password-protected flash drive for the next five years at a safe place.

Data Analysis Technique

For this pragmatic qualitative inquiry study research data analysis, I collected data to answer the research question: What strategies do healthcare industry IT leaders use to implement secure access procedures to protect patient health records on the private cloud-based CIS systems? Morgan and Nica (2020) suggested that thematic data analysis based on interview questions responses, follow up questions in participant's interviews, tentative theme list, and analyzing research question theme using the coding process iteratively. Morgan and Nica (2020) suggested that the pragmatic qualitative inquiry research study data analysis could have more than one analytic method to validate the reliability of the data collected in each participant's interview for the qualitative study. I analyzed data from participant data and industry documents to generate themes.

The data organization software applications helped the researcher to insert, update, or organize data for a qualitative research study. The participant's interview data managed using NVivo data analysis software application. NVivo protected the research participant's confidential information in the qualitative research study (Maher et al., 2018). Since NVivo tool was a secure tool to protect participants' interview data and their confidential private information, I used the NVivo software application to analyze the qualitative data. Qualitative data cannot be expressed in numbers, but NVivo software application was designed to organize and analyze the qualitative data collected during the interviews with participants, open-ended interview questions between researcher and participants, and participant’s responses or observations. I used NVivo 12 for data analysis for this research study. I categorized and coded the interview data to generate the themes of the study. I analyzed the data to convert raw data into meaningful information.

The research study's reliability and validity depended upon multiple data sources, which provided the input to methodological triangulation methods. The methodological triangulation used to verify the finding of this pragmatic qualitative inquiry research study. Many researchers used the methodological triangulation method for reliability, credibility, and confirmability of a research study (Fusch et al., 2018). Andreadis and Kartsounidou (2020) reported that many non-interview groups collected the data from multiple sources that used the methodological triangulation method. The researchers used the computer application assigned code method to the participant's question and response and their own created codes to identify the research study themes and classification based on participant's employer's external data and interview data (Andreadis & Kartsounidou, 2020). I asked qualitative research study questions to each participant using an interview protocol (Appendix C). The data analysis identified differences and similarities, which helped me to create codes in NVivo 12 and identify the study's themes. I used ethical semi-structured qualitative interview strategies. Dadzie et al. (2018) explained that the open-ended semi-structured interview approach produced reliable results during an interview with participant’s sustainability/energy efficiency professionals, building services engineers, project managers, facility managers, and architects. I used interview answers (verbally or visually) to produce themes and codes for this study. I used the secondary data sources documents related to securing access procedures to protect patient online records in triangulation method. This process helped me understand related industry data and provide methodological triangulation about healthcare industry IT leader’s strategies to implement secure access procedures to protect patient health records on the private cloud-based CIS systems. I merged related data documents collected from healthcare secondary data sources and each participant’s interview in to one database NVivo 12 using triangulation method. I developed themes from each participant’s interview and documents collected online from organization’s website using the following steps: I collected the data from participant’s interview and from other online organization’s resources. I compiled the above data collected into NVivo12 data analysis database application; I   broke up the data in NVivo 12 in to manageable units for better organization; I reassembled the data into manageable units; I interpreted the data in visual graph format,; finally I validated the data. These steps helped me to produce the themes of study, which reviewed with conceptual framework and literature view. The data analysis was part of a problem-solving methodology that includes understanding the research study, planning to resolve the problem, designing the procedure, implementing the process, and testing it. Castleberry and Nolen (2018) suggested that researchers use a qualitative data analysis model with five steps: compiling, disassembling, reassembling, interpreting, and concluding the data. My data analysis approach included the following: collect the data, compile the database, and break up the data into small manageable units (disassemble data), reassemble the data into manageable units, read (interpret) data, or display the data in a visual format, and validate the data. Specifically, I used the following steps:

- I collected the data from each participant's interview including audio recording in Zoom meeting, transcribe the data from the audio, and then compile the interview data by using the desktop software application NVivo 12. Broman and Woo (2018) explained that the data analysis's first step was to organize the data properly with the data analysis software application. Maher et al. (2018) reported that NVivo was a qualitative data analysis application that could help the researcher compile the interview data and protect the network's data. I used the NVivo data analysis application to organize and the participant's interview data and healthcare secondary data source related to the research study.
- I broke up the interview data into small manageable units or disassembled it. The second step of data analysis was to dismantle the qualitative research data (Castleberry & Nolen, 2018). Niedbalski and Ślęzak (2017) reported that the NVivo software application is an excellent application for auto-generating and user-created codes for data analysis. I used NVivo 12 to create an auto-generating code for participant's interviews and healthcare industry online archival data collected and break up the collected data into manageable units for data analysis. I used codes from the NVivo application to identify the key elements and relationships with other codes or features using database concept rules. I used NVivo 12 to identify themes for this research study.
- I reassembled the data collected from the participant's interview using NVivo 12 for data analysis. Castleberry and Nolen (2018) mentioned the next step

of data analysis is to reassemble the data collected using proper data analysis software application. Many researchers used NVivo to reassemble the participant's interview and other related data for qualitative data analysis using the iterative method (Niedbalski & Ślęzak, 2017). I used the coding technique to organize the data sets, and to compare, analyze and validate the themes of my study data groups. I examined the participant's interview responses and documents collected as a secondary source into categories of data groups, which provided information about research study theme or research question.

I explained the data sets and categories in-depth with step by step instructions. Castleberry and Nolen (2018) suggested that data analysis's fourth step is to interpret the data. Niedbalski and Ślęzak (2017) explained that the data analysis fourth step is to interpret, or the researcher should describe the data sets, codes, categories of NVivo application information in detail. I categorized the interview data, and it helped me to identify themes and patterns as they merged related to the study. After that, I matched up corresponding data in those themes. I reorganized the data sets in NVivo 12 application, analyzed the data, and converted to meaning units of categories. It helped me to understand the data set a relationship with my research study's theme using member-checking and triangulation methods. Once I got coding, categorizing, and identifying themes using NVivo 12, I analyzed it. The above process generated themes about how IT leaders implement secure access procedures to protect patient health records on the private cloud-based CIS systems and how healthcare industry user tasks mapped to the technical aspects of CIS/EHRs systems based on the TTF theory conceptual framework.

I discussed the findings based on the themes and how they are related to the literature review and conceptual framework.   Castleberry and Nolen (2018) suggested that the data analysis's last step is to write the summary report of the data analysis and relation with study themes. The NVivo 12 software application was beneficial to generate themes and report out as finding.

Reliability and Validity

Weller (2017) suggested that the researcher respecting the participant and using the proper research study consent form with the interview protocol process can build an increase in the study's reliability. I used the participant’s consent form (Appendix A) for a straightforward communication procedure with the participant, transparent interview protocol with interview questions (Appendix C) to increase the study's reliability and validity. I also used strategies explained in data instruments, collection, organization, and analysis during the interview process with participants. I used member-checking and data triangulation in the data collection and data analysis process, which helped my study's reliability. I also presented all my findings in an unbiased manner.

Dependability

The logical, traceable, and documented research process establishes the dependability of a study (Hass et al., 2018). The better the logical structure of a planned research, the better it provides more establishment of the dependability (Onuma et al., 2018).I developed a logical plan to collect the interview data and archival data collected from healthcare industry ’s online resources, which helped develop a reliable dependable research study. Feinbube et al. (2017) suggested that a traceable research study produces reliable results as a part of the enhancement of the dependability and starting point. I used the traceable data collected from participants and from other online resources with validated evidence, which could be traceable any time in future based on the reader’s request. Vizarreta et al. (2020) explained that a well-documented research study creates more reliable dependability of the study. I documented each participant’s interview and also documented the finding from archival data collected from healthcare industry’s website. To address dependability, I used member-checking by having participants verify my interpretations of the data collected from the individual in-depth interviews to ensure that they accurately depict what the participants intended to convey. Member-checking occurs when interpretations are relayed to research participants to check for perceived accuracy and reactions, thus increasing a qualitative inquiry (Perrotta, 2017). Hass et al. (2018) reported that when the researcher has a logical, well documented, and traceable research procedure, dependability can be accomplished. The authors further found that reliability is measured in terms of dependability, reliable system, and accurate data analysis measures. Rose and Johnson (2020) reported that dependability is based on a logical and traceable process. Hass et al. (2018) further suggested that the researcher record data collection, organizing, and analysis activities in the log file to increase the data's reliability. McDonald et al. (2019) provided three types of reliability: stability or consistency of a single coder’s use of codes over time, replicability of results across coders, and accuracy of an established coding scheme compared with others. McDonald et al. (2019) have provided the report that the study data organized, analysis codes and research study themes, met with the participants, and other member-checking researchers compared their code analysis to determine the similarities or differences. I used the interview protocol to collect data consistently by writing notes during participant's interview and I developed electronic journal entries for participant's data collection and also develop the entries for archival data collected from online resources.

Credibility

The research study truthfulness was a crucial factor in maintaining the credibility of the researcher's study and trust established between researcher and participants, and credibility depends on the participants' trustworthiness. Member-checking improves the qualitative research credibility due to participant's feedback. Naidu and Prose (2018) suggested that member-checks could enhance many research studies' credibility, depending upon the plenty of data collected. The researchers used member-checking to improve the credibility, accuracy, and validity of a research study (Madill & Sullivan, 2018). I used a member-checking strategy to guarantee credibility of the interview data. Once I completed the formal interview with all participants, I had interpreted the data collected. I completed member-checking and met with participants in the follow-up meeting. The participants could check the accuracy of the interview data captured in the interview, and this process could increase the validity or credibility of the data. I used member-checking to ensure the creditability and trustworthiness of the study's creditable participants. The data triangulation method helped the researcher collect the data from different sources and different measurements of the research study, increasing the credibility or validity of the study. Fusch et al. (2018) explained that the data triangulation method could be used to collect data from different sources and catch distinct measurement points of the research study. Fusch et al. (2018) also defined that data triangulation as inter-related and ongoing points people, time, and space, which expands the research study's confidence. I used methodological triangulation. I collected data from the interview with participants and documents of healthcare. I collected data from multiple healthcare industry resources and participants using an interview protocol in my pragmatic qualitative inquiry research study. Finally, I used the methodological triangulation to increase the validity of the data.

Transferability

Transferability helped that finding of the study can apply to others in similar situations, individuals, or settings. My research study was transferable because I documented in detail my research and data collection processes. Pratt and Yezierski (2018) suggested that participant’s interview data could be data collected trustworthiness and supported the data collection process's improvement, which further helped the progress of finding transferability. Pratt and Yezierski (2018) found that increasing the population sample size could improve the qualitative data analysis process's generalizability or transferability. I performed the in-depth study using the member-checking method and pragmatic qualitative inquiry study participant data collected from the healthcare industry. I interviewed the qualified participants using the interview protocol (Appendix C) and collect the data and follow a strong validation data process. These methods helped to increase the transferability of my study results for other studies in the future. I recorded the data collection process during an interview with participants to allow the results to be transferable.

Confirmability

The confirmability was the level at which other researchers would confirm the study's objectives, outcomes, or view. FitzPatrick (2019) defined that when study finding ensured due to consistency, truthfulness, and applicability of collected data interpretation from the participants without any bias. Abdalla et al. (2018) explained that confirmability was a quality dimension in the qualitative research study based on reliability, credibility, transferability, and confirmability. I checked and rechecked the collected data during the research study. I interpreted the data collected from each participant's interview and documents and confirmed the data using NVivo application and other online validation tools. I kept the detailed record of all processes and store in password protected file. This process increased the reliability of the study data. I used triangulation method using interview data collected, industry documents and data, and data analysis reports created with NVivo 12 application. This process increased the confirmability of the study without any bias.

Data Saturation

Data saturation was a research study sampling point when no new information or themes emerge, and there was enough data to replicate the study. Faulkner and Trotter (2017) defined data saturation as a sample point when no new data found in data analysis, and the researcher had redundant data at this point. Faulkner and Trotter (2017) further explained that the researcher is confident that further collected data produce similar results, confirming the emerging study's themes and conclusion. Braun and Clarke (2019) also explained that data saturation is when no new codes or themes emerge, and data redundancy occurred during the researcher's study. I continued to collect data from all resources until no more codes or themes emerge. Fusch et al. (2018) suggested that data triangulation is used to find data saturation point when no new codes or themes emerge during the study's depth data analysis process. I used the triangulation method to test the data saturation point in this study. I used the interview data collected during Zoom meeting with each participant and use the same interview protocol questions (Appendix C) to reach the data saturation point. I also contacted and interview participants for a Zoom interview until I got the data saturation point. I collected the healthcare industry data until no new codes or themes emerge. Thus, I continued the data collection process until I found the data saturation point.

Transition and Summary

The objective of this pragmatic qualitative inquiry study was to explore strategies of the healthcare industry information technology (IT) leaders to implement secure procedures to protect patient health records on the private cloud-based CIS systems. I ensured that data collected from the participants' interviews are kept confidential using

NVivo coding method for identifying participants and organized. I mitigated bias using an Interview Protocol (Appendix C). I used ethical and methodological semi-structured qualitative interview strategies. I explored what strategies healthcare industry IT leaders use to implement secure access procedures to protect patient health records on the private cloud-based CIS systems. The triangulation method including healthcare industry or medical service providers' online documents, old archival information, or healthcare industry website document was used to support the finding of this pragmatic research study and this study's themes. I used five participants as a sample size. I got approval from Walden University Institutional Review Board (IRB before moving forward. I worked with the potential participants by using an informed consent form (Appendix A) and interview protocol (Appendix C). I had a video conference meeting by using a Zoom with each participant. I used organizational documents to complete triangulation I imported data collected from all participants interviews in NVivo 12 software application to do data organization, data analysis, and recognize the study's themes. This section two covered the purpose statement, role of the researcher, participants, research method and design, population and sampling, ethical research, data collection instruments, data collection technique, data organization technique, data analysis technique, reliability, and validity .

The next section three covered presentation of findings, applications to professional practice, implication for social change, recommendations for action, recommendations for further study, reflections, and summary and study conclusions.

Section 3 Application to Professional Practice and Implications for Change

Overview of Study

The purpose of this qualitative pragmatic qualitative inquiry study was to explore strategies of the healthcare industry IT leaders to implement secure procedures to protect patient health records on the private cloud-based CIS systems. The study's target population was CIO, CISO, or IT managers from the healthcare industry using strategies to secure private cloud-based CIS systems located in 400 miles radius from San Francisco, California.

Introduction and Presentation of Finding

The objective of the qualitative study was to explore strategies of the healthcare industry information technology (IT) leaders to implement secure procedures to protect patient health records on the private cloud-based CIS systems. I collected the data using Zoom interviews with senior IT managers, CIOs, or CISOs working in the healthcare industry for at least two years on their current jobs. I also reviewed 20 documents collected from government health care organizations, hospital websites, and other related healthcare companies.

I interviewed five IT managers working in the healthcare industry using Zoom communication tools. After permission, I audio-recorded the interviews and took notes during the Zoom interview. I used NVivo for interview data analysis and coding the interview results. The reflections and the conclusion of the study are presented in the end of this section. The four themes resulting from the data analysis process using Nvivo for this qualitative research study were (a) importance of security procedures and Policies, (b) importance of security awareness, (c) user training, and (d) importance of cyber security **r**esponse, which is aligned with Goodhue and Thompson (1995) TTF theory, which is this study's conceptual framework.

The main research question for this research study was: What strategies do healthcare IT leaders use to implement secure access procedures to protect patient health records on the private cloud-based CIS systems?

I found the four major themes during the qualitative data analysis process were (a) Importance of security procedures and policies, (b) Importance of security awareness, (c) User Training, and (d) Importance of cyber security response. The details are explained in Table 1.

Each Interview Candidate Participant (ICP) was assigned a unique number to protect privacy. I have ICP -1 for Interview Candidate Participant 1, ICP -2 for Interview Candidate Participant 2, ICP -3 for Interview Candidate Participant 3, ICP -4 for Interview Candidate Participant 4, and ICP -5 for Interview Candidate Participant 5 and ICP-6 for Interview Candidate Participant 6.

Table 1

Research study's Major themes Findings

Themes	Data Analysis Software NVivo' Word Count	Participant' Count	Participants

Importance of security procedures and policies	35	6	All
Importance of security awareness	31	6	All
User training	50	6	All
Importance of cyber security Response	44	6	All

I found the four major themes during   qualitative data analysis process were (a) Importance of security procedures and policies, (b) Importance of security awareness, (c) User Training, and (d) Importance of cyber security response.

Table 2 shows the six participant candidates their working sector, years of experience in healthcare IT management, number of employees working for them, and working location geographically.

Table 2

Demographic Information (Public hospital, Private hospital, or Mixed (Public and Private Hospitals) about the Interview Candidate Participants

Participants	Sector	Number Year of IT	Employee	Geographic
		Experience	supported	Location
ICP -1	Mixed	19	40	California
ICP -2	Mixed	15	30	California
ICP -3	Mixed	20	150	California
ICP -4	Mixed	11	25	California
ICP -5	Mixed	9	15	California
ICP -6	Mixed	16	60	California

The study research participants were 6 IT security managers who are or were responsible for the healthcare industry's private cloud-based CIS or EHRs systems used in hospitals located in California in a 400 miles radius from San Francisco Bay area. Bauer et al. (2017) suggested that information security managers should implement information security awareness (ISA) programs, which were systematically planned interventions to continuously secure the organization cloud-based application systems. . Robins & Eisen (2017) reported that Nvivo software application helped the researcher analyze the data visually and code that into research study themes. This study's findings were aligned with the researchers discussed in the literature review of this paper. The results of this study also aligned with Goodhue and Thompson's TTF conceptual framework. In the following section, the four themes are explained and reviewed from the lens of the conceptual framework.

Theme 1: Importance of security procedures and policies

The importance of well-defined security procedures and policies used in the healthcare industry's private cloud-based CIS or EHRs systems appeared as a theme based on the data analysis of the interview data of participants. This section has subthemes, including SQL injection, authentication, authorization, security misconfiguration, and encryption sub-policies around the organization procedures.

Table 3

Healthcare Application Information System Security Procedures and Policies References

Data	SQL	Authentication	Authorization	Security	Importance

Source	Injection			Misconfiguration	of Encryption
Participants	6	6	6	6	6
Documents	7	7	7	7	7

The documents listed in Table 4 were used for triangulation and were downloaded from government-recognized websites (www.nist.gov).

Table 3 shows that 6 participants participated in SQL injection, authentication, authorization, security misconfiguration, and encryption sub-policies. Table 3 and Table 4 shows that seven documents support the subthemes mentioned above

Table 4

Interview Participants have implemented used NIST Frameworks to protect their EHR/CIS cloud-based application system

Government Framework	Participants	Document Page Count
NIST Framework 800-140	ICP -1, ICP -4	24
NIST Framework 800-135	ICP -1, ICP -2, ICP -3	23
NIST Framework 800-132	All	18
NIST Framework 800-123	All	53
NIST Framework 800-111	All	40
NIST Framework 800-67	All	32
NIST Framework 800-44	ICP -1, ICP -2, ICP -3, ICP -4	142

The participants in the above table confirmed that they use NIST framework 800 documents in their healthcare cloud-based application system to ensure they can secure their application systems. They reported that they provided training to their users about implementing the NIST security policy framework for the healthcare application system. They also confirmed that they could protect more than 97% of their application system by applying the security policies and procedures aligned with the NIST framework.

Healthcare application system security procedures and policies are the critical component of the healthcare organization or hospital procedures or policies, which should align with IT CIS/EHR application system policies. The following were the subthemes implemented by all participants in their health care organization application systems related to the security vulnerabilities:

SQL Injection

The SQL injection is a web security risk that allows a cyber attacker to use the SQL queries to communicate with the application database server. Patil et al. (2017) defined SQL injection as a web security vulnerability that allows a cyber attacker to use the SQL queries to communicate with database systems. They further described that healthcare organizations should have SQL injection prevention policy to secure their data and network from data breaches. Participant ICP-2 explained that they have detailed security policies to protect the hospital patient or other related data from cyber-attacks coming from the outsider on their cloud-based healthcare application systems. Participant ICP-1 mentioned that his organization provided specific user training to their users on how to avoid sql-injection attacks. Participant ICP-3 also reported that the organization provided a specific strong password policy to protect their application servers from cyber-attacks. Participant ICP-4 confirmed that his organization had used a strong password policy against data breaches to the system. Participants ICP-5 and ICP-6 also confirmed that their organization had used proper user training and a strong password policy to validate their java and PHP programs in their EHR/CIS application systems. ICP -1, ICP -2, and ICP-3 confirmed that they implemented the NIST Framework 800-135 in their application system. All 3 participants confirmed that they had implemented the NIST Framework 800-132 & 123 in their healthcare application system. The participants ICP -1, ICP -2, ICP -3, and ICP 4 confirmed that they implemented the NIST Framework 800-140 in their application system.

My literature review supports this study’s findings. Using the TTF framework, Adamu et al. (2020) explained that weak authentication; cross-site scripting, SQL injection, and cross-site request forgery were the EHRs application system security vulnerabilities. They suggested that networking detection and monitoring tools can reduce the security vulnerabilities in the EHRs application system. Maraj et al. (2020) reported that cloud-based application systems could be secured using the proper organization’s SQL injection protection policy by closing unused network ports and security detection and prevention system, supported by my findings. Leppänen et al. (2020) reported that when IT managers used the SQL injection protection policy, there were fewer cyber-attacks on the web application system. The above literature review and this study’s findings align with the quality attribute of the TTF conceptual framework of this research study.

Authentication

The healthcare cloud-based application authentication and authorization are a critical part of data security based on data collected from the study participants. According to Hamidi (2019), authentication should be part of healthcare IT managers’ strategy to secure patient data in their application system. All participants confirmed that they implemented the NIST Framework 800-140 in their application system. Participant ICP-1 mentioned in his interview that his healthcare organization was using biometric technology face recognition feature as part of first step authentication. Their second step system sends a security code, and the user enters the code with the password to login into the system. He further reported that using the strategy helped the organization reduce the data breaches on their healthcare application system. Participant ICP-2 said that his company did not use the biometric technology face recognition feature as part of authentication last year. They experienced a breach in their system containing their data. As a result, they implemented the biometric authentication strategy and then they saw fewer attacks, and their IT managers felt more comfortable. The other participants, ICP-3, ICP-4, ICP-5, and ICP- 6 also confirmed that using biometric technology face recognition feature helped their healthcare organization reduce data breaches.

This subtheme is supported by my literature review. Hamidi (2019) stated that biometric face technology was a significant component of data security for healthcare application systems. Healthcare organizations should use biometric devices to provide access to hospital cloud-based CIS/EHR application systems. He further explained that hospital managers should utilize users' physical identity such as eye or face recognition when using IoT functions from mobile devices to the healthcare cloud-based application using NIST 800-124 security framework. Zulfiqar et al.(2019) reported that when IT managers implement deep face recognition using biometric devices, it should reduce data breaches in the healthcare application system. The study findings on the use of authentication plans are supported by TTF conceptual framework. Thota et al. (2018) explained that IT managers used authentication plans as part of their strategies to provide better results to secure the web-based application systems using end-to-end IoT mobile devices with user authorization and authentication login process and supported by conceptual TTF framework. The above literature review for this research study and this study's findings are aligned with user connection attributes of the TTF conceptual framework.

Authorization

The healthcare cloud-based application authorization is an essential part of patient record data security, according to data collected from the study participants. ICP-3 reported that his healthcare organization was using an application authorization model based on their specific job function. He gave an example of a doctor working in the emergency room who had authorized different patient data resources to nurses or doctors working in the surgery room. She was looking for various patient records. He said that the specific nurse should not view other patient records because she was not working on that patient at that particular time. He further confirmed that other medical support staff had access to different patient data, so their IT managers updated their authorization policy using an application access monitoring system. Nurses and doctors could access only those patient records they needed to perform their job functions using the network, not others' records. He further confirmed that with the implementation of the above monitoring policy, the results showed that there were fewer violations than before and the IT system notified those affected nurses' activities and their managers. Participant ICP-4 reported that when doctors use their mobile devices to enter the data and later submit it to the cloud-based application systems, they found greater data security vulnerability. He further explained that the doctors used assigned hospital desktop systems to enter the data into private cloud-based application systems. It provided better results than using public cloud-based applications. ICP-1 & ICP-5 also confirmed that authorization, authentication, and strong password policy were a part of user login strategy to the healthcare cloud-based application system. ICP-6 also mentioned that the authorization policy was a part of the user login strategy to the healthcare cloud-based software application system. Salehi et al. (2019) reported that cloud-based application system authorization models were essential in sharing data from different resources and sharing the resources over cross-domain access control systems in the healthcare industry. This subtheme is aligned with the authorization attribute of TTF conceptual framework.

This study's findings are supported by my literature reviewed.   Goodhue (1998) explained that TTF consisted of quality, authorization, compatibility, and location ability, project scheduling user training, user connection, and system reliability different factors; those are the major required factors for secure access procedures of CIS/EHRs systems and are directly relevant to my research study question. Moosavi et al. (2016) explained that IT managers must use the advanced authentication and authorization process to secure the healthcare industry resources and patients' private information. Zulfiqar et al.(2019) reported that when IT managers implement a secure authorization policy to provide access to cloud-based EHR/CIS application systems, the cyber-attacks rate should be reduced. Thota et al. (2018) also confirmed that when hospital IT managers use a proper secure authorization policy to provide access to their healthcare application systems, fewer data breaches would be on the network servers. The study findings on the use of authorization plans are supported by TTF conceptual Framework. All participants ICP -1, ICP-2, ICP-3, ICP -4, ICP-5, and ICP-6 confirmed that they had implemented the NIST Framework 800-140 in their application system as part of the user authorization policy. The literature and my study's finding are aligned with the authorization attribute of TTF conceptual framework.

Security Misconfiguration

According to all participants, the healthcare application system should be required to have a secure configuration using a correct method of deployment and testing of the application, application server, web server, and database. Participant ICP-1 reported that his hospital was using the security defense pathways, including software application development, quality assurance, and production environment configured all the same way with different passwords in those environments. Participant ICP-2 stated that his healthcare organization disabled administrative interfaces to the application system to resolve the security misconfiguration vulnerabilities. Participant ICP-3 mentioned that his healthcare organization disabled default accounts with corresponding passwords of the application system to fix the security misconfiguration vulnerabilities. Participant ICP-4 reported that his healthcare organization disabled the debugging of the software application online, and there were very low data breaches as a result. Participant ICP-5 said his healthcare organization configured application servers to prevent unauthorized access and directory listing to avoid application server security misconfiguration vulnerabilities. Participant ICP-6 noted that his hospital was running scans every week and monthly audits to detect future misconfigurations in the application server. All participants kept track of software updates based on a bug fixing process in the application, updated their environments using software application updates, and applied the patches to the web application. All participants also reported that they do internal audits and run scans to identify the misconfigurations in their application system.

This study's findings are supported by my literature reviewed. He et al. (2021) reported that the cyber attackers attacked the Intelligent Medical Diagnosis System (IMDS) application system and harmed the Healthcare Critical National Infrastructure (CNI). They further said that cyber attackers could damage the application system due to the security misconfiguration of their cloud-based application system. Tiwari (2021) reported that Information security managers could reduce the data breaches to the network application servers by implementing a security misconfiguration policy by eliminating XSS Vulnerabilities. The above literature reviewed for this research study and the finding of this study are aligned with the quality attribute of TTF conceptual framework.

Importance of Encryption

The final subtheme under Theme 1 was the importance of encryption. Participant ICP-1 mentioned in his interview that his healthcare hospital was using data encryption algorithms to transfer the patient data from wired or wireless client devices to web applications to process that data aligned with data encryption NIST 800 -111 framework. His organization used a private encryption strategy based on its security encryption policy. It then monitored the incoming or outgoing data from the cloud-based CIS/EHR online application system. Participant ICP-2 stated that his hospital used the RSA algorithm in data encryption strategies in their healthcare application system aligned with encryption NIST 800 -67 frameworks. As a result, there were very low weekly data breaches. Participant ICP-3 reported that his company used DES and AES in data encryption strategies in their healthcare application system aligned with block cipher encryption NIST 800 -67 framework. Participant ICP-4 reported that his company used the Hashes algorithm in data encryption strategies in their healthcare application system aligned with encryption NIST 800 -111. Participant ICP-5 said that his company used digital certificates algorithm in data encryption strategies in their healthcare application system when data transferred from source to destination aligned with encryption NIST 800 -111. Participant ICP-5 described that his healthcare organization used IPSEC and

PPTP algorithms in data encryption strategies in their healthcare application system when data transferred from source to destination aligned with encryption NIST 800 -63.

This study's findings are supported by my literature reviewed. Huang et al. (2018) mentioned that many healthcare industries ' EHRs are stored on untrusted cloud-based servers. They recommended using the encryption strategies algorithm such as attribute-based encryption on client-based application systems before submitting user data to the server-side application system. Nagasubramanian et al. (2020) explained that the loss of patients' confidential data could cause a severe security risk for the healthcare industry EHRs' cloud-based application system. They provided the solution to this problem to use the keyless signature infrastructure to ensure the digital signature security and authentication process during data transfer from source to destination cloud-based application system. They have suggested using blockchain technology to encrypt user data, which takes 50% less time, file size, and 20% cost less associated with transferring data from one machine to another than other conventional data storage techniques. Khan et al. (2020) suggested that healthcare organizations could use Secure Surveillance Mechanism with Probabilistic Image Encryption using Smart Healthcare IoT Systems such as mobile devices or smartphones. They further proposed that healthcare IT managers should use TensorFlow, python, lightweight YOLOv3 algorithm for extraction of patient imaging or text data key frames and MATLAB simulation for their cryptographically secure and faster communication to reduce transmission cost. All participants of this study implemented a security data encryption policy aligned with the security and quality attribute of the TTF conceptual framework of the study. Chaki et al.

(2019) reported that Healthcare IT managers should understand the Importance of security procedures and policies to prevent their healthcare cloud-based application systems data breaches. He further explained that many hackers used sql injection, authentication, authorization, security misconfiguration, and encryption security vulnerabilities that caused data breaches in the cloud-based application systems. Thota et al. (2018) also confirmed that when hospitals, IT managers cloud use private encryption keys on the client side to encrypt the data and server side to decrypt the data transfer and secure the web-application systems. Moosavi et al. (2016) reported that cloud-based web application data breaches could be reduced if IT managers used encryption keys to transfer data between source and destination servers. The literature reviewed for this research study and findings of the study are aligned with the quality attribute of TTF conceptual framework.

Theme 2: Importance of security awareness

The importance of well-defined security awareness used in the healthcare industry’s private cloud-based CIS or EHRs systems appeared as the second theme based on the data analysis from the interviews of IT security managers participants. This section has four subthemes, including Perform Risk Assessment Reports. Schedule regular testing, be consistent, and Compile Test Results & Make Improvements strategies (Table 5).

Table 5

Healthcare Application Information System Security Awareness

Source of Data	Perform Risk Assessment Reports	Schedule Regular Testing and be consistent	Compile Test Results & Make Improvements strategies
Participants	6	6	6
Documents	5	5	5

The documents listed in Table 6 downloaded from government recognized websites (www.nist.gov), were analyzed as part of the triangulation

Table 6

Interview Participants have implemented used NIST Frameworks to protect their EHR/CIS cloud-based application system

Government Framework	Participants	Document Page Count
NIST Framework 800-50	ICP -1, ICP -2 &	70
NIST Framework 800-39	ICP -1, ICP -2, ICP -3	60
NIST Framework 800-46	All	53
NIST Framework 800-40	All	90
NIST Framework 800-53A	All	792

The participants listed in Table 6 used NIST framework 800 cyber security awareness documents in their healthcare cloud-based application system to make sure they could secure their application systems. They reported that they provided good training to their users about implementing NIST security awareness framework orientation training about healthcare application systems at the beginning of their usage of EHR/CIS cloud-based system. They also confirmed that they could protect more than 99% of their application system by applying the security awareness procedures aligned with NIST framework. Healthcare application system security awareness policies are the critical component of the hospital organizations, which should align with IT CIS/EHR application system policies. Based on the data analysis, the following security awareness subthemes were essential to all participants in their health care organization application systems:

Perform Risk Assessment Reports

The perform risk assessment report is an assessment report completed by healthcare IT professionals, and it includes risk identification about their cloud-based web application systems. Participant ICP-1 explained that his organization identified the security gaps based on security risk assessment reports and performed the application server security measure to resolve those security gaps. Participant ICP-2 reported that his hospital identified the unused network port mentioned in the security risk assessment report and closed those network ports to determine security risks. Participant ICP-3 also noted that his healthcare company chose their internal security protocol and procedures to solve the security risks identified in the risk assessment report. Participant ICP-4 reported that his hospital removed unnecessary or obsolete network application ports from their network to resolve risks identified in the risk assessment report. Participant ICP-5 said that his healthcare organization decided and maintained patient privacy laws based on the risk assessment report. Participant ICP-6 mentioned that his company's risks were related to third party vender EHR/CIS application and coordinated with them to resolve it. ICP -1, ICP -2, and ICP-3 confirmed that they had implemented the NIST Framework 800-135 in their application system. ICP -1, ICP -2, and ICP-3 also verified that they had implemented the NIST Framework 800-50 & 39 in their healthcare application system. Participants ICP -1, ICP -2, ICP -3, and ICP-4 reported implementing the NIST Framework 800-46 & 800-40 in their application system. All participants verified that they implemented the NIST Framework 800-53A in their application system. All participants confirmed that they performed risk assessments as part of their monthly and quarterly internal audits, which were part of the security awareness processes in their application system.

The finding of Perform Risk Assessment Reports subtheme supports the quality attribute of TTF conceptual framework. Singh (2017) defined a risk assessment report as an essential part of the TTF conceptual framework, either in graphical or narrative form. The main things to be studied, such as the key factors, concepts, or variables associated with the purpose statement of the study, were included in the report. Kamerer and McDermott (2020) defined that risk assessments might be performed according to the results documented in a risk assessment report that notifies what actions to be taken to resolve the problems mentioned in the application system security assessment report. They further reported that it was critical to use risk assessment tools to remove the security gaps on healthcare cloud-based application systems. Jofre et al. (2021) reported that once IT managers performed and analyzed risk assessment reports of the security of web application servers, they should take the appropriate actions to resolve the security gaps reported in that report. The literature reviewed for this research study and the participants' weekly or monthly risk assessments were aligned to the quality attributes of the TTF conceptual framework.

Schedule Regular Testing and be consistent

The healthcare cloud-based application regular testing was a second subtheme that is an essential part of data security awareness based on data collected from the study participants. Samkari & Gutub (2019) defined that software schedule regular testing including software application testing procedure including testing of scripts or tools to identify the problems in the application system. They further reported that cloud-based software patient records application testing should be part of healthcare IT managers' strategy in securing patient data in their application system. All participants confirmed that they implemented the NIST Framework 800-202 & 800-192 in their application system. Participant ICP-1 reported that his organization daily monitored cyber-attacks log files and took the appropriate steps to block those attacks. Participant ICP-2 said in his interview that his healthcare organization had been using internal audit software application testing monthly and quarterly using network monitoring data as part of regular testing. Participant ICP-3 reported that his company used an old vendor network technology monitoring application system, which was outdated and was vulnerable to data breaches attack. For the past few years, they have been using a different vendor's network software application. They saw fewer data breaches attacks on their application system, and the updated monitoring strategy helped them reduce the outsider attacks. Afterward, IT managers felt more comfortable about their cloud-based healthcare application system. Participant ICP-4 mentioned that his hospital IT professional did the basic testing for each function of the software application system to remove the security risks associated with the software application. Participant ICP-5 said that his healthcare IT software testers performed internal audit and static code review using static code analysis tools to find the problems in software and took appropriate actions to mitigate it. Participant ICP-6 mentioned that his medical services organization's IT engineers performed the software units testing to identify the security gaps and resolve them using their internal tools. All participants reported that performing software unit testing to determine the security gaps helped reduce data breaches on their web application servers.

Yeboah-Ofori et al.(2019) reported that the IT managers should do the internal and external software application testing audit monthly internal audit and quarterly external software testing audit provided by the certified company on hospital cloud-based CIS/EHR application systems. He further explained that hospitals managers should know users' mobile application access testing, which many users use to access the healthcare cloud-based application using NIST 800-202 security framework.

With the proper mapping of the TTF theory to the cloud-based online application, the system helps the users operate the online application comfortably. Wu and Chen (2017) used the TTF model to calculate how data technology leads to an increase in output by testing the match between technology characteristics and task characteristics. They further explained that a specific user or employee's experience with the information application system helped them adapt to that technology. Wang & Lin (2019) reported that performing software unit testing was an essential part of TTF framework, which increases the quality services attribute of TTF framework. The above literature reviewed for this research study and findings of the study is aligned quality service property of TTF conceptual framework.

Compile Test Results & Make Improvements strategies

IT managers analyze the testing log files produced by networking scanning and protection software tools. They design a strategy to resolve the problems found in test results after analyzing the log files. Das et al. (2021) reported that cloud-based application system compile and analysis application usage log file was a critical process to healthcare organization user data, and IT managers should update their application based on the results of the analysis of the log file. They further suggested that when each user or employee of the healthcare organization logged in to perform their job functions in a cloud-based application system, their access and other related information logged in to the web server log file. Participant ICP-1 reported that they identified the internal and external users of the software application system and notified them about the upcoming software update schedule. Participant ICP-2 mentioned that his organization performed the site review when nurses, doctors, or hospital staff member used their mobile devices inside the hospital and collected the updated requirements for mobile devices for secure access to their software application system. Participant ICP-3 reported that they analyzed healthcare software application update requirements, scheduled a software update schedule, and communicated with affected users before and after the updates. Participant ICP-4 said they investigated the risks assessment report from their internal audit report and planned to update the application system to close out security risks.   Participant ICP-5 reported that his healthcare organization compiled the results of user access and network monitoring log. Then their IT network analyst analyzes the log file and updates their application system accordingly. He further confirmed that IT professionals analyze that network log file frequently to see the unusual network attacks or activities on their application system and made changes to the application system based on the results of their analysis. Participant ICP-6 reported that his organization analyzed the security risks, created an action plan, communicate with users about the software update schedule, performed a software update, tested it and analyzed the results, and finally notified the users by email. All confirmed that they had implemented the NIST Framework 800-202,800-192, 800-140, and 800-166 in their application system as part of the application updated policy.

The web application test results and taking actions on those results could increase the output of the web application network servers, which aligns with the TTF framework's technical characteristics and task characteristics. Wu and Chen (2017) used the TTF model to calculate how data technology can increase output by testing the match between technology characteristics and task characteristics. They further explained that a specific user or employee experience with the information application system helped them adapt to that technology. Wang et al. (2020) also confirmed how networking data technology helps increase the testing output match between networking technology and user tasks properties. The literature reviewed for this research study and participant interviews implemented web application software testing schedule policy aligned to the quality service property of the TTF conceptual framework.

The conceptual framework of this research project was the TTF. These findings of this theme pointed out the importance of security awareness measures in cloud-based EHR/CIS application systems and supported the TTF conceptual framework. Alzubaidi, A. (2021) explained that healthcare IT professionals and managers should understand the importance of security awareness to prevent their healthcare cloud-based application systems data breaches from cyber-attacks. He further explained the Performing Risk Assessment Reports, Providing Interactive Training Courses, Schedule Regular Testing and Compiling Test Results & Make Improvement's strategies could be used to protect EHR/CIS application systems. The literature and participant responses implemented the security awareness policies and updates based on their application system vendor's requirements, which aligned with the quality attributes of TTF conceptual framework.

Theme 3: User Training

Well-planned user training for cloud-based applications for the healthcare industry's private cloud-based CIS or EHRs systems appeared as the third theme based on the data analysis from the interviews of IT security managers participants. This section has several subthemes, including setting training goals, assessing end-user needs, developing training content and delivery methods.

Table 7

Healthcare Application Information System User training

Source of Data	Setting training goals	Assessing end-user needs	Developing training content and delivery methods
Participants	6	6	6
Documents	10	10	10

Table 8

Interview Participants have implemented used NIST Frameworks for User training of EHR/CIS cloud-based application system

Government Framework	Participants	Document Page Count
NIST Framework 800-140	All	24
NIST Framework 800-135	All	23
NIST Framework 800-132	All	18
NIST Framework 800-114	ALL	70
NIST Framework 800-111	All	60
NIST Framework 800-50	All	53
NIST Framework 800-39	All	90
NIST Framework 800-53A	All	792
NIST Framework 800-46	All	53
NIST Framework 800-40	All	90

All participants reported in Table 8 that they used specific documents in their healthcare cloud-based application system from NIST framework 800 cyber security user training to ensure they could secure their application systems (Table 8). They reported that they provide healthcare application system user training at the new employee orientation day and provide updated training on a quarterly basis depending upon security updates on cloud-based application systems, which were aligned with the implementation of the NIST security user training framework. They also confirmed that they could protect more than 97% of their application system by applying the user training procedures aligned with NIST framework.

Healthcare application system security user training policies are an essential part of the hospital organizations, which align with IT CIS/EHR application system user policies. The following were the subthemes implemented by all participants in their health care organization application systems related to the user training:

Setting training goals

Setting up training goals for users of cloud-based application systems is an essential part of their strategies to secure them and is the first subtheme of theme 3. Dang et al. (2018) explained that software application user training was an essential part of cloud-based software applications for hospital IT managers' strategic planning to secure healthcare application systems. They further defined that healthcare organizations should have software application user training as a prevention policy to secure their data and network from data breaches. Participant ICP-1 reported that his healthcare company had software application user training policies for new users and current employees. He further said that his IT managers assessed the needs of the user training and identified the objectives of the training. Participant ICP-2 reported that his hospital analyzed the security risks, set up the software application security training objectives, and developed an action plan to train the users. Participant ICP-3 said that his healthcare organization assessed the training needs according to the user’s feedback, network security risks, and third-party vendor's application system update requirements and prepared training according to user needs. Participant ICP-4 reported that cloud-based software application user training was essential for their security strategy to protect from data breaches. He further said that with the updated user training, they fewer cyber-attacks on their servers. Participant ICP-5 explained detailed security user training policies for new users on their job orientation day. He further said that “Each user needs to complete their cloud-based software application EPIC system training and on the end of training user needs to pass the test. Once the user completes that training, they are allowed to start job function”. He further said that “Their specialized EPIC healthcare application system provided by the vendor helped their hospital secure their system.” Participant ICP-6 also confirmed that cloud-based software application user training was an essential part of the security strategy of their software application system.

All participants confirmed that they implemented the NIST Framework 800-140 in their application system. All participants also confirmed that they had implemented the NIST Framework 800-50 & 39 in their healthcare application system. The participants ICP -1, ICP -2, ICP -3, and ICP-4 confirmed that they implement the NIST Framework 800-132 & 800-114 in their application system. All participants also confirmed that they implemented the NIST Framework 800-50 in their application system. All participants also confirmed that they updated user training goals aligned with the business strategic plan based on EPIC EHR/CIS application system security requirements as part of their monthly and quarterly user training updates published on their internal and public websites. Liang et al. (2017) reported that healthcare IT managers should set up the end-user training goals to educate their users on using the software application system from the users' mobile devices '.

Setting training goals of cloud-based EHR/CIS application systems for user training aligned with the TTF framework's technology user training and task characteristics. The web application technology setting training goals, user training, and user communication are an essential part of user training attribute TTF theory (Dang et al., 2018). The lack of professionally setting up training goals by IT managers can cause data breaches of patent records on cloud-based EHRs/CISs systems (Chen & Benusa, 2017). Wu and Chen (2017) used the TTF model to calculate how setting training goals as part of the user training led to an increase in the security output match between technology user training characteristics and task user training characteristics. The literature and participants' interview data are aligned with the user training feature of TTF conceptual framework. The findings of these sub-themes point out the setting up training goals for cloud-based EHR/CIS application systems and supported the TTF conceptual framework.

Assessing end-user needs

Assessing end-user needs is a second subtheme and critical component of the user-training theme based on the data collected from the participants of this research study. Sebetci (2018) explained that IT managers should analyze and assess the needs of the user of cloud-based software patient records applications in securing patient data. All participants confirmed that they had implemented the NIST Framework 800-132 & 800-114 in their web application system security user training. Participant ICP-1 reported that his healthcare organization IT security managers identified what employees need to perform for EHRs/CIS application system job functions and created a plan to develop application security training for software application systems. Participant ICP-2 reported that his medical services office assessed the user training based on their job responsibilities and scheduled training sessions online and onsite according to their employees' working locations. ICP-3 stated that his hospitals offered cloud-based software application user training based on their needs and assessed their performance during and upon the completion of the training. Participant ICP-4 said in his interview that his healthcare organization IT managers considered user training based on their user job functions. He further said that as IT security manager, he used end-user needs assessment results to develop the user training of the cloud-based healthcare application EPIC system. ICP-5 also reported that his hospital developed customized training for their employees and patients based on their specific user task functions. Participant ICP-6 reported that his company used an open-source created patient healthcare application system and received many data breaches attack. He further said that they evaluated and tested another health NetApp health application based on other user rating 4-5 years back and assessed the needs of user training for their system users for the application.   After providing Netapp health application vendors with the user, they found fewer data breach attacks on their application system. They conducted the updated user training strategy, which helped them reduce the outsider attacks. Afterward, IT managers felt more comfortable about their cloud-based healthcare application system.

Based on the findings, IT security managers should assess end-user needs for their cloud-based EHR/CIS application systems as part of the technology user training, which is aligned between technology user training and task characteristics of the TTF framework. Sebetci (2018) suggested that hospital IT managers perform internal and external user software application training based on user needs. He further recommended that hospital managers provide user training for their healthcare application systems, which many users use to access the healthcare cloud-based application using NIST 800-132 and 800-114 security framework. All participants confirmed that they implemented the NIST Framework 800-132 & 800-114 in their application system. Rathert et al. (2017) suggested that assessing end-user needs by the IT security managers could help them plan cloud-based web application technical training for their system users, which is aligned with the user training feature of TTF framework. The literature and the participant information supported end-user needs of user training of healthcare web application software policy that aligned with the user training property of TTF conceptual framework.

Developing training content and delivery methods

The final subtheme under theme-3 was developing training content and delivery methods. The delivery methods can be Instructor-led training in a classroom, virtual classroom like Zoom, E-Learning like Blackboard or canvas, mobile learning, or hybrid learning methods. Chaturvedi et al. (2019) reported that healthcare organizations could use instructor-led training, Zoom virtual classroom, E-Learning, mobile learning, or hybrid learning methods based on their end-user needs. VonBastian et al. (2016) reported that the user training delivery method consisted of training presentations, discussions, hands-on lab assignments, and assessment of using software application systems. Participant ICP-1 said that his organization provided instructor-led training to their employees based on their job functions. Participant ICP-2 reported that his healthcare organization compiled the results of end-user needs. Then their IT network analyst analyzes the end-user needs data log file and develops their application system user training accordingly. He gave an example that his hospital IT instructors developed the user-training with the vendor support, so user training could be offered to employees and patients based on their needs with onsite as well as online delivery methods. He further confirmed that IT instructors analyze the user feedback of the user training and update the training contents accordingly. Participant ICP-2 reported that when nurses, doctors, or hospital staff members received and passed user-training of cloud-based application systems, they felt more comfortable about their job functions. Participant ICP-3 said that his hospital offered virtual classroom user training based on their doctors, nurses, other employees’ job functions. Participant ICP-4 mentioned in his interview that they require hospital staff to use devices connected to the wired network during their user training and when performing their job functions. He further reported that they provided updated training to the users when they updated their application system. This process helped them secure the application system, and they felt more comfortable. Participants ICP-5 and ICP-6 provided software application system user training based on their job tasks. All participants confirmed that they analyzed the user needs and provided user training based on their needs on their healthcare application system. Liang et al. (2017) explained that user training delivery methods and developing content by IT certified instructors were a critical part of the end-user training of the healthcare cloud-based application system. All participants ICP -1, ICP-2, ICP-3, ICP -4, ICP-5, and ICP-6 confirmed that they had implemented the NIST Framework 800-140,800-135, 800-132, and 800-114 in their application system as part of the cloud-based EPIC application system user training policy.

The literature supports the findings of this study. Klappe et al. (2020) reported that developing training content and delivery methods were an essential part of proper user training of hospitals of cloud-based health records application was the one of the reason that many healthcare organizations could avoid data breaches in their EHR/CIS application systems. They further concluded that redesigning the hospital’s software application system policies to improve user training could increase the security of electronic patient records. Chaturvedi et al. (2019) also reported that developing training content and delivery methods was an essential part of user training of the cloud-based health records application system, reducing data breaches on the web application servers. The literature review and the participants’ findings related to developing training content and delivery methods of user training of healthcare web application software policy, aligned with user training property of TTF conceptual framework.

Theme 4: Importance of cyber security response

The importance of well-defined cyber security response procedures for cloud-based applications for the healthcare industry's private cloud-based CIS or EHRs systems appeared as the fourth theme based on the data analysis of the collected data from the interviews of IT security managers. This section has three subthemes: incident detection and identification, containment and recovery, damage and severity assessment (Table 9).

Table 9

Healthcare Application Information System Cyber Security Response

Source of Data	incident detection and identification	containment and recovery	damage and severity assessment
Participants	6	6	6
Documents	5	5	5

The documents listed in Table 10 were downloaded from government recognized websites (www.nist.gov)

Table 10

Interview Participants have implemented used NIST Frameworks to protect their EHR/CIS cloud-based application system

Government Framework	Participant	Document Page
NIST Framework 800-86	All	65
NIST Framework 800-85	All	59

NIST Framework 800-84	All	65
NIST Framework 800-184	All	97
NIST Framework 800-171A & 172A	All	91

Participants confirmed that they could protect more than 97.99% of their application system by applying the security incident response procedures aligned with the NIST framework. Healthcare application system cyber security incidence and response policies are an essential component of the hospital organizations' security policies, which align with IT CIS/EHR application system policies. The following subthemes detail the security responses by all participants in their health care organization application systems related to the cyber security incidents:

Incident Detection and Identification

The incident detection and identification s for users of cloud-based application systems are an essential part of their cyber security response procedures to secure their cloud-based application systems. McGlade & Scott-Hayward (2019) defined incident detection and identification as the procedure of finding cyber-attackers in hospital network infrastructure, recreating their activity in system log files, and taking appropriate actions or measures to protect cloud-based application system in the future. They further explained that hospital IT managers should notify the users and update their application system using cyber security update procedures to remove the security risks. They also reported that it was essential to find out security threats in software application systems by monitoring and analyzing network log files.

The research study showed that all participants used incident detection and identification activities. Participant ICP-1 explained that his organization identified the data breach incidents daily on their application system server by analyzing system log files. This helped them find the security holes based on their network security tools log files analysis and performed the procedures to resolve those security gaps. Participant ICP-2 reported that his hospital identified the incident and identified unused network ports using Wireshark scan tools to close those network ports to determine security risks. Participant ICP-3 said that his hospital company chosen internal security scanning tools to identify the incidents and applied their procedures to solve those network security problems. Participant ICP-4 reported that his hospital used intrusion detection systems (IDS) to detect cyber-attacks and has taken appropriate measures to resolve those problems. Participant ICP-5 said that his healthcare hospital IT managers used intrusion protection systems (IPS) to see the data breach attacks and resolve those security problems daily. Participant ICP-6 mentioned that his medical services company used strong firewall programs, IDS, and IPS to detect and identify the outsider's cyber-attacks on their application system servers and resolved those security problems using their internal security protection tools. ICP -1, ICP -2, and ICP-3 participants confirmed that they implemented the NIST Framework 800-83 & 84 in their application system. All participants confirmed that they had implemented the NIST Framework 800-50 & 39 in their healthcare application system. Participants ICP -1, ICP -2, ICP -3, and ICP-4 confirmed implementing the NIST Framework 800-84 & 800-85 in their application system. All participants reported that they implemented the NIST Framework 800-86 in their application system. All participants confirmed that they performed risk assessments as part of their monthly and quarterly internal audits, which were part of their application system's security awareness processes.

This subtheme's findings are supported by the literature review. Singh (2017) found that incident detection and identification were critical sections of the TTF conceptual framework and defined the main topics to be studied, such as the key factors, concepts, or variables associated with the purpose statement of the study. Thompson (2018) also reported that incident detection and identification were essential parts of the TTF conceptual framework. Previous research and participant responses supported the use of incident detection and identification methods weekly basis, which were aligned quality attribute of TTF conceptual framework of this research study.

Containment and Recovery

Healthcare cloud-based application containment and recovery of risk incidents were the second subtheme of data cyber security response themes based on data collected from the study participants. According to Thompson (2018), organizations should consider which servers need to be turned off and what files need to be deleted in the software application containment phase. He further suggested that strategies should be defined to bring the software application servers back and secure their network servers, and Software application containment procedures should be part of healthcare IT managers' strategy in securing patient data in their application system. All participants confirmed that they implemented the NIST Framework 800-86 & 800- 184 in their cloud-based EHR/CIS web application system. Participant ICP-1 reported that his organization analyzed the effects of the data breach first and removed the affected systems from the network. Participant ICP-2 said that his healthcare company used its internal tools to see which cyber data breaches damaged network servers and files. Once they analyzed the servers affected by the cyber-attack, they restored the data from the backup servers. Participant ICP-3 confirmed similar action reported by participant ICP-2. ICP-4 said that in his hospital when they saw a data breach on their network, their IT security engineers reviewed web application server log files to identify the affected file systems. He further said that they removed those servers from the network, analyzed the file system, restored the server with a fully functioning backup system, and tested it. Participant ICP-5 and Participant ICP-5   confirmed the similar actions reported by participant ICP-4.

The literature supported the findings of this subtheme. Lim & Greenwood (2017) reported that hospital IT managers should shut down the network servers affected by cyber-attacks and follow the Incidence recovery process and test the servers before putting them back online to provide medical services. They further explained that hospital managers use the proper firewall and virus scanning tools, monitor the log files, and take appropriate measures to secure their EHR/CIS application system. They also suggested that hospital IT managers should use NIST 800 framework to secure their network from outsiders. Thompson (2018) explained that IT managers should shut down those network servers affected by cyber-attacks and follow the incidence recovery process and test the servers before putting them online for providing medical services. This study’s findings are aligned with the literature and with TTF conceptual framework.

All participants confirmed using NIST cyber security framework 800-86 & 800- 184 at their healthcare organization to secure their web application software systems. The participant responses are aligned with the quality service properties of TTF conceptual framework.

Assess the damage and severity

The last subtheme of the cyber security response theme is based on data collected from the study participants. Jofre et al. (2021) reported that it was crucial or critical to complete damage assessment of user data caused by healthcare point-of-sale data stored on cloud-based application system servers; IT managers should compile the assessment report and then secure their cloud-based application servers against the data breaches based on the results of the analysis of the damage assessment log file. They further suggested that all user and data breach activities should be logged into the application system web server log file. Participant ICP-1 reported that his company assessed the system data damage by analyzing the assessment log file using their internal scanning tools and finding weaknesses in their network. He further said that once they saw the cause of the system data breach, their IT managers used data breach response policy protocol to resolve the problems. Participant ICP-2 mentioned that his hospital collected the data breach information from IT departments based on their analysis of the system scanning tools and then secured the system based on the causes reported in the log file. Participant ICP-3 said that they analyzed healthcare software application security gaps based on data breach causes and applied their cyber security response plan procedures to mitigate intrusions in their application systems. Participant ICP-4 said they analyzed the damaged system assessment report and updated their application system according to the damage assessment report.   Participant ICP-5 reported that his healthcare organization compiled results of their security scanning tools, restored their system with good backup data from the previous iteration, and tested it. Participant ICP-6 mentioned that his hospital analyzed the data breaches assessment report, made an action plan, communicated with users about the application software server data breaches, and took specific measures to resolve the problem in the future. He further reported that their IT managers performed software updates, tested and analyzed the results, and finally notified the users by email. After the process, their users felt comfortable using cloud-based application systems. All confirmed that they had implemented the NIST Framework 800-171A and 800-172A in their application system as part of the application system response policy.

This study's findings in this subtheme are supported by the TTF conceptual framework of the study. Arndt et al. (2017) used the TTF model to calculate how data technology leads to an increase in the output by testing and updating the match between technology application systems characteristics and task characteristics. Lim & Greenwood (2017) also confirmed that TTF conceptual framework could be used to calculate how data technology leads to an increase in the output by testing and updating with needed updates to secure the system, which was aligned with the quality property of TTF framework.

The findings in the last theme, which is the importance of cyber security response, are supported by the TTF conceptual framework of the study. Arndt et al. (2017) explained that Healthcare IT professionals and managers should understand the importance of cyber security response procedures to prevent their healthcare cloud-based application systems data breaches from cyber-attacks. Jofre et al. (2021) also reported that the importance of cyber security response was critical for IT security managers' security procedures to secure their cloud-based web application systems. This theme's findings are aligned with the quality attribute of TTF conceptual framework and supported by the literature.

Applications to Professional Practice

This study explored strategies of the healthcare industry information technology (IT) leaders to implement secure procedures to protect patient health records on the private cloud-based CIS systems located within 400 miles radius from San Francisco, California. The study's findings are suitable for Chief Information Officers (CIOs), CISO, or IT managers working in the healthcare industry to use strategies to secure their private cloud-based CIS systems located in California. Participants specified that their contribution could play an essential role in implementing secure strategies to secure their hospital's web-based software application systems in a private cloud system.

The scheduled user training, education, communication with users about the software updates, and cyber security response procedures strategy are significant components to increase the security awareness of cloud-based CIS application systems and reduce the data breaches in current internet-based healthcare application systems.

Rathert et al. (2017) reported that when healthcare companies implement successful, secure procedures to secure patient health records on the private cloud-based CIS systems, the systems' user confidence level increases about the usage of cloud-based CIS application systems. Dang et al. (2018) further explained that if the Chief Information Officers (CIO), CISO, or IT managers offer the threat protection on their network following the features of TTF by offering user training programs before users start using the online application, it would help the users to avoid social engineering attacks. The user training provided by IT professionals to application system users plays an essential role in securing CIS application systems used in hospitals.

This study’s findings may help California hospital IT managers implement secure procedures to protect cloud-based software application systems. Healthcare IT companies can use the strategies identified in the findings to build trust inpatients and hospital system users and secure patient data. The distinct and clear-cut security strategies such as SQL Injection avoidance procedures and strong authentication and authorization policies such as strong password policy and encryption procedures can help hospital CIO, CISO, or IT managers secure the cloud-based software application systems. This study’s results offered strategies for healthcare organizations' IT managers to upgrade their security policies and help their healthcare organizations improve their confidence in application users and become comparative with CIS application systems. Hospital IT managers can implement secure procedures to protect user data on the private cloud-based CIS systems by providing user training and improving their reputation in the public domain. The hospital CIO, CISO, or IT managers can minimize the data breaches on their network servers by using strategies identified in the finding.

Implications for Social Change

Using strong strategies to protect healthcare systems, healthcare industry information technology (IT) leaders can implement secure procedures to ensure the safety of patient health records on the private cloud-based CIS application systems. The strategies identified may help healthcare organizations CIO, CISO, or IT managers understand and implement more secure procedures to protect hospital cloud-based software application systems, affect social change in their hospital culture, support a better reputation to the general public, and improve system users confidence levels. An empowered culture in healthcare companies allows IT, managers, to prepare better strategies to implement secure procedures to protect their network servers and reduce cyber data breaches, which will improve CIS/EHR cloud-based application system security in the patients and users domain.

The awareness of the fundamental strategies to protect cloud-based CIS/EHRs hospital application systems can be another implication for a social change. Bao et al. (2017) suggested that data breaches on healthcare applications systems could be reduced significantly if IT managers use strong strategies to identify the network vulnerabilities and risks and then use specific strategies to resolve those risks. The IT managers' clear communication and open-door policy with their IT security engineers and other supporting IT staff teamwork, helps the healthcare organization IT managers to resolve the security risks associated with software application systems, which may promote great social change in local healthcare organizations. This process also demonstrated that IT staff members and when IT managers' provide leadership dedication, and support for their IT security professionals, moral improves which, in turn have lower unemployment rate in the local community. According to a the literature review less communication between healthcare executive IT managers and other IT staff members may cause more data breaches in hospital cloud-based application systems. Wong & Laplante (2017) reported that good communication between senior-level IT managers and IT security administrators and IT managers often would help them provide specific security procedures strategies to secure their application network servers.

The results of this study and effective communication between hospital IT managers and other professional IT staff members may help other hospitals in the US and other parts of the world reduce the data breaches on their EHRs/CIS cloud-based application system. The findings of this study may help the other hospitals and healthcare services secure their application system, which will promote major social change in the community.

Recommendations for Action

This study is about strategies for healthcare industry information technology (IT) leaders or managers working in hospitals in California, other states in the USA, and worldwide to protect their cloud-based application systems. My first recommendation to a healthcare organization or hospitals IT security managers or chief information officers (CIO) is to team up with their cloud-based application security administrators or IT professionals to review their current security procedures and policies to make sure they have strong authentication rules in place to avoid cyber-attacks on their network application servers. Healthcare IT managers should understand the vulnerabilities of their healthcare cloud-based application systems to data breaches. Many hackers use sql injection, weak authentication and authorization policies, security misconfiguration, and encryption security vulnerabilities to cause data breaches in cloud-based application systems. Any small or medium-sized hospitals organization IT managers using weak security procedures should review their current policies and review the strategies identified in this study to help them better protect their EHRs cloud-based application systems from data breaches.

The second recommendation is the importance of developing security awareness among the healthcare and hospital employees as a critical component for IT security managers to secure their network application servers from outsiders or data breaches on their application system. To develop security awareness, hospital IT security managers should perform risk assessment reports and generate risk reports; schedule regular, consistent testing to compile and use test results to improve strategies to secure their EHR/CIS application systems from cyber-attacks. Sharing the results of these measures increases employee security awareness.

The third recommendation is to provide security system user training to maintain the security of the cloud-based EHRs/CIS application. The cloud-based EHRs/CIS application system user training between healthcare organizations or hospital employees is essential to secure network application servers from outsiders or data breaches on their application system. The developing training content and delivery methods are a critical part of user training for the hospital of cloud-based health records application systems. Providing web-based application system user training may avoid data breaches in their EHR/CIS application systems. By redesigning software application system policies hospital, IT managers can improve user training increase the security of electronic patient records.

The final recommendation is to have well-defined cyber security response procedures for cloud-based applications for the healthcare industry's private cloud-based CIS or EHRs systems. These are essential to hospital IT managers in securing their network application servers. The cyber security response procedures play a crucial role in reducing data breaches on hospital cloud-based EHRs application systems. IT managers review should implement strong policies to handle Incident Detection and Identification; Containment and Recovery, Assessment of the damage and severity to reduce the severity of the data breaches in their healthcare cloud-based application systems from data breaches.

The study's findings will be published or disseminated to hospital IT managers, IT security managers, or other IT professionals working in the healthcare industry all over the United States of America or around the world. The further research is recommended in hospitals or healthcare organizations located in other states. This study was conducted 400 miles radius from San Francisco bay area and further study may be disseminated in other parts of country and it may produce better diversified results securing hospital cloud-based web application systems. The disseminating and sharing of those finding may help IT managers located in part of the United States of America.

Recommendations for Further Study

I interviewed hospital IT security managers in the California bay area findings shown. My first recommendation is to generalize to other parts of the US by broadening the participant geographic pool. My second recommendation is to expand the research question to healthcare insurance companies' IT security managers to study the secure procedures on the medical insurance web-based software application systems. The purpose of this qualitative study was to explore strategies of the healthcare industry information technology (IT) leaders to implement secure procedures to protect patient health records on the private cloud-based CIS systems. My last recommendation is that other researchers could use a mixed design method, which is a combination of quantitative and qualitative research methods. This may give them the opportunity to interview large number of participants once the covid pandemic is over. They can collect data from a large population using questionnaires, thus having findings are more diverse.

Reflections

I have been working as a CIO/CTO/ IT security consultant and manager for many years to develop, set up, and secure web-based application systems, including healthcare application systems. I have taken many advanced classes in cyber security to secure and manage web application systems used in California higher education colleges and universities, healthcare industries, finance industry, information technology, hardware semiconductor and software companies, and auto industries. I am a CIO/ CTO and have more than 20 years of highly technical experience with many projects in software web, cloud, or mobile applications development, develop software network management applications, cyber security, central processing design, graphics chip design, system-level validation, web application design and testing, and Cisco Networking system administration projects, at many companies including INTEL, IBM, California Business and Technology, Broad Com, ITT-TECH, DeVry, and other customer sites., VMWARE, or Citrix, etc. I have many years of interview experience with technology professionals as part of hiring committees in companies, colleges, and universities. I experienced interviewing the participants of this research study and writing down their responses to the interview questions in a humble environment. The data collection and analysis based on participants' responses were a significant part of the research study with no bias. These research results would help IT managers working for hospitals or healthcare organizations secure their cloud-based application systems using their secure strategies.

Summary and Study Conclusions

The hospitals or healthcare medical services providers' main responsibility is to protect patent's health records and compliance with government HIPPA law. The hospital IT managers, CIOs, CISO, or other security IT managers should understand their cloud-based EHRs/CIS application systems importance of security procedures and policies, importance of security awareness, user training for their employees or patients, and importance of cyber security response. The hospital IT managers should join IT cloud-based professional development organizations, so that they can attend cutting edge hospital cloud-based application systems conferences all over the USA and implement the new security procedures to protect their cloud-based EHRs/CIS application systems and then there are less chances for data breaches on their web-based application systems.

References

Abdalla, M. M., Oliveira, L. G. L., Azevedo, C. E. F., & Gonzalez, R. K. (2018). Quality in qualitative organizational research: Types of triangulation as a methodological alternative. *Administração: Ensino e Pesquisa*, *19*(1), 66-98. https://doi.org/10.13058/raep.2018.v19n1.578

Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. *Journal of Big Data*, *5*(1), 1. https://doi.org/10.1186/s40537-017-0110-7

Adamu, J., Hamzah, R., & Rosli, M. M. (2020). Security issues and framework of electronic medical record: A review. *Bulletin of Electrical Engineering and Informatics*, *9*(2), 565-572.doi: https://doi.org/10.11591/eei.v9i2.2064

Akhu-Zaheya, L., Al-Maaitah, R., & Bany Hani, S. (2018). Quality of nursing documentation: Paper-based health records versus electronic-based health records. *Journal of clinical nursing*, *27*(3-4), e578-e589. https://doi.org/10.1111/jocn.14097

Alase, A. (2017). The interpretative phenomenological analysis (IPA): A guide to a good qualitative research approach. *International Journal of Education and Literacy Studies, 5*(2), 9-19. https://doi.org/10.7575/aiac.ijels.v.5n.2p.9

Albladi, S. M., & Weir, G. R. (2018). User characteristics that influence the judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences*, *8*(1), 5. DOI: https://doi.org/10.1186/s13673-018-0128-7

Aldosari, B. (2017). Patients’ safety in the era of EMR/EHR automation. Informatics in Medicine Unlocked, 9, 230-233. https://doi.org/10.1016/j.imu.2017.10.001

Alharbi, F., Atkins, A., Stanier, C., & Al-Buti, H. A. (2016). Strategic value of cloud computing in healthcare organizations using the Balanced Scorecard approach: a case study from a Saudi healthcare industry . *Procedia Computer Science*, *98*, 332-339. https://doi.org/10.1016/j.procs.2016.09.050

Allahyari, Z., KHodami, A., Farhadi, A., Hajiyoni, R., AnsariFar, A., & Marzban, M. (2020). Factors Affecting the Satisfaction of Healthcare Workers with the Healthcare System Reform Plan in Healthcare Networks in Bushehr Province in 2018: A Qualitative Study. *ISMJ*, *23*(5), 475-493. http://ismj.bpums.ac.ir/article-1-1353-en.html

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, *7*(1), e06016. doi: https://doi.org/10.1016/j.heliyon.2021.e06016

Arndt, B. G., Beasley, J. W., Watkinson, M. D., Temte, J. L., Tuan, W. J., Sinsky, C. A., & Gilchrist, V. J. (2017). Tethered to the EHR: primary care physician workload assessment using EHR event log data and time-motion observations. *The Annals of Family Medicine*, *15*(5), 419-426. https://doi.org/10.1370/afm.2121

Andreadis, I., & Kartsounidou, E. (2020, April). The impact of splitting a long online questionnaire on data quality. In *Survey Research Methods* (Vol. 14, No. 1, pp. 31-42). https://doi.org/10.18148/srm/2020.v14i1.7294

Angappa, Gunasekaran, Yahaya Y. Yusuf, Ezekiel O. Adeleye & Thanos Papadopoulos (2018) Agile manufacturing practices: the role of big data and business analytics with pragmatic qualitative inquiry studies, *International Journal of Production Research*, *56*:1-2, 385-397, https://doi.org/10.1080/00207543.2017.1395488

Arquilla, J., & Guzdial, M. (2020). Transitioning to distance learning and virtual conferencing. https://doi.org/10.1145/3398386

Aschemann-Witzel, J., De Hooge, I. E., Rohm, H., Normann, A., Bossle, M. B., Grønhøj, A., & Oostindjer, M. (2017). Key characteristics and success factors of supply chain initiatives tackling consumer-related food waste–A pragmatic qualitative inquiry study. *Journal of cleaner production*, *155*, 33-45. https://doi.org/ 10.1016/j.jclepro.2016.11.173

Ash, J., & Simpson, P. (2016). Geography and post-phenomenology. *Progress in Human Geography*, *40*(1), 48-66. https://doi.org/10.1177/0309132514544806

Audrey, S., Brown, L., Campbell, R., Boyd, A., & Macleod, J. (2016). Young people's views about the purpose and composition of research ethics committees: findings from the PEARL qualitative study. *BMC medical ethics, 17*(1), 53 https://doi.org/10.1186/s12910-016-0133-1

Bachiri, M., Idri, A., Fernández-Alemán, J. L., & Toval, A. (2018). Evaluating the privacy policies of mobile personal health records for pregnancy monitoring. *Journal of medical systems*, *42*(8), 144.https://doi.org/10.1007/s10916-018-1002-x

Bahga, A., & Madisetti, V. K. (2015). Healthcare data integration and informatics in the cloud. *Compute, 48*(2):50–57. https://doi.org/ 10.1109/MC.2015.46

Bai, G., Jiang, J. X., & Flasher, R. (2017). Healthcare industry risk of data breaches. *JAMA internal medicine, 177*(6), 878-880. https://doi.org/10.1001/jamainternmed.2017.0336

Bao, S. D., Chen, M., & Yang, G. Z. (2017). A method of signal scrambling to secure data storage for healthcare applications. *IEEE Journal of Biomedical and Health informatics*, *21*(6), 1487-1494. https://doi.org/10.1109/JBHI.2017.2679979

Braun, V., & Clarke, V. (2019). To saturate or not to saturate? Questioning data saturation as a useful concept for thematic analysis and sample-size rationales. *Qualitative Research in Sport, Exercise and Health*, 1-16. https://doi.org/10.1080/2159676X.2019.1704846

Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. computers & security, 68, 145-159.doi: https://doi.org/10.1016/j.cose.2017.04.009

Bender, J. L., Cyr, A. B., Arbuckle, L., & Ferris, L. E. (2017). Ethics and privacy implications of using the internet and social media to recruit participants for health research: A privacy-by-design framework for online recruitment. *Journal of Medical Internet Research*, *19*(4), e104. https://doi.org/10.2196/jmir.7029

Berg, C. (2016). The ‘Rules of engagement’: The ethical dimension of doctoral research. *Journal of Research Initiatives, 2*(2), 7. Retrieved May 22, 2020, from https://digitalcommons.uncfsu.edu/jri/vol2/iss2/7

Bero, L. (2017). Addressing bias and conflict of interest among biomedical researchers. *Jama*, *317*(17), 1723-1724. https://doi.org/10.1001/jama.2017.3854

Berry, L. E. (2016). The research relationship in narrative inquiry. *Nurse researcher, 24*(1). https://doi.org/10.7748/nr.2016.e1430

Bhuyan, S. S., Bailey-DeLeeuw, S., Wyant, D. K., & Chang, C. F. (2016). Too much or too little? How much control should patients have over EHR data?. *Journal of medical systems, 40(*7), 174. https://doi.org/10.1007/s10916-016-0533-2.

Blijleven, V., Koelemeijer, K., Wetzels, M., & Jaspers, M. (2017). Workarounds emerging from electronic health record system usage: Consequences for patient safety, effectiveness of care, and efficiency of care. *JMIR human factors*, *4*(4), e27. https://doi.org/10.2196/humanfactors.7978

Brennan, G. P., Hunter, S. J., Snow, G., & Minick, K. I. (2017). Responsiveness to Change of Functional Limitation Reporting: Cross-sectional Study Using the Intermountain ROMS Scale in Outpatient Rehabilitation. *Physical Therapy*, *97*(12), 1182-1189. https://doi.org/10.1093/ptj/pzx093

Broman, K. W., & Woo, K. H. (2018). Data organization in spreadsheets. *The American Statistician*, *72*(1), 2-10. https://doi.org/10.1080/00031305.2017.1375989

Brothers, K. B., Rivera, S. M., Cadigan, R. J., Sharp, R. R., & Goldenberg, A. J. (2019). A belmont reboot: Building a normative foundation for human research in the 21st century. *The Journal of Law, Medicine & Ethics*, *47*(1), 165-172 https://doi.org/10.1177/1073110519840497

Bryant-Waugh, R., Micali, N., Cooke, L., Lawson, E. A., Eddy, K. T., & Thomas, J. J. (2019). Development of the Pica, ARFID, and Rumination Disorder Interview, a multi-informant, semi-structured interview of feeding disorders across the lifespan: A pilot study for ages 10–22. *International Journal of Eating Disorders*, *52*(4), 378-387. https://doi.org/10.1002/eat.22958

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

Chaki, S. M. H., Din, M. M., & Siraj, M. M. (2019). Integration of SQL Injection Prevention Methods. *International Journal of Innovative* Computing, 9(2).doi:https://doi.org/10.11113/ijic.v9n2.232

Chard, K., Lidman, M., McCollam, B., Bryan, J., Ananthakrishnan, R., Tuecke, S., & Foster, I. (2016). Globus Nexus: A Platform-as-a-Service provider of research identity, profile, and group management. *Future Generation Computer Systems*, 56, 571-583. https://doi.org/10.1016/j.future.2015.09.006

Chatti, D., Archer, M., Lennon, M., & Dove, M. R. (2017). Exploring the mundane: towards an ethnographic approach to bioenergy. *Energy research & social science*, *30*, 28-34. https://doi.org/10.1016/j.erss.2017.06.024

Chaturvedi, R. R., Etchegaray, J. M., Raaen, L., Jackson, J., & Friedberg, M. W. (2019). Technology isn't the half of it: integrating electronic health records and infusion pumps in a large healthcare industry . *The Joint Commission Journal on Quality and Patient Safety*, *45*(10), 649-661. https://doi.org/10.1016/j.jcjq.2019.07.006

Chen, G., Zhao, Y., Zhang, N., Wang, F., & Guo, X. (2015). TTF in workplaces: theoretical framework and empirical analysis in the context of mobile government. *International Journal of Mobile Communications, 13*(5), 455-477. https://doi.org/10.1504/IJMC.2015.070960

Chen, J. Q., & Benusa, A. (2017). HIPAA security compliance challenges: The case for small healthcare providers. *International Journal of Healthcare Management*, *10*(2), 135-146. https://doi.org/10.1080/20479700.2016.1270875

Cheng, X., Fu, S., & de Vreede, G. J. (2017). Understanding trust influencing factors in social media communication: A qualitative study. *International Journal of Information Management*, *37*(2), 25-35. https://doi.org/10.1016/j.ijinfomgt.2016.11.009

Cottrell, E. K., Gold, R., Likumahuwa, S., Angier, H., Huguet, N., Cohen, D. J., & DeVoe, J. E. (2018). Using health information technology to bring social determinants of health into primary care: a conceptual framework to guide research. *Journal of health care for the poor and underserved*, *29*(3), 949-963. https://doi.org/10.1353/hpu.2018.0071

Crowther, S., Ironside, P., Spence, D., & Smythe, L. (2017). Crafting stories in hermeneutic phenomenology research: A methodological device. *Qualitative health research*, *27*(6), 826-835. https://doi.org/10.1177/1049732316656161

Cumyn, A., Ouellet, K., Côté, A. M., Francoeur, C., & St-Onge, C. (2019). Role of researchers in the ethical conduct of research: A discourse analysis from different stakeholder perspectives. *Ethics & Behavior*, *29*(8), 621-636 https://doi.org/10.1080/10508422.2018.1539671

Cutland, C. L., Lackritz, E. M., Mallett-Moore, T., Bardají, A., Chandrasekaran, R., Lahariya, C., & Muñoz, F. M. (2017). Low birth weight: Case definition & guidelines for data collection, analysis, and presentation of maternal immunization safety data. *Vaccine*, *35*(48Part A), 6492. https://doi.org/10.1016/j.vaccine.2017.01.049

Dadzie, J., Runeson, G., Ding, G., & Bondinuba, F. K. (2018). Barriers to adoption of sustainable technologies for energy-efficient building upgrade—semi-Structured interviews. *Buildings*, *8*(4), 57. https://doi.org/10.3390/buildings8040057

Dang, Y. M., Zhang, Y. G., Brown, S. A., & Chen, H. (2018). Examining the impacts of mental workload and TTF on user acceptance of the social media search system. *Information Systems Frontiers*, 1-22. https://doi.org/10.1007/s10796-018-9879-y

Das, M. S., Govardhan, A., & Doddapaneni, V. L. (2021). A Model of Cloud Forensic Application With Assurance of Cloud Log. *International Journal of Digital*

Crime and Forensics (IJDCF), 13(5), 114-129. doi: 10.4018/IJDCF.20210901.oa7

Day, F. C., Pourhomayoun, M., Keeves, D., Lees, A. F., Sarrafzadeh, M., Bell, D., & Pfeffer, M. A. (2019). Feasibility study of an EHR-integrated mobile shared decision making application. *International journal of medical informatics, 124*, 24-30. https://doi.org/10.1016/j.ijmedinf.2019.01.008

Degenholtz, H. B., Resnick, A., Lin, M., & Handler, S. (2016). Development of an applied framework for understanding health information technology in nursing homes. *Journal of the American Medical Directors Association*, 17(5), 434-440. https://doi.org/10.1016/j.jamda.2016.02.002

Edwards, B., Hofmeyr, S., & Forrest, S. (2016). Hype and heavy tails: A closer look at data breaches. *Journal of Cybersecurity*, *2*(1), 3-14. https://doi.org/10.1093/cybsec/tyw003

Evans, S. K., Pearce, K. E., Vitak, J., & Treem, J. W. (2017). Explicating affordances: Conceptual framework for understanding affordances in communication research. *Journal of Computer-Mediated Communication, 22*(1), 35-52. https://doi.org/10.1111/jcc4.12180

Erskine, M. A., Khojah, M., & McDaniel, A. E. (2019). Location selection using heat maps: Relative advantage, TTF, and decision-making performance. *Computers in Human Behavior*, *101*, 151-162. https://doi.org/10.1016/j.chb.2019.07.014

Eyisi, D. (2016). The Usefulness of Qualitative and Quantitative Approaches and Methods in Researching Problem-Solving Ability in Science Education

Curriculum. *Journal of Education and Practice*, *7*(15), 91-100. Retrieved June 25, 2020, from https://eric.ed.gov/?id=EJ1103224

Farhadi, M., Haddad, H., & Shahriar, H. (2018). Static Analysis of HIPPA Security Requirements in Electronic Health Record Applications. In *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)* (Vol. 2, pp. 474-479). IEEE. https://doi.org/10.1109/COMPSAC.2018.10279.

Farley, R. (2020). The Importance of Census 2020 and the Challenges of Getting a Complete Count. *Harvard Data Science Review*, *2*(1). https://doi.org/10.1162/99608f92.8a0cc85c

Faulkner, S. L., & Trotter, S. P. (2017). Data saturation. *The international encyclopedia of communication research methods*, 1-2. https://doi.org/10.1002/9781118901731.iecrm0060

Feinbube, L., Pirl, L., Troger, P., & Polze, A. (2017, December). Dependability stress testing of cloud infrastructures. In *2017 18th international conference on parallel and distributed computing, applications and technologies (PDCAT)* (pp. 453-460). IEEE. https://doi.org/10.1109/PDCAT.2017.00078

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

Fusch, P., Fusch, G. E., & Ness, L. R. (2018). Denzin's paradigm shift: Revisiting triangulation in qualitative research. *Journal of Social Change*, *10*(1), 2. https://doi.org/10.5590/JOSC.2018.10.1.02

Garg, S. K., Lyles, C. R., Ackerman, S., Handley, M. A., Schillinger, D., Gourley, G., & Sarkar, U. (2015). Qualitative analysis of programmatic initiatives to text patients with mobile devices in resource-limited health systems. *BMC medical informatics and decision making, 16*(1), 16. https://doi.org/10.1186/s12911-016-0258-7

Garthwaite, K. (2016). Stigma, shame, and people like us': an ethnographic study of foodbank use in the UK. *Journal of Poverty and Social Justice, 24*(3), 277-289. https://doi.org/10.1332/175982716X14721954314922

Gebauer, J., Shaw, M. J., & Gribbins, M. L. (2005). *TTF for mobile information systems* (No. 05-0119). https://doi.org/ 10.1057/jit.2010.10

Gentles, S. J., Charles, C., Ploeg, J., & McKibbon, K. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *The Qualitative Report*, *20*(11), 1772-1789. Retrieved June 25,2019, from https://nsuworks.nova.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=2373&context=tqr/

Gong, N., Zhou, Y., Cheng, Y., Chen, X., Li, X., Wang, X., & Zhang, M. (2018). Practice of informed consent in Guangdong, China: a qualitative study from the perspective of in-healthcare industry patients. *BMJ open*, *8*(10), e020658. http://dx.doi.org/10.1136/bmjopen-2017-020658

Goodhue, D. L., & Thompson, R. L. (1995). TTF and individual performance. *MIS quarterly,* 213-236. https://doi.org/10.2307/249689

Goodhue, D. L. 1998. "Development and Measurement Validity of a Task–Technology Fit Instrument for User Evaluations of Information Systems," *Decision Sciences (29:1),* pp. 105-138. https://doi.org/10.1111/j.1540-5915.1998.tb01346.x

Hamidi, H. (2019). An approach to develop the smart health using Internet of Things and authentication based on biometric technology. Future generation computer systems, 91, 434-449.doi: https://doi.org/10.1016/j.future.2018.09.024

Hass, R. W., Rivera, M., & Silvia, P. J. (2018). On the dependability and feasibility of layperson ratings of divergent thinking. *Frontiers in Psychology*, *9*, 1343. https://doi.org/10.3389/fpsyg.2018.01343

He, Y., Camacho, R. S., Soygazi, H., & Luo, C. (2021). Attacking and defence pathways for Intelligent Medical Diagnosis System (IMDS). International Journal of Medical Informatics, 148, 104415.doi: https://doi.org/10.1016/j.ijmedinf.2021.104415

Howell, E. A., Brown, H., Brumley, J., Bryant, A. S., Caughey, A. B., Cornell, A. M., & Mhyre, J. M. (2018). Reduction of peripartum racial and ethnic disparities: a conceptual framework and maternal safety consensus bundle. *Journal of Obstetric, Gynecologic & Neonatal Nursing, 47*(3), 275-289. https://doi.org/ 10.1016/j.jogn.2018.03.004

Huang, Q., Yue, W., He, Y., & Yang, Y. (2018). Secure identity-based data sharing and profile matching for mobile healthcare social networks in cloud computing. *IEEE Access*, *6*, 36584-36594. https://doi.org/10.1109/ACCESS.2018.2852784.

Hussain, M., Zaidan, A. A., Zidan, B. B., Iqbal, S., Ahmed, M. M., Albahri, O. S., & Albahri, A. S. (2018). The conceptual framework for the security of mobile health applications on the android platform. Telematics and Informatics, 35(5), 1335-1354. https://doi.org/10.1016/j.tele.2018.03.005

Hunter, D., McCallum, J., & Howes, D. (2019). Defining Exploratory-Descriptive Qualitative (EDQ) research and considering its application to healthcare. *Journal of Nursing and Health Care*. http://eprints.gla.ac.uk/180272/

Ido, K., Nakamura, N., & Nakayama, M. (2019). Miyagi Medical and Welfare Information Network: a backup system for patient clinical information after the Great East Japan Earthquake and tsunami. *The Tohoku journal of experimental medicine*, *248*(1), 19-25. https://doi.org/10.1620/tjem.248.19

Jacquelynn, P.(2018). Literacy Research: theory, method, and practice. *Sage Publications, Inc*. Retrieved May 22,2019, from http://journals.sagepub.com.ezp.waldenulibrary.org/home/lrx

Jayabalan, M., & O’Daniel, T. (2019). A Study on Authentication Factors in Electronic Health Records. *Journal of Applied Technology and Innovation (e-ISSN: 2600-7304)*, *3*(1). Retrieved May 25, 2019, from https://jati.sites.apiit.edu.my/files/2019/05/A-Study-on-Authentication-Factors-in-Electronic-Health-Records.pdf

Jofre, M., Navarro-Llobet, D., Agulló, R., Puig, J., Gonzalez-Granadillo, G., Mora Zamorano, J., & Romeu, R. (2021). Cybersecurity and Privacy Risk Assessment of Point-of-Care Systems in Healthcare—A Use Case Approach. *Applied Sciences*, *11*(15), 6699.doi: https://doi.org/10.3390/app11156699

John, G. (2015). Design Science: an international journal. *Cambridge University Press*. Retrieved June 20, 2019, from http://journals.cambridge.org.ezp.waldenulibrary.org/action/displayJournal?jid=DSJ

Kamerer, J. L., & McDermott, D. (2020). Cybersecurity: Nurses on the front line of prevention and education. *Journal of Nursing Regulation*, *10*(4), 48-53.doi: https://doi.org/10.1016/S2155-8256(20)30014-4

Khan, J., Li, J. P., Ahamad, B., Parveen, S., Haq, A. U., Khan, G. A., & Sangaiah, A. K. (2020). SMSH: secure surveillance mechanism on smart healthcare IoT system with probabilistic image encryption. IEEE Access, 8, 15747-15767. doi: 10.1109/ACCESS.2020.2966656

Kahn, M. G., Callahan, T. J., Barnard, J., Bauck, A. E., Brown, J., Davidson, B. N., & Liaw, S. T. (2016). A harmonized data quality assessment terminology and framework for the secondary use of electronic health record data. *Egems, 4*(1). https://doi.org/10.13063/2327-9214.1244

Kallio, H., Pietilä, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of advanced nursing*, *72*(12), 2954-2965. https://doi.org/10.1111/jan.13031

Khan, S. I., & Latiful-Hoque, A. S. M. (2016). Digital health data: A comprehensive review of privacy and security risks and some recommendations. *Computer Science Journal of Moldova*, *24*(2). Retrieved August 10, 2019, from http://www.math.md/files/csjm/v24-n2/v24-n2-(pp273-292).pdf

Khorram Niaki, M., & Nonino, F. (2017). Impact of additive manufacturing on business competitiveness: a pragmatic qualitative inquiry study. *Journal of Manufacturing Technology Management*, *28*(1), 56-74. https://doi.org/10.1108/JMTM-01-2016-0001

Kissam, E., Quezada, C., & Intili, J. A. (2018). Community-based canvassing to improve the US Census Bureau's Master Address File: California's experience in LUCA 2018. *Statistical Journal of the IAOS*, *34*(4), 605-619. https://doi.org/10.3233/SJI-180480

Klappe, E. S., de Keizer, N. F., & Cornet, R. (2020). Factors influencing problem list use in electronic health records—application of the unified theory of acceptance and use of technology. *Applied Clinical Informatics*, *11*(03), 415-426.doi:10.1055/s-0040-1712466

Koczkodaj, W. W., Mazurek, M., Strzałka, D., Wolny-Dominiak, A., & Woodbury-Smith, M. (2019). Electronic health record breaches as social indicators. *Social Indicators Research*, *141*(2), 861-871. https://doi.org/10.1007/s11205-018-1837-z

Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for electronic health records. *Journal of medical systems, 41*(8), 127. https://doi.org/10.1007/s10916-017-0778-4

Lai, P. C. (2017). The literature review of technology adoption models and theories for the novelty technology. *Journal of Information Systems and Technology Management*, *14*(1), 21-38. https://doi.org/10.4301/s1807-17752017000100002

Lanford, D., & Quadagno, J. (2016). Implementing ObamaCare: The politics of medicaid expansion under the affordable care act of 2010. Sociological Perspectives, 59(3), 619-639. https://doi.org/10.1177/0731121415587605

Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017, October). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In *2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC)* (pp. 1-5). IEEE. doi: 10.1109/PIMRC.2017.8292361

Leppänen, A., Toiviainen, T., & Kankaanranta, T. (2020). From a Vulnerability Search to a Criminal Case: Script Analysis of an SQL Injection Attack. *International Journal of Cyber Criminology, 14*(1), 63-80. Retrieved from https://www.proquest.com/openview/b35f1c597bb87456904124a58b7ce5dd/1?pq-origsite=gscholar&cbl=55114

Lim, J. S., & Greenwood, C. A. (2017). Communicating corporate social responsibility (CSR): Stakeholder responsiveness and engagement strategy to achieve CSR goals. *Public Relations Review*, *43*(4), 768-776. https://doi.org/10.1016/j.pubrev.2017.06.007

Lopez, D., & Sekaran, G. (2016). Climate change and disease dynamics-a big data perspective. International Journal of Infectious Diseases, 45, 23-24. https://doi.org/10.1016/j.ijid.2016.02.08

Loss, J., Brew-Sam, N., Metz, B., Strobl, H., Sauter, A., & Tittlbach, S. (2020). Capacity Building in Community Stakeholder Groups for Increasing Physical Activity: Results of a Qualitative Study in Two German Communities. *International Journal of Environmental Research and Public Health*, *17*(7), 2306. https://doi.org/10.3390/ijerph17072306

Ludo, W. (2019). Quantitative Science Studies. *M I T Press.* Retrieved March 30, 2020, from https://www.mitpressjournals.org/loi/qss

Madill, A., & Sullivan, P. (2018). Mirrors, portraits, and member-checking : Managing difficult moments of knowledge exchange in the social sciences. *Qualitative Psychology*, *5*(3), 321. https://doi.org/https://doi.org/10.1037/qup0000089

Mahabir, R., Stefanidis, A., Croitoru, A., Crooks, A. T., & Agouris, P. (2017). Authoritative and volunteered geographical information in a developing country: A comparative case study of road datasets in Nairobi, Kenya. *ISPRS International Journal of Geo-Information*, *6*(1), 24. https://doi.org/10.3390/ijgi6010024

Maher, C., Hadfield, M., Hutchings, M., & de Eyto, A. (2018). Ensuring rigor in qualitative data analysis: A design research approach to coding combining NVivo with traditional material methods. *International Journal of Qualitative Methods, 17*(1), 1609406918786362. https://doi.org/10.1177/1609406918786362

Malley, A. S., Draper, K., Gourevitch, R., Cross, D. A., & Scholle, S. H. (2015). Electronic health records and support for primary care teamwork. *Journal of the American Medical Informatics Association, 22*(2), 426-434. https://doi.org/10.1093/jamia/ocu029

Manogaran, G., Thota, C., Lopez, D., & Sundarasekar, R. (2017). Big data security intelligence for healthcare industry 4.0. In Cybersecurity for Industry 4.0 (pp. 103-126). *Springer, Cham*. https://doi.org/10.1007/978-3-319-50660-9_5

Maraj, A., Rogova, E., & Jakupi, G. (2020). Testing of network security systems through DoS, SQL injection, reverse TCP and social engineering attacks. *International Journal of Grid and Utility Computing, 11*(1), 115-133.doi: https://doi.org/10.1504/IJGUC.2020.103976

McDonald, N., Schoenebeck, S., & Forte, A. (2019). Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on Human-Computer Interaction*, *3*(CSCW), 1-23.https://doi.org/10.1145/3359174

McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, *108*, 57-68. https://doi.org/10.1016/j.dss.2018.02.007

McGlade, D., & Scott-Hayward, S. (2019). ML-based cyber incident detection for Electronic Medical Record (EMR) systems. *Smart Health*, *12*, 3-23.doi: https://doi.org/10.1016/j.smhl.2018.05.001

Mehraeen, E., Ayatollahi, H., & Ahmadi, M. (2016). Health information security in healthcare industry : The application of security safeguards. *Acta Informatica Medica*, *24*(1), 47. https://doi.org/10.5455/aim.2016.24.47-50

Miko, J. (2017). *Collaboration Strategies to Reduce Technical Debt*. Available from ProQuest Dissertations and Thesis Databases (ProQuest No. 10635282)

Morgan, D. L., & Nica, A. (2020). Iterative Thematic Inquiry: A New Method for Analyzing Qualitative Data. *International Journal of Qualitative Methods*, *19*, 1609406920955118. https://doi.org/10.1177/1609406920955118

Mori, S., Wu, D., Ceritoglu, C., Li, Y., Kolasny, A., Vaillant, M. A., & Miller, M. I. (2016). MRICloud: delivering high-throughput MRI neuroinformatics as cloud-based Software as a service. *Computing in Science & Engineering*, 18(5), 21-35. https://doi.org/10.1109/MCSE.2016.93

Morris, R. G. (2018). Information Technology Manager Characteristics andInformation Security Breaches in Publicly Traded Companies: *A Correlational Study Using Secondary Data (Doctoral dissertation, Capella University*). Proquest number: 10846636

Moosavi, S. R., Gia, T. N., Nigussie, E., Rahmani, A. M., Virtanen, S., Tenhunen, H., & Isoaho, J. (2016). End-to-end security scheme for mobility enabled healthcare Internet of Things. *Future Generation Computer Systems*, *64*, 108-124. https://doi.org/ 10.2147/DDDT.S96936

Muzammal, S. M., Shah, M. A., Khattak, H. A., Jabbar, S., Ahmed, G., Khalid, S., & Han, K. (2018). Counter measuring conceivable security threats on smart healthcare devices. *IEEE Access, 6*, 20722-20733. https://doi.org/10.1109/ACCESS.2018.2826225.

Naderifar, M., Goli, H., & Ghaljaie, F. (2017). Snowball sampling: A purposeful method of sampling in qualitative research. *Strides in Development of Medical Education*, *14*(3), 1-6. https://doi.org/10.5812/sdme.67670.

Nagasubramanian, G., Sakthivel, R. K., Patan, R., Gandomi, A. H., Sankayya, M., & Balusamy, B. (2020). Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. *Neural Computing and Applications*, *32*(3), 639-647. https://doi.org/10.1007/s00521-018-3915-1

Naidu, T., & Prose, N. (2018, September). Re-envisioning member-checking and communicating results as accountability practice in qualitative research: A South African community-based organization example. In *Forum Qualitative*

Sozialforschung/Forum: Qualitative Social Research (Vol. 19, No. 3).http://dx.doi.org/10.17169/fqs-19.3.3153

Neville, S., Adams, J., & Cook, C. (2016). Using internet-based approaches to collect qualitative data from vulnerable groups: reflections from the field. *Contemporary Nurse, 52*(6), 657-668. https://doi.org/10.1080/10376178.2015.1095056

Niedbalski, J., & Ślęzak, I. (2017). Computer assisted qualitative data analysis software. Using the NVivo and Atlas. ti in the research projects based on the methodology of grounded theory. In *Computer supported qualitative research* (pp. 85-94). Springer, Cham. https://doi.org/10.1007/978-3-319-43271-7_8

Olteanu, A., Castillo, C., Diaz, F., & Kiciman, E. (2019). Social data: Biases, methodological pitfalls, and ethical boundaries. *Frontiers in Big Data*, *2*, 13. https://doi.org/10.3389/fdata.2019.00013

Onuma, Y., Takai, T., Koshiyama, T., & Matsuno, Y. (2018). D-case steps: New steps for writing assurance cases. In *International Conference on Computer Safety, Reliability, and Security* (pp. 71-78). Springer, Cham. https://doi.org/10.1007/978-3-319-99229-7_8

Palinkas, L.A., Horwitz, S.M., & Green, C.A.. Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. *Adm Policy Ment Health* **42,** 533–544 (2015). https://doi.org/10.1007/s10488-013-0528-y

Patil, A., Laturkar, A., Athawale, S. V., Takale, R., & Tathawade, P. (2017, August). A multilevel system to mitigate DDOS, brute force and SQL injection attack for cloud security. In 2017 International Conference on Information, Communication, Instrumentation and Control (ICICIC) (pp. 1-7). IEEE. doi: 10.1109/ICOMICON.2017.8279028

Papoutsi, C., Reed, J. E., Marston, C., Lewis, R., Majeed, A., & Bell, D. (2015). Patient and public views about the security and privacy of Electronic Health Records (EHRs) in the UK: Results from a mixed-methods study. *BMC Medical Informatics and Decision Making, 15*(1), 86. https://doi.org/10.1186/s12911-015-0202-2.

Perrotta, C. (2017). Beyond rational choice: How teacher engagement with technology is mediated by culture and emotions. *Education and Information Technologies*, *22*(3), 789-804.https://doi.org/10.1007/s10639-015-9457-6

Pratt, J. M., & Yezierski, E. J. (2018). A novel qualitative method to improve access, elicitation, and sample diversification for enhanced transferability applied to studying chemistry outreach. *Chemistry Education Research and Practice, 19*(2), 410-430. https://doi.org/10.1039/C7RP00200A

Queirós, A., Faria, D., & Almeida, F. (2017). Strengths and limitations of qualitative and quantitative research methods. *European Journal of Education Studies*. https://doi.org/10.5281/zenodo.887089

Råheim, M., Magnussen, L. H., Sekse, R. J. T., Lunde, Å., Jacobsen, T., & Blystad, A. (2016). Researcher–researched relationship in qualitative research: Shifts in positions and researcher vulnerability. *International journal of qualitative studies on health and well-being,* 11(1)*,* 30996. https://doi.org/10.3402/qhw.v11.30996

Ramani, V., Kumar, T., Bracken, A., Liyanage, M., & Ylianttila, M. (2018, December). Secure and efficient data accessibility in blockchain based healthcare systems. In *2018 IEEE Global Communications Conference (GLOBECOM)* (pp. 206-212). IEEE. https://doi.org/10.1109/GLOCOM.2018.8647221.

Rasmi, M., Alazzam, M. B., Alsmadi, M. K., Almarashdeh, I. A., Alkhasawneh, R. A., & Alsmadi, S. (2018). Healthcare professionals' acceptance Electronic Health Records system: Critical literature review (Jordan case study*). International Journal of Healthcare Management*, 1-13. https://doi.org/10.1080/20479700.2017.1420609

Rathert, C., Mittler, J. N., Banerjee, S., & McDaniel, J. (2017). Patient-centered communication in the era of electronic health records: what does the evidence say?. *Patient education and counseling, 100(*1), 50-64. https://doi.org/10.1016/j.pec.2016.07.031

Ratna, S., Astuti, E. S., Utami, H. N., Rahardjo, K., & Arifin, Z. (2018). Characteristics of tasks and technology as a driver of TTF and the use of the hotel reservation information system. *VINE Journal of Information and Knowledge Management Systems*. https://doi.org/10.1177/1467358420907176

Ratwani, R. M., Zachary Hettinger, A., Kosydar, A., Fairbanks, R. J., & Hodgkins, M. L. (2016). A framework for evaluating electronic health record vendor user-centered design and usability testing processes. *American Medical Informatics Association- Journal, 24*(e1), e35-e39. https://doi.org/10.1093/jamia/ocw092

Rawal, B. S., Vijayakumar, V., Manogaran, G., Varatharajan, R., & Chilamkurti, N. (2018). Secure disintegration protocol for privacy preserving cloud storage. *Wireless personal communications*, *103*(2), 1161-1177.doi: https://doi.org/10.1007/s11277-018-5284-6

Robins, C. S., & Eisen, K. (2017). Strategies for the effective use of NVivo in a large-scale study: Qualitative analysis and the repeal of Don’t Ask, Don’t Tell. Qualitative Inquiry, 23(10), 768-778.doi: https://doi.org/10.1177/1077800417731089

Rose, J., & Johnson, C. W. (2020). Contextualizing reliability and validity in qualitative research: toward more rigorous and trustworthy qualitative social science in leisure research. *Journal of Leisure Research*, 1-20. https://doi.org/10.1080/00222216.2020.1722042

Salehi, A. S., Rudolph, C., & Grobler, M. (2019, April). A dynamic cross-domain access control model for collaborative healthcare application. In 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM) (pp. 643-648). IEEE. Retrieved from https://ieeexplore.ieee.org/abstract/document/8717924/citations#citations

Salleh, M. I. M., Zakaria, N., & Abdullah, R. (2016). The influence of system quality characteristics on health care providers’ performance: Empirical evidence from Malaysia. *Journal of infection and public health, 9(*6), 698-707. https://doi.org/10.1016/j.jiph.2016.09.002

Samkari, H., & Gutub, A. (2019). Protecting medical records against cybercrimes within Hajj period by 3-layer security. *Recent Trends Inf Technol Appl*, *2*(3), 1-21. DOI: http://doi.org/10.5281/zenodo.3543455

Santana, M. J., Manalili, K., Jolley, R. J., Zelinsky, S., Quan, H., & Lu, M. (2018). Practice person-centered care with a conceptual framework. *Health Expectations*, *21*(2), 429-440. https://doi.org/10.1111/hex.12640

Sebetci, Ö. (2018). Enhancing end-user satisfaction through technology compatibility: An assessment on health information system. *Health Policy and Technology*, *7*(3), 265-274.doi: https://doi.org/10.1016/j.hlpt.2018.06.001

Sgora, A., Vergados, D. D., & Chatzimisios, P. (2016). A survey on security and privacy issues in wireless mesh networks. *Security and Communication Networks*, *9*(13), 1877-1889. https://doi.org/10.1002/sec.846

Shaharudin, M. R., Govindan, K., Zailani, S., Tan, K. C., & Iranmanesh, M. (2017). Product return management: Linking product returns, closed-loop supply chain activities and the effectiveness of the reverse supply chains. *Journal of Cleaner Production*, *149*, 1144-1156. https://doi.org/10.1016/j.jclepro.2017.02.133

Shankman, S. A., Funkhouser, C. J., Klein, D. N., Davila, J., Lerner, D., & Hee, D. (2018). Reliability and validity of severity dimensions of psychopathology assessed using the Structured Clinical Interview for DSM-5 (SCID). *International journal of methods in psychiatric research*, *27*(1), e1590.. https://doi.org/10.1002/mpr.1590

Simpao, A. F., Ahumada, L. M., Martinez, B. L., Cardenas, A. M., Metjian, T. A., Sullivan, K. V., & Gerber, J. S. (2018). Design and implementation of a visual analytics electronic antibiogram within an electronic health record system at a tertiary pediatric healthcare industry . *Applied clinical informatics*, *9*(1), 37. https://doi.org/10.1055/s-0037-1615787

Singh, S. K. (2017). Conceptual framework of a cloud-based decision support system for arsenic health risk assessment. *Environment Systems and Decisions, 37*(4), 435-450. https://doi.org/10.1007/s10669-017-9641-x

Smith, J. (2015). Health Data Breaches Compromised 29 Million Patient Records in 2010–2013. *Caring for the Ages*, *16*(6), 6. http://dx.doi.org/10.1016/j.carage.2015.05.008

Spacey, A., Harvey, O., & Casey, C. (2020). Postgraduate researchers' experiences of accessing participants via gatekeepers:'wading through treacle!'. *Journal of Further and Higher Education*, 1-18. https://doi.org/10.1080/0309877X.2020.1774051

Steven, D. (2015). Phenomenological Reviews. *sdvig press*. Retrieved February 17, 2018, from http://reviews.ophen.org/2019/07/17/steven-delay-phenomenology-in-france/

Surmiak, A. D. (2018, September). Confidentiality in qualitative research involving vulnerable participants: Researchers' perspectives. In *Forum Qualitative*

Sozialforschung/Forum: Qualitative Social Research (Vol. 19, No. 3). http://dx.doi.org/10.17169/fqs-19.3.3099

Theofanidis, D., & Fountouki, A. (2018). 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

Thompson, E. C. (2018). Eradication, Recovery, and Post-incident Review. In *Cybersecurity Incident Response* (pp. 117-123). Apress, Berkeley, CA. **DOI :** https://doi.org/10.1007/978-1-4842-3870-7_9

Thota, C., Sundarasekar, R., Manogaran, G., Varatharajan, R., & Priyan, M. K. (2018). Centralized fog computing security platform for IoT and cloud in the healthcare system. In *Fog Computing: Breakthroughs in Research and Practice* (pp. 365-378). IGI global. https://doi.org/10.4018/978-1-5225-5649-7.ch018

Tiwari, V. (2021). DPLOOP: Detection and Prevention of Loopholes in Web Application Security. In *Advances in Computational Intelligence and Communication Technology* (pp. 161-172). Springer, Singapore. doi: https://doi.org/10.1007/978-981-15-1275-9_14

Tolich, M. (2019, October). What Qualitative Researchers Must Do When Ethical Assurances Disintegrate? Recognise Internal Confidentiality, Establish Process Consent, Reference Groups, Referrals for Participants and a Safety Plan. *In World*

Conference on Qualitative Research (pp. 22-32). Springer, Cham. https://doi.org/10.1007/978-3-030-31787-4_2

Tutty, M. A., Carlasare, L. E., Lloyd, S., & Sinsky, C. A. (2019). The complex case of EHRs: examining the factors impacting the EHR user experience. *Journal of the American Medical Informatics Association, 26*(7), 673-677. https://doi.org/10.1093/jamia/ocz021

US Department of Health & Human Services. (2019). Tennessee diagnostic medical imaging services company pays $3,000,000 to settle breach exposing over 300,000 patients' protected health information. Retrieved December 10, 2019, from https://www.hhs.gov/about/news/2019/05/06/tennessee-diagnostic-medical-imaging-services-company-pays-3000000-settle-breach.html

Van de Weerd, I., Mangula, I. S., & Brinkkemper, S. (2016). Adoption of Software as a service in Indonesia: Examining the influence of organizational factors. *Information & Management, 53*(7), 915-928. https://doi.org/10.1016/j.im.2016.05.008

Vizarreta, P., Trivedi, K., Mendiratta, V., Kellerer, W., & Mas-Machuca, C. (2020). DASON: Dependability Assessment Framework for Imperfect Distributed SDN Implementations. *IEEE Transactions on Network and Service Management*, *17*(2), 652-667.https://doi.org/10.1145/3018896.3036364

VonBastian, Claudia. C., & Eschen, A. (2016). Does working memory training have to be adaptive?. *Psychological research*, *80*(2), 181-194.https://doi.org/10.1007/s00426-015-0655-z

Verba, N., Chao, K. M., James, A., Goldsmith, D., Fei, X., & Stan, S. D. (2017). Platform as a service gateway for the Fog of Things. *Advanced Engineering Informatics, 33*, 243-257. https://doi.org/10.1016/j.aei.2016.11.003

Waibel, S., Vargas, I., Aller, M. B., Gusmão, R., Henao, D., & Vázquez, M. L. (2015). The performance of integrated health care networks in the continuity of care: a qualitative pragmatic qualitative inquirystudy of COPD patients. *International journal of integrated care*, *15*(3). https://doi.org/10.5334/ijic.1527

Walumbwa, F. O., Hartnell, C. A., & Misati, E. (2017). Does ethical leadership enhance group learning behavior? Examining the mediating influence of group ethical conduct, justice climate, and peer justice. *Journal of Business Research*, *72*, 14-23. https://doi.org/10.1016/j.jbusres.2016.11.013

Wang, J., Ding, Y., Xiong, N. N., Yeh, W. C., & Wang, J. (2020). GSCS: General Secure Consensus Scheme for Decentralized Blockchain Systems. *IEEE Access*, *8*, 125826-125848. https://doi.org/10.1109/ACCESS.2020.3007938.

Wang, S. L., & Lin, H. I. (2019). Integrating TTF and IDT to evaluate user intention of big data analytics in mobile cloud healthcare system. *Behaviour & Information Technology*, *38*(9), 974-985. https://doi.org/10.1080/0144929X.2019.1626486

Wang, H., Tao, D., Yu, N., & Qu, X. (2020). Understanding consumer acceptance of healthcare wearable devices: An integrated model of UTAUT and TTF. *International Journal of Medical Informatics*, 104156. https://doi.org/10.1016/j.ijmedinf.2020.104156

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

Williams, W. (2018). *Video Game Development Strategies for Creating Successful Cognitively Challenging.* Available from ProQuest Dissertations and Thesis Databases (ProQuest No. 10743115)

Wilkes, L. M., Luck, L., & Ng Chok, H. (2017). Participant recruitment: tips and tricks. *International Journal of Qualitative Methods,* 46-46. https://doi.org/10.1177/1609406916688525

Wong, W. E., Li, X., & Laplante, P. A. (2017). Be more familiar with our enemies and pave the way forward: A review of the roles bugs played in software failures. *Journal of Systems and Software*, *133,* 68-94.doi: https://doi.org/10.1016/j.jss.2017.06.069

Wu, B., & Chen, X. (2017). Continuance intention to use MOOCs: Integrating the technology acceptance model (TAM) and task technology fit (TTF) model. *Computers in Human Behavior, 67,* 221-232. https://doi.org/10.1016/j.chb.2016.10.028

Yeboah-Ofori, A., Abdulai, J., & Katsriku, F. (2019). Cybercrime and Risks for Cyber Physical Systems. *International Journal of Cyber-Security and Digital Forensics (IJCSDF), 8*(1), 43-57.doi: https://doi.org/10.17781/P002556

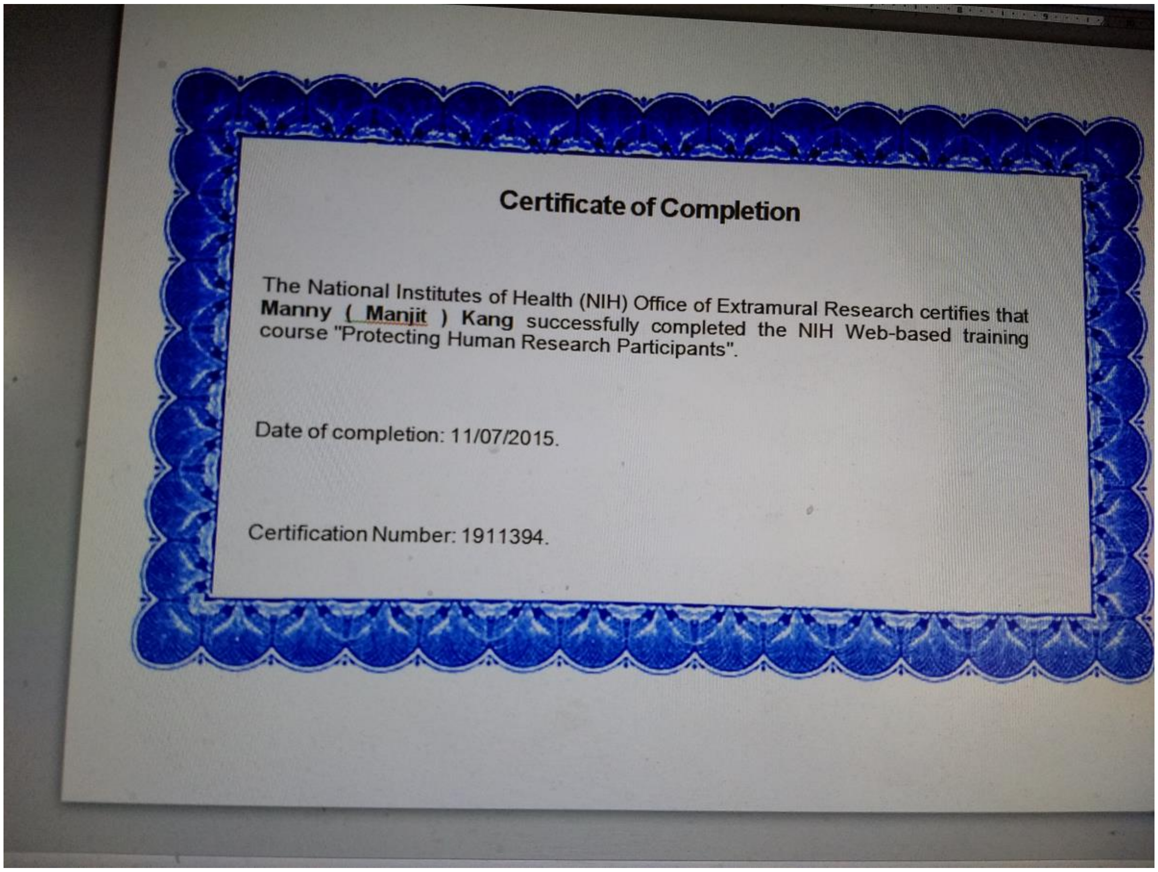
Yin, R. K. (2017). *Case study research and applications: Design and methods*. Sage publications.

Zigurs, I., & Buckland, B. K. (1998). A theory of task/technology fit and group support systems effectiveness. *MIS Quarterly*, *22*(3). 313-334. https://doi.org/10.2307/249668

Zuchowski, O., Posegga, O., Schlagwein, D., & Fischbach, K. (2016). Internal crowdsourcing: conceptual framework, structured review, and research agenda. *Journal of Information Technology, 31*(2), 166-184. https://doi.org/10.1057/jit.2016.1

Zulfiqar, M., Syed, F., Khan, M. J., & Khurshid, K. (2019, July). Deep face recognition for biometric authentication. In 2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE) (pp. 1-6). IEEE. doi 10.1109/ICECCE47252.2019.8940725

Appendix A: National Institute of Health (NIH) Human Subject Research Certificate of Completion



Certificate of Completion

The National Institutes of Health (NIH) Office of Extramural Research certifies that **Manny (Manjit) Kang** successfully completed the NIH Web-based training course "Protecting Human Research Participants".

Date of completion: 11/07/2015.

Certification Number: 1911394.

Appendix B: Interview Questions for Participants

The Major interview Questions:

Note: The research participants for this interview will be IT security managers, who are responsible for the healthcare industry's private cloud-based CIS or EHRs systems

- What procedure have you used in the past to eliminate non-public cloud-based CIS or EHRs system data breaches?
- What, if any, general complaints from patients are related to the management or use of the CIS or EHRs data system?
- What type of private cloud-based CIS or EHRs system application training did you provide to staff or users in the past?
- Are you comfortable supporting a private cloud-based CIS or EHRs system? If not, what are your concerns?
- What are security risks you have seen related to a protected cloud-based CIS or EHRs system used in your healthcare industry?
- Have you discovered security loopholes in your healthcare industry network? If so, how were they remedied?
- Do you have a budget to implement new security procedures? If so, it adequate. If not, what should be done about it?

- Does your healthcare industry have IT security staff members who have the knowledge to implement new security procedures? How does this impact your ability to keep the system safe?

- Would more funding security tools help your organization prevent data breaches, or other measures are needed to minimize breaches? Why or why not?

Appendix C: Interview Protocol

Part 1	**Script**
Introduction and interview stage setup	Hello, my name is Manny Kang; I am currently a student at Walden University pursuing a doctoral degree in Information Technology (DIT). I thank you for participating in my study , which is to explore strategies of the healthcare industry information technology (IT) leaders to implement secure procedures to protect patient health records on the private cloud-based CIS systems. The interview will be a half hour in length and then a 30-minute follow-up session. The interview with the participants will be face to face in a video conference meeting by using Zoom or other internet tools available and allowed by the healthcare industry. Once I complete the interview meeting with participant, I will email them copy of the Zoom transcript. The interview questions will be open ended qualitative, so there is no correct or wrong answer. You can ask me any question related with informed consent form, before we start our interview meeting. If not, let us get started with our first interview question.
Part 2	**Interview Questions**
	• What procedure have you used in the past to eliminate

	non-public cloud-based CIS or EHRs system data breaches? • What, if any, general complaints from patients are related to the management or use of the CIS or EHRs data system? • What type of private cloud-based CIS or EHRs system application training did you provide to staff or users in the past? • Are you comfortable supporting a private cloud-based CIS or EHRs system? If not, what are your concerns? • What are security risks you have seen related to a protected cloud-based CIS or EHRs system used in your healthcare industry? • Have you discovered security loopholes in your healthcare industry network? If so, how were they remedied? • Do you have a budget to implement new security procedures? If so, it adequate. If not, what should be done about it?

	• Does your healthcare industry have IT security staff members who have the knowledge to implement new security procedures? How does this impact your ability to keep the system safe? • Would more funding security tools help your organization prevent data breaches, or other measures are needed to minimize breaches? Why or why not?