2022

Security Strategies of Electronic Health Record Systems

Benjamin Gerke
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Benjamin Gerke

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

Review Committee
Dr. Charlie Shao, Committee Chairperson, Information Technology Faculty
Dr. Cheryl Waters, Committee Member, Information Technology Faculty
Dr. Jon McKeeby, University Reviewer, Information Technology Faculty

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

Walden University
2022

Abstract

Security Strategies of Electronic Health Record Systems

by

Benjamin T. Gerke

MS, Walsh College of Accountancy and Business Administration, 2003

BS, University of Wisconsin La Crosse, 1999

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

May 2022

Abstract

Users of electronic health record (EHR) systems lack data security mechanisms and are at risk of patient data breaches. Grounded in routine activities theory, the purpose of this qualitative case study was to explore strategies information technology security managers in the health care industry use to minimize electronic health record data breaches. The participants were nine information security managers of large, medium, and small health care organizations in the Midwest United States. Data collection included semistructured interviews and organizational documents. Through methodological triangulation, three themes emerged: (a) requirements based on government and organizational regulations, (b) implementation of best practice industry-standard security measures, and (c) emerging interoperability with a security and privacy program. A key recommendation is for information security managers to understand the motivations and triggers of positive behavior change that minimizes organizations' external and internal data breaches. The implications for positive social change include the potential to enhance the security presence and reputation of the health care organizations.

Security Strategies of Electronic Health Record Systems

by

Benjamin T. Gerke

MS, Walsh College of Accountancy and Business Administration, 2003

BS, University of Wisconsin La Crosse, 1999

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

May 2022

Dedication

I am dedicating this study to my family, friends, and most of all to my mother. Throughout this process, you all have been there with me. You all have been my primary support, and this is our study. Thank you, Mom, Mrs. Patricia Gerke, for believing in me and instilling in me that my goals are always attainable, and if I cannot reach for the skies, reach for the mountain top. Finally, I would like to dedicate this study to my supportive family and friends who gave me support and encouragement when I lost interest over the years. Your words of encouragement motivated me and helped me reach the finish line.

Acknowledgments

I would like to extend my gratitude to my committee: Committee Chair Dr. Charlie Shao, Second Committee Member Dr. Cheryl Waters, and University Research Reviewer Dr. Jon McKeeby. Your continuous feedback has prepared me to this point, and now I have a better understanding of scholarly writing.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Problem Statement

Health care organizations have communities with growing data breach concerns and fears of unwanted data exposure by health care practitioners requiring personal medical information to be secure and protected (Kwon & Johnson, 2013). According to Cascardo (2015), the 2013 Redspin Breach Report indicated that more than 800 patient data breaches have occurred since 2009, with 29 million patient records affected by Health Insurance Portability and Accountability Act of 1996 (HIPPA) violations. The general information technology (IT) problem was that users of electronic health record (EHR) systems lack data security mechanisms and are at risk of patient data breaches. The specific IT problem was that some information security managers within Midwest United States health care organizations lack strategies to prevent data breaches of the organization's EHR system.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the security strategies used by information security managers in Midwest United States health care organizations to prevent data breaches within EHRs. The targeted population consisted of information security managers of three health care organizations who had implemented strategies to prevent data breaches within their EHRs and were located in the Upper Midwest United States. The results of this study may impact social change by improvement of EHR security awareness promoting enhanced identity theft protection for patients and competitive business growth of critical access hospitals. Health care

associations' financial development is subject to trust and notoriety of patient care, and enhanced security measures could change ways of life in patients by giving extraprovincial healing facilities by the Centers for Medicare and Medicaid Services (CMS) management of data records.

Nature of the Study

A qualitative case study was chosen for this study. Using a qualitative approach allows the researcher to examine and investigate the issues pertinent to gaining an in-depth understanding of the phenomenon (Creswell & Guetterman, 2019; Houghton et al., 2015). The qualitative method was appropriate for the current study because I explored the issues pertinent to securing EHRs and gaining an in-depth understanding of the strategies used to secure EHRs. Quantitative research includes testing of hypotheses and analysis of independent and dependent variables with a distinction between experimental and correlational methods (Levitt et al., 2018; Mohajan, 2018). A quantitative method was not selected for the current study because the study did not require data to test a hypothesis involving independent and dependent variables. Mixed-methods research integrates quantitative and qualitative methods of data collection and analysis. This approach was also unsuitable for the current study because no quantitative data needed to be collected. Qualitative methodology was appropriate for this study because no hypothesis was tested and no relationships between variables were studied.

For this study, several designs were taken into consideration: ethnographic, phenomenology, and case study. Researchers using an ethnographic method explore the participants' lifestyles, behaviors, knowledge, beliefs, habits, perspectives, and cultural

practices (Yin, 2014). The ethnographic research method was not appropriate for the current study because human characteristics such as participants' lifestyles and behaviors would not have provided details regarding information security managers' strategies in EHRs. A phenomenological design focuses on understanding lived experiences of a sample population. This design was unsuitable for the current study because I did not intend to explore the lived experiences of information security managers related to data breaches. A case study is conducted when a researcher wants to study a phenomenon, understand how decisions were made for similar cases, and capture unique data on the subject being studied (Hyett et al., 2014). A case study design was appropriate for the current study because it provided a method to conduct an in-depth analysis of how health care organizations' information security managers secure their EHR systems by the implementation of secured patient record strategies.

Research Question

What strategies do information security managers within health care organizations use to prevent data breaches of the organization's EHR system?

Interview Questions

The following interview questions were used to collect data to answer my research question:

1. What is your IT background, such as education, work experience, etc.?
2. What is your role in respect to database security measures for the EHR?
3. What security measures does your organization use to prevent EHR breaches?

4. What solutions does your organization provide with regards to preventing EHR breaches?
5. What lessons learned do you have regarding preventing EHR data breaches?
6. With your experience as an IT professional, what obstacles does your organization face with regards to implementing EHR security measures, and why?
7. In terms of EHR, are there any concerns in implementing security measures, and if so, what has the organization done to rectify these concerns?

Conceptual Framework

The conceptual framework chosen for this study was the routine activities theory (RAT). The RAT theory was developed by L. E. Cohen and Felson in 1979. This theory requires three elements to be present: a motivated offender, a suitable victim or target, and the absence of a capable guardian (Reynald et al., 2018). Motivated offenders refer to wrongdoers with criminal intentions and the ability to act on these inclinations. A suitable victim or target can be a person, object, or place. Finally, a capable guardian is a person who is able to act in a protective manner or in the form of more passive mechanical devices.

RAT posits that a crime will occur in the presence of motivated offenders, the absence of effective guardians, and the availability of suitable targets in the same time and space (Choi, Kyungseok, & Yong, 2016; W. Reyns, 2013, 2015). This framework was appropriate for exploring the security strategy of EHR systems because the lack of a guardian presence of the EHR system could provide reasonable assurance of lacking

strategic measures. In the context of the current study, a motivated offender was defined as an internal or external person of interest who seeks personal gain or exploitation of a patient's records. Patients of the identified health care organization constituted suitable targets. The more suitable and accessible the target, the more likely that a crime will occur. Guardianship in relation to electronic medical records in this study referred to the information security managers who are able to act in a protective manner. RAT relates the pattern of offending to the everyday patterns of social interaction, which applied to my study by referencing the routine use of patient EHRs.

Definitions of Terms

The following key operational terms were used in the study:

Electronic health record (EHR): An electronic version of a patient's medical and health care history that may include all of the key administrative and clinical data relevant to that person's care, maintained by providers (Joseph et al., 2014).

Electronic medical record (EMR): The original content of the paper medical records of patients with the overall medical processes administered, representing the entire medical information of patients (He & Yan, 2014).

Enterprise architecture: The organizing logic for an organization's IT infrastructure and business processes (Vessey & Ward, 2013).

Health information technology (HIT): The computer hardware and software used to privately and securely store, retrieve, and share a patient's health and medical information (HealthIT, 2015).

Interoperability: The ability of two or more systems to communicate, exchange information, and use the exchanged information (Andrade et al., 2013).

Meaningful use: Using certified EHR technology to (a) improve quality, safety, efficiency, and reduce health disparities; (b) engage patients and family; (c) improve care coordination and population and public health; and (d) maintain privacy and security of patient health information achieve to qualify for CMS Incentive Programs (Silverman, 2013).

Nonfederal acute care hospitals: Acute care general medical and surgical, general children's, and cancer hospitals owned by private/not-for-profit, investor-owned/for-profit, or state/local government and located in the 50 U.S. states and District of Columbia (Charles et al., 2015).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are expectations that the researcher believes are true and that may pose a risk to the study. Identifying assumptions allows the reader to better understand what the researcher believes to be true in regard to the study (Rubin & Babbie, 2016). My first assumption was that hospital information security managers who participated in this study would have thorough knowledge of information systems employed in their facilities, knowledge of the IT infrastructure, and experience with security strategies used for the successful implementation of EHR systems. The digitalization of information in medical care was intended to include persistent consideration, information quality, information move, and navigation. Harrington (2019) stated that the issues dealt with

ineffectively managed and planned infrastructures and PC interfaces alongside advanced cloning. My second assumption was that participants would provide honest and in-depth responses to the interview questions and would be honest about their experiences when participating in the study. My third assumption was that the justifications and rationale for the selection of the conceptual framework and the method and design were appropriate for the goals of this study based on previously published recommendations of research experts.

Limitations

The limitation of this research study was a geographical constraint because it included IT security managers in health care organizations located only in the Upper Midwest United States. This geographical limitation may not have represented the views of IT security managers throughout the United States. In Section 2, I provide detailed rationales for the choices, discussions of the steps, and descriptions of the population and sample to improve the likelihood that appropriate decisions about transferability could be made (see Forero et al., 2018).

Delimitations

Delimitations are statements about items the researcher believes are outside the boundaries of the research problem (Rubin & Babbie, 2016). Rubin and Babbie (2016) contended that delimitations are the boundaries of research, and items outside these boundaries are not relevant to the research problem. A delimitation of the current study was the inclusion of participants who actively worked in EHR development; I excluded other project stakeholders. A second delimitation was the interview questions, which

were limited to EHR security strategies to prevent data breaches. The third delimitation was a geographic location of the Upper Midwest United States. A fourth delimitation was health care providers. A fifth delimitation was the relatively small sample size. A larger sample size would have been costlier and more time-consuming.

Significance of the Study

This study may be valuable to information security managers because I explored security strategies to prevent data breaches in EHR systems. I investigated security strategies because security of confidential and sensitive data remains a challenge for health care organizations. Furthermore, the expanding volume of literature related to EHR utilization represented a test to the executives' capacities of medical services associations (Y. Wang et al., 2018). Exploring these security strategies to prevent data breaches may also be beneficial in cost savings and may improve both operations and technical capabilities of the organizations because this study may increase the use of leveraged information security controls. With these security strategies in place to minimize data breaches, patients may feel confident that their data are secure and will not be compromised.

This research may impact social change in communities because the implementation of a security strategy improves identity theft protection. Enhanced patients' confidence in personal data protection promotes greater overall security presence and reputation of the health care organization. Improved overall reputation could lead to enhanced management of the health care organization. Additionally, health care professionals in hospitals regularly share the medical information of patients by their

health care providers. If the security strategies are in place to protect data breaches, this may increase the confidence of patients to share health care network resources, which could facilitate revenue growth to primary care provider services as referrals. Securing patient information and their personal identity data may save lives and help to keep patients' personal information from being compromised. In conclusion, diminished health care reputation through the lack of strategies to prevent data breaches could prompt loss of income with declining quiet repeating visits, which could prompt negative group medical problems.

A Review of the Professional and Academic Literature

The purpose of this qualitative case study was to explore security strategies used by information security managers in Midwest United States health care organizations to prevent data breaches within EHRs. EHR reception has turned into a pressing public need in the United States (Ebnehoseini et al., 2020; Rajaram et al., 2020). The medical services industry has carried out and consolidated innovation at an outstanding rate contrasted with some other industries (Capece & Lorenzi, 2020). In 2015, approximately 80% of doctors had made or were making arrangements to join an EHR framework, but only 15% of mental emergency clinics had embraced a fundamental EHR (Hu et al., 2020). Researchers have not satisfactorily investigated authority practices in medical services as a likely arrangement in alleviating insider danger issues (Guhr et al., 2019; Haqaf & Koyuncu, 2018; Vasileiou & Furnell, 2019). Insiders have knowledge of security access, organizational trust, and procedures and protocols. Insider threats account for almost 70% of data fraud (Bhuyan et al., 2020). Contemporary EHR executions frequently influence

cloud-based foundations to meet execution prerequisites in essential consideration settings because cloud structures consolidate practical handling power, high accessibility, unwavering quality, and adaptability (Hertzog et al., 2019; Mues et al., 2018). As indicated by Dalal et al. (2019), medical services associations have worked with specialists in the human elements and frameworks designing an area with an end goal to approve medical care processes and work on the execution of new EHR frameworks. Salwei et al.'s (2019) study underlined the requirement for work process investigation during human-centered design interaction to distinguish positive and adverse consequences on physician work processes. A few associations have a mixture work framework in which suppliers work in two unique ways by recording on paper as a workaround and archiving in an electronic framework (Blijleven et al., 2019; Pescatore, 2019). Contrasted with actual record frameworks, electronic frameworks give a reasonable benefit of killing a large part of the waste that accompanies medical services tasks and patient therapy (Kocher, 2021; Mayer et al., 2019). EHR frameworks advance cooperation among patients and medical services providers (Misto et al., 2020). EHRs also may decrease billing errors (Atasoy et al., 2019). EHR systems likewise provide freedom to bind the correspondence and information handling frameworks (Wencheng et al., 2018). Rathert et al. (2019) revealed that the additional corresponding themes for the EHR challenge included (a) lack of standardization, (b) increased workload, (c) the overreliance of technology, (d) lack of patient–provider relationships, and (e) insufficient training, and (f) the mistrust in information. Lanier et al. (2018) featured the numerous obstructions to coordinating and carrying out an EHR framework into medical care and

recorded them as (a) absence of console abilities, (b) a lack of staff who have the information on various frameworks, (c) a deficiency of medical care data technologists who know how to execute and deal with the frameworks appropriately, and d4) a lack of distinctive EHRs frameworks to acquire mechanical information. Looking back, obviously, the previously mentioned is legitimate in the present innovative world (Sittig et al., 2018).

The current study's literature review method was systematic (see Angraini et al., 2019). A systematic literature review is an explicit, transparent, and thorough method for defining, analyzing, and synthesizing the findings of works by researchers, academics, scholars, and practitioners (Angraini et al., 2019). IS researchers have utilized the hypothetical focal point of coerciveness and strengthening to conceptualize the executives 'approaches to data security strategy consistency (Balozian et al., 2019). In my review of the academic literature, I discuss RAT as the conceptual framework for this study and provide a background for security strategies while relating the topic to the central research question: What strategies do information security managers within health care organizations use to prevent data breaches of the organization's EHR system? In the following review of the literature, I examine themes that emerged from the literature regarding the topic of security strategies and illustrate (a) how security strategies have become an applied IT problem worthy of research, (b) how security strategies are defined and explained through the RAT, (c) security strategies as they relate to rival theories, (d) security strategies in health care, (e) security strategies data breaches, and (f) models and frameworks supporting security strategies. Other themes that emerged throughout the

literature regarding security strategies included regulatory compliance, health care sector regulatory requirements, and benefits/barriers to security strategies provided in a symbolisms analysis of terms referenced as architecture, framework, and model.

This literature review comprised 307 articles, journals, and conference proceedings. The primary research libraries and databases included the ACM Digital Library, EBSCOhost Computers and Applied Sciences Complete, IEEE Xplore Digital Library, ScienceDirect, ProQuest Computing, and ProQuest Dissertations and Theses Global. I also used the Google Scholar search engine. I identified the peer-reviewed status of articles using Ulrich's Global Serials Directory. Nabor (2015) contended that the literature review might include knowledge that could prompt resolutions or add to the current study. The meticulousness of subjective research coordinated toward information building includes an iterative approach as the examination progresses. Along these lines, a broad review of the writing required diverse techniques to reveal studies important to the current research.

The inquiry procedure is basic to assess the quality and amount of writing uncovered to the researcher. Top-to-bottom analysis of writing for this research happened through a topical methodology including the thought and consideration of different insightful works, original writing, administrative reports, and related books. Search techniques involved the following key terms: *advantages of EHRs*; *EHR foundation and history*; *EHR usage procedures*; *obstructions to EHR selection*; *health and security of PHI*; *health data innovation*; *CIOs, administrators, and authority ways to deal with EHR*; *RAT and strategies for innovation reception, utilize, protection, and acknowledgment*;

and *subjective contextual analysis, qualitative research, and thorough companion assessed strategies and outlines*. Resources accessed in this literature included U.S. government sites; Walden University library databases such as EBSCO Academic Search Complete, ProQuest Central, SAGE Full-Text Collection, and Thoreau Multi-Database; Google Scholar; and electronic and printed books. I used the Ulrich Periodicals Directory for peer-reviewed status.

Evolution of the Routine Activities Theory

The RAT includes three elements: a motivated offender, a suitable victim or target, and the absence of a capable guardian (Reynald et al., 2018). A motivated offender is a wrongdoer with criminal intentions and the ability to act on these inclinations. A suitable victim or target can be a person, object, or place. The probability of exploitation relies on how much a casualty's internet-based conduct is for all intents and purposes general to a culprit's modified malware, including PC infections, worms, Trojan ponies, ransomware, spyware, and other malignant codes (Hsieh & Wang, 2018). Finally, a capable guardian is a person who is able to act in a protective manner or in the form of more passive mechanical devices (McKillop et al., 2020). RAT relates the pattern of offending to the everyday patterns of social interaction, which applied to my study by referencing the routine use of patient EHRs.

RAT posits that a crime will occur in the presence of motivated offenders, the absence of effective guardians, and the availability of suitable targets in the same time and space (Choi et al., 2016). The RAT framework was appropriate for the current study because the lack of a guardian presence could provide reasonable assurance of lacking

strategic measures. A motivated offender can be defined as an internal or external person of interest who seeks personal gain or exploitation of a patient's records. Patients at the study site health care organization would be the offender's target; the more suitable and accessible the target, the more likely it is that a crime will occur. Petrescu et al. (2018) suggested guardians in relation to EMRs are information security managers who are able to act in a protective manner.

I used the RAT in conjunction with L. E. Cohen and Felson's (1979, as cited in Williams, 2015) proposal that a crime is likely when the three statutes of RAT are joined in space and time. The three statues are a persuaded wrongdoer, a reasonable target, and the nonappearance of a skilled gatekeeper (Choi et al., 2016; Elmaghraby & Losavio, 2014). RAT was well suited for the current study because it helped me identify and understand how and why the case study organizations decided to implement security strategy practices based on whether wrongdoer, target, and gatekeeper statues played a role as influencing factors (see Tyler, 2018). Further, new regulations and forces continue to emerge in the field that deals with the security of HITRUST and PHI (Hughbanks, 2018). By better understanding and identifying these factors from the viewpoint of RAT, I aimed to identify factors from data collection that could be used as strategies to answer the research question.

At an individual level, propelled wrongdoers, able guardianship, and target engaging quality would likely increase the danger of cyber exploitation (Moir et al., 2018). The linkage of these components enhances the likelihood of crime; the nonappearance of a segment decreases it (Elmaghraby & Losavio, 2014). RAT can

prescribe guidance, leadership, and framework for information security and prescribe potential vulnerabilities and recommendations for redesigned IT security. Knowing how to diminish the danger of exploitation is imperative. By applying security strategies associated with RAT, IT experts might be in a better position to reduce the risk of exploitation (Argaw et al., 2020; Choi et al., 2016).

The spurred guilty party class is recognized by motivations that range from advantageous to outrageous conditions. Motivations may be free or in items get a handle on allurement, instigation, helpful time, and weariness (Elmaghraby & Losavio, 2014). The closeness of competent watchmen implies routinely introducing individuals who have the ability to divert offenses or direct recovery by repair (Elmaghraby & Losavio, 2014). At the point when skilled gatekeepers regulate reasonable targets, inspired wrongdoers are checked by handlers, directors manage submissive spots, and crime avoidance is conceivable (Choi et al., 2016). RAT is used as a lens through which to view the perceptions of expanding guardianship and diminishing target reasonableness of individuals most in danger of exploitation from cybercrime (Choi et al., 2016). Exploitation fits inside the RAT segments of decreasing target qualification by making potential aggressors mindful that higher hazard bunches are associated with IT experts who go about as tutors inside health care conditions.

RAT is a hypothesis of criminal occasions that can be connected to innovation. RAT has often been used in the teaching of victimology (B. W. Reyns et al., 2015). Fundamentals of RAT include the potential outcomes for exploitation when persuaded wrongdoers defy reasonable focuses in conditions requiring fit watchmen (B. W. Reyns

et al., 2015). Without these three basic criteria, exploitations are less likely to occur. Scientists propose that RAT was set up as a hypothesis for different criminal exercises (Leukfeldt & Yar, 2016). One such clarification of the different variables of crime is a mix of inspiration, opportunity, and the nonappearance of a competent gatekeeper (Leukfeldt & Yar, 2016).

RAT is additionally helpful in creating clarifications for data breaches. L. E. Cohen and Felson (1979) affirmed that specific components must be available for a crime to occur: a person with criminal intent and the ability to commit a crime. By thinking about a few data breaches, comes about can not be conjectured (Leukfeldt & Yar, 2016). In the event that casualties are contrary to noncasualties, any appearing connection connecting exploitation and ways of life would be misleading (B. W. Reyns & Scherer, 2018). Bunch et al. (2014) contemplated the impact of exploitation on routine exercises and attested that they consider either defrauded individuals change their standard exercises following exploitation or if there is an association between exploitation and high-hazard exercises. Exploitation ways of life are the consequence of fundamental factors that prompt both the exploitation and the ways of life (Bunch et al., 2014). Vecchio (2013) noted that although the association between culpability and exploitation has been established, researchers have not addressed how exploitation influences foreseen conduct. Casualties accumulated less academic review than wrongdoers, accentuation on the casualty populace and their encounters is currently ordinary.

RAT researchers have speculated that casualties and guilty parties are frequently demographically, socially, and typically comparative. As the individual danger of

exploitation increases with the time potential casualties spend around spurred guilty parties, the people most in danger are those associated with illegal medication utilization and road violations (Vecchio, 2013). Additional intensifying exploitation among guilty road parties is a typical reluctance or inadequacy to report crimes (Vecchio, 2013). According to RAT, individuals 'social lead influences the potential for exploitation. In a wide sense, the odds of turning into a casualty of an assault are substantially higher on a night out than on a night spent home alone (Näsi et al., 2015). Casualties of an assault can happen whenever.

RAT might be valuable to make the feeling that various parts of online exploitation strengthen a practically identical hypothetical approach (Williams et al., 2019). From the RAT perspective, one could fight that both appropriateness for transforming into a target and the piece of guardianship expect a noticeable part both on the system and isolated circumstances (Näsi et al., 2015). Wide urban regions give openings and sensible concentrations to offenders. Living in a bigger city may similarly identify with life choices that enhance the likelihood of exploitation (Näsi et al., 2015). The nonappearance of guardianship is regular for those living in the major urban territories (Whitty, 2019). The same may apply to some degree to the people who are less fused socially (Näsi et al., 2015). Casualty presumption presumes that casualties can totally translate the criminal demonstration, and RAT is extraordinary compared to other known, best contemplated, and most alluded for exploitation (Doerner & Lab, 2015). Exploitation is alluded to as a casualty.

According to RAT, opportunity structures influence the pervasiveness of freak conduct. Guilty parties remain keen on objectives to which they relegate an incentive for reasons unknown and the progression of the presence of a spurred wrongdoer and an appropriate target, and the deficiency of an able watchman controls these structures (Leukfeldt & Yar, 2016). Crime counteractive action should originate from an unexpected edge in comparison to target solidifying alone (Leukfeldt & Yar, 2016). As indicated by RAT, skilled guardians likewise assume a critical part.

Theory of Rational Behavior and Elements of RAT

RAT and Krstić's (2014) theory of rational addiction behavior (TORB) provided supporting theory for this study. RAT worked under the suspicion that individuals purposefully settle on reasonable decisions to carry out crimes (Wang et al., 2015). Wang et al. (2015) utilized RAT to control violations by focusing on where to discover and how to catch criminals, which filled in as an obstacle keeping thieves from perpetrating crimes. RAT was not used to offer reasons why a few people go without unfortunate behavior and what spurs others to carry out violations, yet it provided the way to investigate situational and natural variables of crimes (Wang et al., 2015).

While anchoring data that included PHI, RAT assumes an essential job while evaluating the connections among circumstances and weaknesses to effectively shield patients ʾpersonal records or information (Khey and Sainato, 2013). As indicated by Khey and Sainato (2013), a perceptible increment in extortion prompted $1 trillion misfortunes in medicinal services inclusion credited to national and global cybercrimes (Khey and Sainato, 2013) performed by criminals for individual and monetary profit.

Wang et al. (2015) expressed that the RAT idea worked under the supposition whereby individuals settle on judicious decisions because of motivation, opportunity, and when surroundings are appropriate to submit violations. RAT was at first acquainted with clarifying savage criminal exercises (Wang et al., 2015). The statement of RAT asserted that specific individuals are equipped for debilitating violations and keeping them from happening through the reception of physical security (Wang et al., 2015). The theory involved four primary elements that included value, inertia, visibility, and access: (a) Value involves the act of reducing risk relating to insider attacks by introducing internal resistance about improper use of functionality, movement of data, and discovery to commit crimes. For example, criminals could steal information including names, phone numbers, SSNs, credit cards, bank accounts, and other consumer data trading such valuable information for sale on the black market, (b) Inertia deals with the strength and control making it difficult for the internal perpetrator to steal information with malicious intent to control input, processing, and output to ensure accuracy and validity of criminal actions performed by an offender, (c) Visibility occurred when a person realized the existence of a target knowing the whereabouts malicious action, and (d)Access involved the action enabling offender or perpetrator to modify data due to necessity and needs (Wang et al., 2015).

Utilizing TORB could prompt a superior comprehension of why a few people settle on choices for personal matters picking the method of reasoning just without over-the-top wants (Krstić, 2014). RAT and TORB structures were likewise suited in investigating the techniques some healthcare services pioneers used to avoid identity theft

and medical personality extortion to enhance execution. Both RAT and TORB theories gave bits of knowledge in regard to why a few people settle on cognizant choices to carry out violations while others abstain from unfortunate criminal behavior, which could aid avoidance endeavors.

Rational Choice Theory

Rational choice theory (RCT) was another theory likewise important for establishing this study. Becker (1968) presented the RCT financial methodology of crime while Cornish and Clarke (1986) returned to the idea noticing that a few people intentionally settle on normal decisions to carry out violations (Matthews, 2014). Cornish and Clarke declared that individuals carried out violations by gauging the chances against the expense of not getting caught or punished (Matthews, 2014). The RCT idea was critical to this study since imposters settled on judicious decisions and carried out identity theft by mimicking exploited victims and perpetrated restorative medical identity extortion for medicinal services benefits in the wake of deciding the risk merited carrying out the crime. Understanding preventive strategies additionally incorporate the comprehension of hindrances making identity security theft increasingly troublesome and less engaging for imposters who took calculated risk to imitate individuals and submit medicinal personality misrepresentation and got medical procedure records under someone else's name through distortion of patients' therapeutic records (Taitsman et al., 2013).

Wortley and Mazerolle (2008) characterized fraud as a professional crime (WCC) and a levelheaded decision (Madensen, 2009). Madensen (2009) expressed that medicinal

personality misrepresentation fell under the domain of WCC identifying with health care crime. FBI authorities characterized WCC as a nonviolent crime for individual, money-related, and authoritative gain referred to by (Champion, 2011). RCT gave the way to explore restorative practice pioneers 'basic leadership strategies to deflect potential impersonators and forestall security identity theft and medicinal character misrepresentation crimes (Byrd, 2019).

Applications of RAT in Different Fields

The focal parts of RAT (motivated offender, suitable target, lack of guardians) have been operationalized to gauge RAT ideas in an assortment of ways. Thus, the consistency of measures stays nonexistent, and the generalizability and consequent legitimacy of these measures are powerless. Further, Tewksbury and Mustaine (2003), just as Mustaine and Tewskbury (1997), demonstrate that operationalization of factors used to inspect RAT are circuitous, best-case scenarios.

1,513 school and college understudies from eight states were utilized to evaluate guardianship by method for self-defensive measures. The dependent variable utilized in this study was ownership and conveying of self-defensive measures (Tewskbury and Mustaine, 2003). Self-defensive measures were operationalized, by method for self-report measures, into dichotomous factors to decide if understudies had conveyed a weapon, mace, a club, body caution, or a blade inside the previous half-year. Respondents were likewise requested to report statistic qualities, network attributes, way of life practices, dread of crime, view of individual security, just as extra proportions of substance and liquor use. Tewksbury and Mustaine (2003) announced that most proportions of

neighborhood structures and neighborhood conditions, dread, and impression of security were poor indicators of guardianship.

The study revealed that social complications of neighborhoods, living close to junk food eateries, dwelling in a network with huge quantities of youth, and business were all decidedly identified with the utilization of self-defensive measures. Utilization of medications, particularly crack, was additionally decidedly corresponded with the utilization of self-defensive measures (Tewksbury and Mustaine, 2003). Tewksbury and Mustaine (2003) announced that way of life practices estimating expanded presentation to risky conditions or potential guilty parties are simply the most critical indicators of security.

Wang (2002) connected RAT to clarify the causal elements of an arrangement of bank burglaries executed by Asian males. In spite of the fact that bank burglaries are not viewed as a novel criminal marvel, crimes executed by Asians speak to a topic that has just been inspected since the late 1990s. Further as yet, applying RAT speaks to the wide pertinence of this theory. Wang (2002) estimated target reasonableness through the factors (1) overwhelming pay days (2) bank area close interstates (3) major banks with a large number of customers and employers (4) non-Asian claimed banks. Inadequate safety efforts were used to survey the absence of guardians. The factors early morning thefts, unarmed security officers, and learning of the encompassing police offices shift change plan was operationalized to gauge guardianship. The outcomes demonstrated that explicit crime measures are a fitting technique for looking at the benefits of RAT (Wang, 2002).

Various studies have joined RAT as the focal theoretical clarification of criminal wonder. Most studies, in any case, use RAT to survey criminal exercises executed outside of the home (bank burglaries, undergrads' exploitation, car burglary, Amish beatings, and pre-adult male exploitation, to give some examples). Scarcely any exploitation ponders the focal standards of RAT (suitable target, motivated offender, lack of capable guardians) to evaluate criminal acts executed inside the home by those known to each other. The present study used the defenders of routine activity theory in connection to the lack of EHR security strategies and factors that may expand the likelihood of this criminal demonstration.

Criticism of RAT

As indicated by Clarke and Felson (1993), "the standard action approach started by considering just direct-contact ruthless infringement." In the first theoretical record, routine activities theory saw people as items, not human units. Subsequently, the fundamental inspirations for the commission of legitimate infringement stayed discussion unworthy. It was essentially accepted that a "motivated offender" (one of the three key segments of RAT) classified any being that carried out a criminal demonstration. De Waal et al. (2018) expressed that creators have estimated that patients powerless to analysis might keep away from associations with people inclined to fierce conduct. Plus, the connection between some illness 'indications, for example, marginal behavioral condition and encounters of fierce exploitation, is completely directed by feeling guideline troubles, which expands patients 'weakness to rough exploitation, and patients who think that it is trying to manage extreme passionate encounters might be more

inclined to hazardous practices and inclusion in oppressive connections (De Waal et al., 2018).

RAT applies to this study as it gives immense comprehension to why individuals take part in data breaches. The conceptual framework infers that RAT is appropriate for examining and depicting data breaches. RAT is experimentally connected to different data breaches and records a portion of the methodological issues it requires. RAT focus is on offenses at the event level and thinks about the basic regular conditions for a crime to occur at a specific place and time. RAT conditions feature the system between parts that deliver crime opportunity and, finally, crime events (Johnson & Groff, 2014). Since we can figure what routine exercises offer rising to transnational crime, it is then possible to do crime-neutralizing activity exercises that stay to diminish crime on an overall scale. These fuse crimes that incorporate data leaks of an individual or corporate protection, infringement executed by individuals that purposefully change data inside organizations or government workplaces income-driven, individual or political objectives, and infringement that incorporate endeavors to annoy the activity of the system (Mikeal, 2019).

There is a critical hole or gap in the review of literature that meets the requirement for additional and further studies. Thorough assessments of the theory are verifiably absent qualifications and clarification from the writing. With a couple of oversights, most investigations have not operationalized all the center considerations of the theory (Reyns, 2015). The time-based relationship of the framework gives exhaustive knowledge into the matter of consistency (McCarthy et al., 2014). Harmful customers can

store patient previews containing PHI of patient records in open file formats consulting with available distribution to various entities or even published in the cloud (Hashizume et al., 2013). On the off chance that another customer utilizes this data, the transference that this customer performs will debase the covering of a data breach. Additionally, unintentional data spillage can be exhibited by EHR replication (Hashizume et al., 2013).

Contrasting Rival Theories

Rival theories of the conceptual framework that were initially seen as plausible to support the study included lifestyle exposure theory (LET) and lifestyle routine activity theory (LRAT). Hindelang, Gottfredson, and Garofalo (1978) introduced LET in 1978 to inquire about exploring the relationship associating ways of life and crime ought to abstain from pooling or be earning crime principles, since estimating the outcomes of ways of life on composite measurements of crime prompts opposing conclusions (Hindelang et al., 1978). LET is one of the main efficient theories of criminal exploitation created by Hindelang et al. (1978). LET was initially planned to represent disparities in the dangers of brutal exploitation crosswise over social gatherings. Yet, it has been stretched to suit property crime, and it shapes the reason for more detailed theories of target choice procedures. Since the 1950s, exploitation theories have created down-to-earth and episodic help, which most equate as a way of life introduction (Hindelang et al., 1978). The essential start hidden the LET is that statistic contrasts in the credibility of exploitation.

LET, and RAT surfaced as critical indicators of exploitation. LET and RAT was developed in the late 1970s as entire illustrations plot to exhibit disparities in the danger

of exploitation (Pratt & Turanovic, 2015). Specialists utilize LET and RAT to see exploitation as the merging of aroused guilty party, an objective, and the nonattendance of guardianship (Pratt & Turanovic, 2015). A fit watchman can go up against numerous structures, and individuals assume a huge part in a crime. LET gives a conceptualization of hazard in probabilistic articulations; RAT just speaks to the exploitation occasion itself (Pratt & Turanovic, 2015). These theories contrast with how the elements of individuals are “in danger” for exploitation.

RAT and LET are perceived to be impacted by exploitation. RAT and LET recommend that exploitation rates differentiate over a statistic group of onlookers since individuals in social orders take part in different exercises (Bunch et al., 2015). Routine exercises mediate the associations between statistic characteristics and exploitation. On account of the center supposition conveying the two contemplations, a few scientists have endeavored to test its authenticity, and the tests that do persevere ought to depend principally on cross-sectional, non-practically identical data (Bunch et al., 2015). The change of routine exercises and lifestyle perspectives have essentially helped in the examination of the casualty and wrongdoer cover (Vecchio, 2013).

According to lifestyle routine activity theory (LRAT), normal exercises may open a few people and their property to more genuine dangers. Risk occurs if certain practices increase the chances of being exploited, and one of the three key components (i.e., persuaded guilty party, alluring target/casualty, and nonappearance of fit guardianship) is missing (Pratt & Turanovic, 2015). Miethe and Meier (1990) exhibited a basic hypothesis of exploitation known as LRAT. With the assurance of an episode, casualties inside a

socio-spatial setting controlled by the standard utility concentrate less finished RAT versus LET (Miethe & Meier, 1990). LRAT, for instance, single individuals experience higher individual violations than do different gatherings in light of more noteworthy presentations.

LRAT perceives that likeness to persuaded liable gatherings, introduction to dangerous conditions, target engaging quality, and the shirking of capable watchmen are the key factors that choose the likelihood of criminal exploitation. Ages of victimologists have incorporated RAT and LET into an LRAT of criminal exploitation that underlines the noteworthiness of ways of life and routine exercises in delivering open doors for exploitation (Reyns & Henson, 2015). With the attention to the social idea of a crime, RAT sets that the synchronization of the three parts (i.e., inspired guilty parties, appropriate and appealing targets, able gatekeepers) enhances the likelihood of rough exploitation (Cohen & Felson, 1979). The danger of exploitation happens when offenders are in the region to each other (Singh and Bakar, 2019).

Criminology centers around the LRAT of crime. Cohen and Felson (1979) argued that crime as an arranged marvel in people in the general field is liable to three portions: a propelled wrongdoer, a reasonable target, and an absence of competent guardianship. Combining these parts enhances the likelihood of criminal or drive activity and increases the likelihood of exploitation. LRAT is the most convincing criminological hypothesis (Ilievski, 2016). The approach relies on two essential contemplations: that the offense happens when animated liable gatherings are closer to unprotected targets, and that

demonstration relies on the likelihood of an occasion affecting normal activities, which fuse organizations, family, unwinding, and other regular exercises.

From a methodological viewpoint, the measure of despising crimes used as a piece of misuse thinks about does not on an exceptionally essential level shift from those of various kinds of crime either. Van Kesteren (2016) announced that since detest crimes are particular, there is no inspiration driving why their dissemination among target peoples couldn't speak to tantamount components as other individual infringement, for example, way of life-related land or social closeness to potentially liable gatherings. A positive connection between informational accomplishment and savage crime exploitation isn't an abnormal finding in victimological thinks (Van Kesteren, 2016). There are four classes for victimology: (a) digital trespass; (b) digital double-dealing robbery; (c) digital porn and vulgarity; (d) digital savagery. Data breaches typology is viewed as a standout amongst the most extensive systems to perceive the foundation of innovation into different classes of culpable (Holt and Bossler, 2013b). Understanding the explanations behind defenselessness and the danger of individuals through both a general hypothesis of crime and methods for LRAT has a central place in victimology (Pratt, Turanovic, Fox, & Wright, 2014). Related to irregularities in lifestyle choices, it is simply a single reason people move toward becoming casualties.

Marcum, Higgins, and Ricketts (2014) observed that casualties brought by driving forces of digital stalkers could fit into two classes: mechanical and social. The two classes infer more discernible data and capacities of the Internet, and moreover, an anomalous condition of the lack of definition of degenerate digital conduct. The current

writing applies the figured thoughts with a particular ultimate objective to test the connection between routine action, way of life, and malware crime. More conspicuous levels of prologue to blameworthy gatherings, target drawing in quality, and lower levels of guardianship enhanced the shot of staying away from malware crime.

RAT and opponent speculations LET and LRAT theories are used to set up similarity by including the reasonableness of targets and inspiration inciting data breaches. RAT is an expansion of LET and an audit of personal computing crime and exploitation (Elmaghraby & Losavio, 2014). One of the principal thoughts in the LET is lifestyle factors, which is implied in RAT as their objective reasonableness segment. Along these lines of life, factors add to potential PC crime exploitation (Cohen & Felson, 1979). RAT gives a genuine and careful comprehension of the purposes behind violations. At its root is the likelihood that without incredible controls, blameworthy gatherings will follow engaging targets. To have a crime, a persuaded guilty party must go to an equivalent place from an appealing target. Since that appealing target is never in a similar circumstance from a driving liable gathering, the target won't be taken, hurt, or struck. RAT has associated any way with the affirmation that LET gives a whole elucidation of the sensible target principal found in RAT.

Data Breaches Consequences in Health Care

In the United States, government associations, for example, CMS, have accepted a methodology to work on the wellbeing and prosperity of the populace at large by advancing enormous scope reception of EHRs to modernize the conveyance of clinical benefits (Kroning, 2018). Criminals focus on the medical services area on account of the

volume of important information that is traded every day (Ahmed, Naqvi, and Joseph, 2019). While EHR has been powerful, end-users, as well as patients, have shifting degrees of admittance to these records, which has prompted irregularity in current medical services strategies and tasks (Hemsley et al., 2018). The monetary effect from taken clinical information by data breaches or ransomware has been assessed to represent billions of dollars in fraudulent medical services, as per the National Health Care Anti-Fraud Association (National Health Care Anti-Fraud Association, 2020). As indicated by Yaokumah, Walker, and Kumah (2019), associations rely upon data frameworks to reinforce usefulness and execution, accordingly accomplishing the upper hand and achieving key objectives. Users of data frameworks are, in any case, inclined to deliberate and unexpected risks, as expressed by Yaokumah et al. (2019). The accompanying models take a gander at three data breaches that increased national consideration in 2015. The digital crooks that assaulted the three organizations purportedly procured representative credentials that enabled them to get to the corporate database where ePHI was put away. Every business was required to make open declarations and unveil data identified with the rupture.

Anthem Blue Cross Blue Shield

The Anthem Blue Cross Blue Shield data breach increased national consideration in February 2015. As the second biggest health insurance plan in the US, the breach was monstrous in measure, with 78.8 million PHI records stolen (Munro, 2015). At first, thought to be an advanced assault, an examination later uncovered that the digital criminal started an assault utilizing a procedure named skewer phishing (Ragan, 2015).

The FBI characters skewer phishing as a virtual trap set by digital criminals that utilizations official-looking messages to draw a client to counterfeit sites and deceives you into uncovering your own data (FBI, 2009). With skewer phishing, digital culprits endeavor to mimic people in a focused-on group of onlookers with particular qualifications or individual data that is important for them to access a focus on organizing (Martin et al., 2018). The lance phishing is customarily the starting strides of an assault. On account of Anthem, the digital criminal was fruitful in catching the accreditations of a database director (DBA) (Ragan, 2015). Once the digital criminal had control of the qualifications, the digital criminal could access Anthem's database. The examination uncovers that Anthem had scrambled the PHI; however, the utilization of the stolen qualifications by the digital criminal made the PHI uncovered and obvious.

As per reports from Anthem, the digital criminal got the certifications of the DBA and effectively accessed the organization's database on December 10, 2014. The digital criminal stayed undetected until January 27, 2015, when the DBA perceived that their qualifications were utilized to run sketchy inquiries against the database (Ragan, 2015). After the underlying revelation, the examination announced that five tech workers ' qualifications were endangered. Anthem issued a public statement educating clients that the organization had in certainty endured an information data breach and that the assailant could get names, birthday celebrations, distinguishing restorative proof, standardized savings numbers, road addresses, email locations, and worker data, including salary information (Anthem BCBS, 2015). The consequence of the Anthem Blue Cross Blue Shield data breach litigation settled for $115 million, the largest

settlement ever for a data breach, to be used to pay for credit monitoring for victims of the cyber breach. The Anthem BCBS cyber breach is one of many high-profile data breaches that have cost the US substantial monetary loss (Reuters, 2017).

Excellus BlueCross BlueShield

EBCBS found that its data frameworks were under assault for over 20 months, going back to December 23, 2013. The aftereffect of the information data breach was that 10.5 million PHI records had been uncovered for about two years (Kern, 2015). The EBCBS CEO posted on the organization site that the uncovered data included names, date of birth, government-managed savings numbers, postage information, phone number, part IDs, money-related record data, and cases data (Excellus BCBS, 2015).

EBCBS is doing combating against a putative legal claim documented in the US District Court of New York for wrongfully unveiling touchy individual data because of their inability to find a way to anchor and secure individual health data and the subsequent danger of digital criminals utilizing the stolen PHI against the people uncovered (Burns, 2015). The offended parties documented the legal claim referring to that EBCBS ought to have paid attention to the admonitions from different data breaches, including BlueCross BlueShield subsidiaries, and completed a superior security strategy in preparation against a digital assault. EBCBS claims that there is no proof that the programmer expelled any of the encoded PHI records from EBCBS data frameworks. What is essential to note is the digital criminal increased unapproved access with authoritative benefits to the EBCBS frameworks to see PHI, making the encryption debatable (McGee, 2015). The breach serves as a reminder for organizations to have a

proper security strategy that includes authentication in place to either prevent these types of errors or to quickly detect misconfigured or improperly uploaded data. Excellus has not released details of its expected costs in 2016, although the $17.3 million total is likely to rise considerably. In May 2015, the Ponemon Institute calculated the average cost of a healthcare data breach to be $363 per record. If those figures hold true, the consequence cost of the Excellus BlueCross BlueShield data breach could be as high as 3.6 billion.

VA

The Department of Veteran Affairs (VA) agreed to pay $20 million to veterans affected by a breach that took place in 2006. The breach was the result of an employee whose home was burglarized, and a VA laptop containing PHI was stolen. It took the VA employee nearly three weeks to notify his superiors of the theft, which sparked outrage on the part of the Secretary of the VA, James Nicholson. The payout was to be dispersed to those who showed harm from data theft, with any remaining balance to be paid out to veterans' charities. There were approximately 26.5 million active and retired servicemen and women whose information had been compromised (Yen, 2009).

Security Strategies: Informal and Formal

As recently expressed, this study's purpose is to explore the security strategies used by information security managers within the Midwestern United States (or Midwest) healthcare organizations to prevent data breaches within EHRs. It is basic that upper and midlevel executives know about the risks of online protection chances that exist with medical care strategies and what dangers are available in their associations, and get ready likewise (Abraham, Chatterjee and Sims, 2019). Three separate classifications

characterized these strategies: informal, formal, and technical. Al-Issa et al. (2019) utilized these classifications as subsidiaries from RAT; these classes shaped the establishment of this study's conceptual framework. The conceptual framework may distinguish vulnerabilities that hackers could endeavor to execute different assaults in the distributed computing setting (Mohammadi et al., 2019). It may likewise help information security managers in executing viable security strategies to manage inner and outer dangers in the EHR environment. EHR systems, to a great extent, characterized the security instruments conceivable to address security strategy intricacy. Nobles (2018) states that human-related errors cause around 95% of data breaches. Research showed that most occupants, colleagues, and understudies utilized their cell phones to save and move clinical pictures (Guo et al., 2018). To start with, Ghafir et al. 2018 guaranteed that informal controls give training on data security and make a security culture in the association (Miranda, 2018). Putting resources into quality EHR preparation ends up being valuable to all gatherings included; be that as it may, the medical services association should be available to contribute the time, assets, and monetary necessities to help improve the training system (Longhurst et al., 2019). James et al. (2018) made an answer dependent on study outcomes that justified upgraded preparing whose objectives were to "increment abilities, information and certainty" among the doctor populace. Formal controls require consistency with guidelines and strategies identified with compliance to regulations for data security (Muller and Lind, 2020). Ehrenfeld and Wanderer (2018) accentuated that having sufficient preparation prompts a useful doctor community with regard to EHRs. At long last, technical controls address issues with

access management (Tafreshi, 2018). These strategies stay pointless without a guardian to execute them.

Guardians are essential for security strategy operations. Researchers like Weisburd, Groff and Yang (2014) characterized guardians are people with the capacity to prevent a crime. Asserting that guardians are essential to the prevention of crime since they keep up cautiousness and execute security mitigations to dissuade potential guilty parties. Guardians characterize an association's inside and outside strategies as either informal, formal, or technical in nature. Pyrooz, Decker, and Moule Jr. (2015) noticed that an absence of capable guardians, just as a proper target and a conceivable guilty party, were three parts of data breaches in RAT. These angles are required for crime commission in light of the fact that their fleeting and spatial joining give important chances to carry out a crime. In this way, the ramifications of RAT are that a crime can possibly happen when those three perspectives are available (Pyrooz, Decker, and Moule Jr, 2015).

Much the same as a guardian is imperative to the prevention of data breaches, and different elements play in too. A recent report by the Healthcare Information and Management Society (HIMMS), on the accentuation of the significance of network safety, comprised of center gatherings included healthcare chief information officers (CIOs), chief technical officers (CTOs), chief information security officers and information technology (IT) directors. 67% of the gathering expressed that they focused on network safety to the mid or lower-mid level for their association (HIMMS, 2019; Howe et al., 2018). Mid or lower-mid level management finds it far more challenging to

have a dedicated IT staff or a specialized security team, which example, healthcare organizations are aware of the potential vulnerabilities yet lack the resources to fix those vulnerabilities (Alder, 2019; Sidhu, 2018). Reyns (2015) assumed there would dependably be aroused guilty party willing to carry out a crime if the correct open door shows up. This presupposition is the means by which another component, the rational choice theory, worked into this study's conceptual framework. Haimes, Horowitz, Guo, Andrijcic, and Bogdanor (2015) assumed that potential guilty parties ascertain their normal risks, costs, and advantages before executing a crime. Usage of formal strategies requires somewhere around a fundamental familiarity with circumstances that could be viewed as enticing. Consequently, to comprehend strategies better, one must likewise perceive the four properties that decide a reasonable assault target, in particular: value, inertia, visibility, and accessibility. Moon, Morash, Jeong, and Yoon (2015) contended an objective with high permeability, restricted inactivity, simple openness, and noteworthy esteem draws in a criminal. In an exhibit of their cozy relationship, the four properties effectively portray two parts of RAT, in particular, chances and an absence of capable guardians (Weisburd, Groff, and Yang, 2014).

Informal Strategies

Informal strategies center around giving data that conventional controls provide education on information security and create a security culture in the organization (Ghafir et al., 2018; Kuo et al., 2018). Moore and Frye (2020) contended these strategies are managed by giving training on data security to make a security culture in the association. In such a manner, management or guardians ought to give staff preparing to expand their

consciousness of the inside or outside danger (Safa et al., 2018). McGuire (2019), a specialist at Johns Hopkins, determined that offering extra instruction past the standard pre-execution preparation builds commitment from doctors and improves the nature of documentation in EHRs. Van Galen et al. (2018) researched the requirement for basic preparation to help the extension of telehealth patient consideration, and the outcomes exhibited the need to constantly offer training to help the developing necessities of medical care. Moreover, gatekeepers on this issue make a careful network in the association, which can assume a critical job in applying discouragement against insider or wrongdoers exercises. Security awareness programs set up a culture of security that is appropriate for an association (Sabillon et al., 2019).

Formal Strategies

Formal strategies are related to regulatory compliance and policies about data security (Muller and Lind, 2020). Stern et al., 2019 proposed that associations reliably uphold and impart data security approaches with the goal that security managers as gatekeepers promote workers see how to avoid insider or wrongdoers assaults. There ought to be clearness in the policies regarding satisfactory utilization of hierarchical assets, data, and frameworks, the utilization of special records, and the procedures for managing worker complaints. Additionally, all IT administration systems accessible to end users can use best practices and strategies to accomplish comparative advantages (Rouse, 2019a; Rouse, 2019b). What's more, the policies should diagram the ramifications for disregarding the normal guidelines.

Likewise, far-reaching Service Level Agreements (SLAs) ought to be set up to give guidance on the best way to cover data security breaches presented by insiders or wrongdoers (Ambre and Shekokar, 2015). The meaning of SLA boundaries is vital for both healthcare organizations and patients (Mazzoli, 2021). Consequently, in light of Terfas, the predefined SLA boundaries in the beginning phase of the SLA lifecycle can influence the entire SLA lifecycle and impact the degree of administration required (Terfas et al., 2018). The SLAs should portray checking abilities, administer the exercises of staff, and decide the dimension of confinements for getting to the customer's private, sensitive or classified data (Campbell, 2019; Shackleford, 2019). SLAs are important to ensure that organizations surpass or fulfill the required security guidelines; the SLAs should likewise affirm embracement to moderating controls to limit the danger of inside and outer data breaches. Another formal strategy is to set up procedures and policies for incident reporting; this strategy empowers staff to report any malicious action by their colleague (Aldawood & Skinner, 2019). Incident reporting should address the incident submitted by insiders or wrongdoers and ought to have a chain of escalation; they should lay out the essential specialists who settle on choices about a specific issue. This blueprint furnishes staff in an association with a component for revealing insider or pariah data breaches, furnishing IT administrators with open doors for starting the fundamental cures.

Security Strategies: Compliance and Regulation

Many years of exploration have uncovered the force of perception to empower quicker, more exact clinical determination and further developed results for patients

(Elhoseny et al., 2018). While executing protection and security controls inside a medical services climate, there should be a harmony between strategy assumptions and how the innovation is utilized (Berkeyheiser, 2019). Researchers admit that EMR breaches in healthcare are no longer just an issue of someone hacking into the hospitals ’computer system, but also an issue of negligence and non-compliance with formal security strategies, e.g., leaving an unattended laptop or iPad with unencrypted patient data or sending patient’s records to a wrong address. Employee training, communication, and motivation are key security strategies in preventing data breaches due to non-compliance. Lopez, Omizo, and Whealin (2018) identified four main components that contributed to successful training, (a) on-sight and face-to-face instruction, (b) training that involves the hands-on application of practices, (c) Including trainers who are practicing providers and thus familiar with work flow demands, and (d) using training topics tailored to the needs of the trainees. By better understanding and distinguishing these employee variables from the perspective of RAT, I expect to recognize factors from information gathering that could be utilized as strategies as a lens through which to view the perceptions of expanding guardianship and diminishing target reasonableness of individuals most in danger of exploitation from data breaches. When employees receive training and communication, they are more likely to believe that Information Assurance policies are beneficial to all parties involved Ganiga et al., (2020). They improve healthcare employees ’beliefs in the importance of EHR security. The research mentioned above leads us to identify security managers as guardians through the strict government regulations that enforce the protection of healthcare records.

Since the presentation of HIPAA in 1996, the US medicinal services division has dealt with approaches to enhance security for ePHI (Grachis, 2015). For healthcare services administrators, understanding the present condition of data security inside their associations and figuring out how HIPAA protection and security rules apply has turned into a best need. Organizations wind up taking a gander in danger administration projects to help deal with their hazard and boost openings (Clifton Larson Allen, 2013). The present condition of data security and IT Risk management frameworks (RMF) security strategy show both are still in the development organization. In an article about The State of Security and Risk Management in Healthcare, Dwayne Melancon, Chief Technology Officer for Tripwire, calls attention to that half of medicinal services and pharmaceutical associations are not utilizing any sort of formal risk evaluations, nor are they open to testing current presumptions. These components could make these associations be highly exposed and vulnerable to the expanding number of digital security dangers to their organizations (Valladares, 2014). Distributed denial of service (DDoS) attacks is one of the known digital security dangers where network packets overload the system with large amounts of fake data requests. This large amount of information blocks legitimate requests. The system's CPU, memory, and bandwidth are all overwhelming and cannot serve users (Chen, 2019). DDoS attacks cause serious problems such as B. Deny access to the system where the EHR resides. This prevents sharing of EHR records (Hughbanks, 2018).

The Ponemon Institute 2019 research report, *The State of Risk-Based Security Management in the US and UK*, noticed that associations still in the beginning periods of

risk-based security strategies have not yet encountered its advantages (Ponemon Institute, 2019). The report brings up the wariness from the organizations overviewed with respect to the advantages of chance-based security programs. Moreover, overviewed organizations put accentuation on the accompanying inquiries with respect to the incentive of a risk-based security strategy: (1) timeframe to actualize security patches (Blue & Furey, 2018; Shackelford, Mattioli, Myers, Brady, Wang, & Wong, 2018); (2) logging and monitoring for critical for incident detection (Agana & Wario, 2018; McGlade & Scott-Hayward, 2019); (3) number of records or documents distinguished as consistence infractions (Ahmed, Naqvi, & Joseph, 2019); (4) system hardening to minimize security vulnerabilities and threats (Applied Risk, 2019); (5) decrease in lapsed authentications (Herwono & El-Moussa, 2018); (6) decrease in administrative activities and claims; and (7) reduction in the number or level of end clients requirement activities as a proportion of adequacy of consistence with executed inward guidelines (Ponemon Institute, 2019). The report featured that reviewed organizations are as yet checking the viability of consistence to interior controls, understanding that the interest in time, assets, and cost to actualize the program must be talked about and have the aggregate help from administration through fulfillment.

Their duty regarding information assurance has social insurance organizations concentrating on what security frameworks are powerless against chance as patient information courses through their security strategy. The requirement for health care organizations to include chance administration systems and inside security controls keeps on developing as organizations take in more about their surroundings and the apparatuses

that can help with ensuring PHI. The advantage of RMF in the health services industry is very much characterized by protection controls that assist exhibit consistency with enactment, strategies, and quantifiable and enforceable security prerequisites. What's more, the linkage to healthcare security strategies that give a strong establishment to protection enhances undertaking wide safeguard top to bottom for security (O'Donnell et al., 2018).

Risk management frameworks (RMF) security strategies enable us to comprehend conditions, potential dangers, and dangers that make a presentation to assaults, a potential information break, or HIPAA infringement. An RMF framework describes how various functions of the IT operation relate to the mission. Its purpose is guided by four main principles: (1) Solidify what IT is trying to accomplish by articulating the vision and strategy of the IT organization, (2) Describes the objectives and priorities, (3) Provides a means to measure results and outcomes, and 4) Accountability (Lutchen, 2004). For medicinal services administrators, executing patient critical administration systems and controls helps to feature the significance of teaching workers that they are responsible while getting to health data. For IT experts, IT guides them to utilize chance evaluations appropriately to recognize and relieve potential security dangers can enable a business to oversee and line up with HIPAA Privacy and Security Rules (HealthIT, 2020).

As medicinal services organizations hope to assemble more secure situations, the necessities to execute instruments that give rules and interior controls help business partners encourage a culture that keeps data security as a point of convergence while

actualizing new items and including new business connections that will require the sharing of patient health data.

Sound security strategy development and management starts and finishes at the top official dimension of corporate and government associations. Constraints and confinements to how data is overseen and spread are held in the created hierarchical strategies and orders. So, the very idea of security strategy charges the consistent audit and update of arrangement and arrangement systems (Hedda et al., 2018). Execution of arrangement is intensely impacted by the regulations and needs of ranking directors inside the association. Hence, best business practice in security strategy administration is almost altogether connected to proactive administration and venture mindfulness preparing. In like manner, a successful security strategy may require the expansion of established national standards or provide interoperability of multiple frameworks (Collier, 2018; Kadam, 2007).

Health Information Exchange

Criminal behavior is significantly influenced by the nature of the immediate environment in which it occurs. The RAT environmental perspective depends upon the principle that all behavior results from a lack of vision and framework for interoperability. The framework is not just a passive backdrop for criminal behavior but rather, it plays a fundamental role in defeating the risk of data breaches. Thus, data breach events result not only from a motivated offender; they are equally caused by the absence of capable guardian enforcement of a framework. The Health Information Exchange (HIE) framework explains how the structure provides an environment that

affects behavior and why some environments are more susceptible to data breaches. Standardization is usually done by the EHR system but is facilitated by the electronic medical record system (Howe et al., 2019). An EHR utilizing HIE innovation empowers the chosen medical care partners to encounter higher patient standards guidelines through electronic participation in a patient's continuum care model, including numerous providers (Heyde, 2018; Hatef et al., 2019).

The HIE broad vision and framework for interoperability is to give care offices the capacity to course EHRs among various medicinal security strategies that can have federated, centralized, or hybrid architectures (Walker, 2018). The particular pace of information trade inside associations and between associations likewise will, in general, increment with the execution of EHR frameworks (Sieck, Pearl, Bright, &Yen, 2019). The united structure requires nearby patient information stockpiling at every medicinal services association to guarantee a more elevated amount of information security and protection. The conveyance of data electronically requires expanded security conventions and insurances also, as recognized by a few government and state acts in regards to the putting away and trade of individual and wellbeing-related data for patients (Shi et al., 2020). In the event that an outside association needs to get to understand data, it must recover it from the health care organization (HCO) holding the data. What's more, to get to the data, the element must be an individual from affiliation, and in the meantime, must invest in offering the data to different individuals from the system. The members in this strategy are regularly considered in charge of guaranteeing that data is gotten to by the approved individuals, as it were.

The incorporated HIE strategy, additionally alluded to as the merged model, includes putting away all health data in a solitary information vault or distribution center (e.g., cloud). Every individual from the brought together HIE strategy is relied upon to transmit patients ’health data to the remote vault, where the data is safely put away. The health data is consistently refreshed through interfaces associated straightforwardly to every human services association’s data vault keeping in mind the end goal to enhance security and secrecy. These interfaces normally consider unaltered patient data stream to the focal expert. At whatever point a part association demands get to, it is subjected to pre-characterized interesting patient identifiers previously being approved.

The mixture HIE strategy joins the components of incorporated and combined systems. This strategy holds huge record identifiers alongside demands for persistent information dispersed over a system. To guarantee security and protection, access to the information is regularly subject to stern measures. All things considered, a record locator scratch is routinely utilized not exclusively to accumulate health data yet additionally to exchange it to the human services association. The framework utilizes calculations inside the system applications to guarantee positive patterns in social affairs the patient data put away in the remote storehouse.

HIPPA

The occurrences of data breaches in time and space are non-random. The RAT criminal behavior is dependent upon situational factors; data breaches are patterned according to the availability of environments. Crime will be concentrated around crime opportunities the Health Portability and Accountability Act (HIPAA) and other

environmental features that electronic health data (ePHI) introduced criminal activity (Newman, 2019). Crime rates vary from suburb to suburb and from street to street and may peak at different times of the day, four different days of the week, and different weeks of the year. The purpose of incorporating protection and security rules is to identify and mitigate potential data breach patterns.

In 1996, Congress placed HIPPA into law with double objectives of making medicinal services conveyance progressively proficient and expanding the quantity of Americans with medical coverage inclusion (Patil and Chakrabarti, 2020). Congress needed to set a security strategy for transmitting electronic health information for individuals who changed or misfortune their activity and required an approach to exchange or hold medical coverage. HIPAA was the response for giving an approach to organizations and individuals to exchange electronic ensured health data (ePHI) in any shape, for instance, electronic, paper, or oral data between substances (Jalali & Kaiser, 2018). Nonetheless, HIPAA doesn't order explicit innovations. The techniques and innovation executed are passed on to the attentiveness of the covered medical care organization (Schmeelk, 2019).

The inclusion of the US Department of Health and Human Services (DHHS) helped HIPAA advance throughout the years to incorporate protection and security rules. The joint effort with people in general and private division helped DHHS make HIPAA norms that would enhance the administration and security of PHI. In 2003, the Privacy Rule was presented, giving human services organizations definitions and approaches for security and approval gauges to access health data (Pritchard, 2018; Vidich, 2021). The

Privacy Rule built up the accompanying identifiers viewed as PHI: (1) names; (2) address; (3) birth dates; (4) phone numbers; (4) email address; (5) standardized savings number; (6) Medical record number; (7) health plan recipient number; (8) gadget identifiers and sequential numbers; (9) web widespread asset locator (URL) and web convention (IP); (10) full-face photographic picture; (11) biometric identifiers.

In 2005, the Security Rule for HIPAA helped characterize how medicinal services organizations guarantee security gauges are connected to PHI. The new standard suggested that social insurance organizations actualize regulatory, physical, and specialized shields to ensure ePHI. The managerial shield required the assignment of security duty to a security officer and security standards preparing for representatives. The physical shields expected organizations to oversee access to data frameworks containing ePHI. Specialized protections proposed robotized forms for human services organizations to scramble ePHI amid transmission (The University of Chicago Medical Center, 2010). Security Rule for HIPAA does not prevent social engineering attacks which comprise one of the primary attack vectors used on healthcare (Arapi, 2018; Patel, 2020; Ward, Banks, & Pritam, 2018).

With HIPAA Privacy and Security Rule set up by 2005, the Office of Civil Rights (OCR) alongside DHHS could energize and uphold HIPAA consistency benchmarks on human services organizations (Bennington, 2020). On the off chance that a medicinal services business is resistant, DHHS-OCR can explore to decide whether the business has abused the protection or security rule (Raths, 2020; Thomas & Ingargiola, 2021). OCR can demand common money-related punishments to those social insurance organizations

that are chargeable of the infringement and access fines extending from $100 for unconsciously abusing HIPAA up to $1.5 million for persistent carelessness (Privacy Rights Clearinghouse, 2019; Sheffer et al., 2019).

HIPAA necessitates that social insurance organizations direct hazard appraisals intermittently. To help human services organizations, DHHS-OCR has built up a security chance evaluation (SRA) apparatus to help direct a social insurance business through leading and effectively archiving a hazard appraisal. The SRA is accessible allowed to a social insurance business through the HealthIT.gov/security-chance evaluation site (DHHS, 2014). DHHS-OCR supports consistency from human services business to lead hazard appraisals on a continuous premise to remain refreshed with security assurances. Since HIPAA Security Rule and EHR motivation program have the chance examination and hazard evaluations as key necessities, human services organizations are encouraged to start the hazard the boarding procedure before the start of EHR answering to help to dispense with security insufficiencies (HRSA, 2014).

In 2009 the Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted to promote the use of Information technology in healthcare organizations (Everson et al., 2020). On January 5, 2021, previous President Donald Trump signed HR 7898, otherwise called the Safe Harbor bill, that altered the HITECH Act to require the Department of Health and Human Services (HHS) to boost best practice network protection for meeting HIPAA prerequisites (Davis, 2021). The alteration to the HITECH Act expected HHS to consider assuming practices had completely perceived that network protection rehearses set up when researching an

information break (Colicchio et al., 2019). Under the new law, HHS would consider whether an association had been utilizing perceived HIPAA online protection best practices to consent to the HIPAA Security Rule (Danielson, 2021).

Congress passing the law for HIPAA perceived the significance of ensuring health records while on the move between substances (Nass, Levit, and Gostin, 2009). The US human services part is presently in charge of the administration and security of ePHI when in their ownership. The new Privacy and Security Rules concentrated on shielding patients from the unapproved introduction of health data and permitted DHHS-OCR to review social insurance organizations to guarantee consistency with the necessities, gauges, and systems (Nass, Levit, and Gostin, 2009). Title I of HIPAA is concerned with the portability of health insurance and protecting the rights of workers between jobs to ensure health insurance coverage is maintained, which has nothing to do with the HITECH Act. However, there is a strong relationship between HIPAA Title II and HITECH.

HITECH

RAT relates to understanding the role of criminogenic environments and being aware of the way that a motivated offender is prevented by patterns mitigated by the Health Information Technology for Economic and Clinical Health (HITECH) control and prevention of data breaches (Center, 2020). A couple of studies have zeroed in on measuring the elements that depict the peculiarities of “meaningful use” of EHR frameworks (Bui et al., 2018; Kim et al., 2019). Understanding the usability and the significant utilization of the EHR relying upon the size of the association has a major

impact on its acknowledgment from medical services experts and different clients (Kooienga, 2018). The HITECH mandate also included penalties for non-compliance with meaningful use requirements (Wang, Wang, Shen, Rastegar-Mojarad, & Liu, 2019). Stage 1 certification was 2011, Stage 2 was postponed to 2014, and Stage 3 requirements were scheduled for 2017 to include computerized order entry, implementation of e-prescription, and recording of clinical details such as vital signs and smoking status (Bae, Ford, Kharrazi, & Huerta, 2018). This key provision allows capable guardian enforcement to concentrate resources on particular crime problems in particular locations. Incorporation of the criminogenic aspects of the targeted environment can reduce the incidence of data breaches in that location. HITECH criminology mitigation and crime best practices combined provide oversight for legitimate obligation for rebelliousness by medicinal services organizations.

The HITECH was presented as part of the American Recovery and Reinvestment Act (ARRA) on February 17, 2009. US President Barack Obama passed the AARA to spare and make employments, give alleviation programs, and put resources into US framework, health, and instruction for zones most influenced by the 2008-2009 US financial subsidence (Savas, Smith, & Hay, 2019). The HITECH Act concentrated on the medicinal services industry's selection of electronic health record (EHR) security strategies to help social insurance organizations in the administration and security of ePHI.

The HITECH Act fills in as a key arrangement to HIPAA by giving a few activities that reinforce the protection and security rules consolidated in 2003 and 2005:

(1) money related motivating forces given to medicinal services organizations that actualized EHR; (2) the HITECH Act expanded the potential legitimate obligation for social insurance organizations for resistance; (3) common and criminal authorization of the HIPAA rules (DHHS-Office of Secretary, 2009). DHHS's contribution to the HITECH Act gave the office the specialist to enhance social insurance quality and security with the utilization of innovation. Human services organizations that actualize health information technology (HIT) intended to anchor ePHI when transmitted could do as such as indicated by national models set up by HIPAA (HRSA, 2014). Clinical decision support systems (CDSS), telemedicine, mHealth, and EHRs are instances of HIT innovations (Serova and Guryeva, 2018).

With EHR security strategies expanding in social insurance organizations, there is a decrease in therapeutic blunders and enhancements in patient consideration. For social insurance organizations that couldn't bear the cost of the speculation for an EHR, the money-related motivations helped influence the change to happen sooner than at first foreseen. The consequences for the general medicinal services correspondence indicated enhanced clinician fulfillment when taking care of and overseeing ePHI.

The HITECH Act furnished DHHS with more oversight for legitimate obligation for rebelliousness by medicinal services organizations (DHHS-Office of Secretary, 2009). The appropriation of HITECH came with difficulties as medicinal services organizations attempted to make successful and proficient human services frameworks that met the necessity of HIPAA and HITECH (Landi, Healthcare Informatics, 2015).

The change to powerful electronic health record security strategies should help human services organizations better comprehend the duty and risk to anchor ePHI.

The difficulties that health services organizations look inside the part are fixing to the administration and capacity of PHI as it moves to start with one substance then onto the next. For a healthcare organization that is assigned as a human services supplier, HHS sees that business as a Covered Entity (CE), which is an individual or business that gives medicinal services administrations to a patient (Center for Medicare and Medicaid Services, 2013). The CE is in charge of overseeing and transmitting ePHI in a sheltered and secure condition and keeping an unapproved individual or business from getting to the PHI outside of approved channels. A CE has an association with outside administrations known as business partners (BA). A BA is an individual or business that gives administrations to the secured element, enabling the BA to access the PHI by the administrations given. A human services clearinghouse (HCH) interfaces with the CE as an element that is permitted to encourage the handling of health data got from a CE in a nonstandard configuration that does not require the data to meet industry standards when transmitted. These administrations may incorporate charging or preparing of data that gives HSH access to PHI. In these cases, the electronic type of PHI can move between two or every one of the three recognized human services organizations.

Inside the US human services part, organizations that give administrations are required to pursue HIPAA protection and security rules. The HHS-OCR has fabricated a security strategy that makes responsibility among the individuals who are engaged with patient consideration and the individuals who give administrations and innovation

explicit to tolerant consideration. For instance, doctors enter quiet data notes in a PC or PC into an EHR, and human services suppliers are urged to scramble ePHI put away on the PCs and workstations. Additionally, because of their long life cycle, these clinical gadgets are utilized persistently for quite a long time; however, the gadget might convey obsolete, unpatched, unreliable, or unsupported programming or equipment (Monson, 2019). This convention has permitted HHS-OCR to lawfully uphold the strategies set up by advising and playing out a HIPAA consistency review on an element that winds up getting to PHI (Snell, HeathIT Security, 2015). Altogether, for a human services business to conform to the prerequisites of HIPAA, said organizations ought to be focused on understanding the significance of insurance and security of the data that goes through their data frameworks.

With best practices, a human services business endeavors to join data security (IS) best practices and hazard the board structures inside the organization by executing arrangements and tenets with the objective of teaching and enabling representatives to settle on the correct choices when taking care of PHI. For instance, the data innovation (IT) division of a social insurance organization will direct hazard appraisals to see how information streams all through healing centers ’electronic medicinal record (EMR) frameworks (Roney, 2012). At the point when an association hopes to utilize chance administration rules like ISO 31000:2009, the association can give standards, structure, and procedures for overseeing hazard that enables the association to improve the probability of accomplishing goals for tending to chance issues, enhancing its odds of

recognizing dangers, and dispensing assets for hazard treatment (International Organization for Standardization, 2005).

The strategy for IS best practices is vital for health services organizations in light of their communication with ePHI. It ends up basic for a social insurance business to execute IS administration and consolidate security strategies to guarantee the development of data is in accordance with the corporate arrangement. The IT division ought to have encryption programming on all organization PCs, PCs, and tablets, notwithstanding understanding where PHI is found and how it is being utilized (Snell, HeatlhIT Security, 2015). The corporate approach ought to pursue HIPAA agenda prerequisites that workers change passwords and comprehend the significance of consistency and moral obligation (Alohali et al., 2018; Mun et al., 2018).

The significance of realizing how to characterize IS security strategy inside a medicinal services business is an imperative advance to set up administration strategies to which a business can follow. The obligation of supporting and authorizing the IS administration strategy has a place with the top managerial staff and senior administrators (Joshi et al., 2018). Senior administrators can fill in as a guide for the executives and representatives to actualize administration strategies that will engage the association to address issues where health data is helpless against introduction. For instance, a medicinal services business should know where electronic health data lives, know which office representatives approach electronic health data, and can evaluate hazards (DHHS, 2010).

Security Strategy: Technical

Healthcare organizations have a few security apparatuses accessible today that can help with the assurance of EHR data breaches through a security strategy. Abu et al. (2018) presented four issues and difficulties in making interoperability of numerous stages: thread data overload, the dependency of threat data, legal issues, and incompatibility of different platforms. Other contributing elements are with the framework that comprises associated PCs and different gadgets where working frameworks and conventions have huge contrasts (Offner, Sitnikova, Joiner, and Macintyre, 2020). Medicinal services organizations that consider data security techniques within a security strategy help themselves plan and oversee hazards to diminish the conceivable outcomes of an information break or unapproved access to the system. The accompanying apparatuses are a couple of countermeasures that medicinal services organizations may use in a security strategy to decrease the danger of data breaches and information ruptures (Open Web Application Security Project, 2020).

The Health Information and Management System Society (HIMSS) is a non-benefit HIT proficient enrollment association giving the medical care community an initiative and expert improvement inspired by the utilization of electronic computerized HL7 health innovation developments (Gagnon and Stephen, 2018; (HIMSS, 2019). Zinszer, Robyn, Bates, and Buckeridge (2013) comparatively guaranteed that an ideal security strategy with joining and interoperability procedure is through programming extensions and interfaces. An elective way to deal with the security strategy of EHR

usage offered by Cegielski, Bourrie, and Hazen (2013) originated from a four-round Delphi concentrate to acquire an arrangement of issues influencing IT official choices in embracing rising IT innovations into corporate IT system. The main issue examined by Cegielski et al. was the capacity to increase upper hands through innovation use, identified with the second issue that was about the capacity to manage upper hands utilizing innovation. The third issue Cegielski et al. talked about was the security of the innovation, and the fourth issue related to acknowledgment of innovation by clients and customers. Cegielski et al. suggested that pioneers consider the four issues in IT methodologies utilized by CIOs.

A large number of proposed EHR security strategies exist because of the absence of institutionalization and uniqueness of every medicinal supplier. He and Yan (2014) recommended a Simple Network Management Protocol controlled by the Internet Activities Board; the convention is a formally dressed interface fit for trade with large numbers of various system hardware, making an available and reasonable program. The strategy for usage rearrangements was the use of existing foundations and applications (He and Yan, 2014). Huerta, Thompson, Ford, and Ford (2013) alluded to the Big Bang hypothesis of EHR usage, with an emphasis on making a strategy operational within one year. Be that as it may, this methodology prompted the distinguishing proof of a low aggregate profitability factor; in light of these discoveries, Huerta et al. contended that IT aftereffects of effectiveness, lessened cost, and enhancing medicinal services conveyance might be conflicting and unsuccessful.

McAlearney, Hefner, Sieck, and Huerta (2015) led 45 interviews with six U.S. social insurance associations intentionally chosen in light of effective walking EHR execution. McAlearney et al. 2015 finished six center gatherings with 37 doctors who gave far-reaching information to deductive and inductive examination that prompted answers to their exploration inquiries concerning IT security strategies. McAlearney et al. 2015 announced three procedures that rose up out of their information investigation: (a) utilization of existing HIT writing that underlines execution facilitators, (b) center around work process, and (c) join basic administration factors that encourage usage. Adding to the discoveries, Johnson and Lederer (2013) asserted that business pioneers assess security strategies through eight IS procedures detailed by Johnson and Lederer: (a) forcefulness, (b) examination, (c) outside protectiveness, (d) inner preventiveness, (e) futurity, (f) creativity, (g) expert liveliness, and (h) hazard.

Based on whether wrongdoer, target, and gatekeeper statutes played a role as influencing factors in creating clarifications for data breaches within the RAT theory, technical security strategies correlate specific mechanisms the wrongdoer must defeat. Silvius and Stoop (2013) stated that the accomplishment of key data frameworks is arranging and significant in guaranteeing the arrangement of data innovation frameworks and administrations with business methodologies. Arranging and strategizing for consolidated adequacy requires broad coordination and an incorporated vital approach that conquers the challenges and boundaries to the selection of EHRs (Silvius and Stoop, 2013). However, Johnson and Lederer (2013) broadcasted that CEOs and CIOs as gatekeepers have alternate points of view on the best system to seek after in EHR

execution. Gatekeepers ’viewpoints rotate around proactive investigation, though gatekeepers see imaginativeness and forcefulness procedures as essential roads for EHR execution (Johnson and Lederer, 2013). Joined contributory assertions among CEO and CIO may result in a successful by and large methodology for the test of EHR execution (Johnson and Lederer, 2013).

Access and Identity Management

Offenders are going to choose the target that shows the least amount of challenge. An assumption that can be drawn from routine activities theory then is that the offender makes a rational choice to choose the target that is least restrictive to achieving his or her criminal goal. Access and identity management mitigates the risk of the person who walks with their eyes to the ground unaware of their surroundings, or the person that makes the availability of data breaches for the motivated offender the chance of them succeeding is highly possible (Harmon, 2018).

Access and identity management appear to be best suited for IS managers to include in their technology strategies. Authentication is regularly the initial move toward affirming the client is approved to get to the framework. The essential confirmation technique to access organization assets is a username and secret word. Secret phrase creation and execution has been a security Achilles heel for more than twenty years, in view of poor secret phrase choice, the executives, or assurance. In 2012, a powerless framework manager secret phrase caused the break of the Utah Dept. of Technology Service’s (DTS) server, uncovering 780,000 Medicaid tolerant records likewise noticed the most well-known passwords still being used today are “1234567” and “secret phrase.”

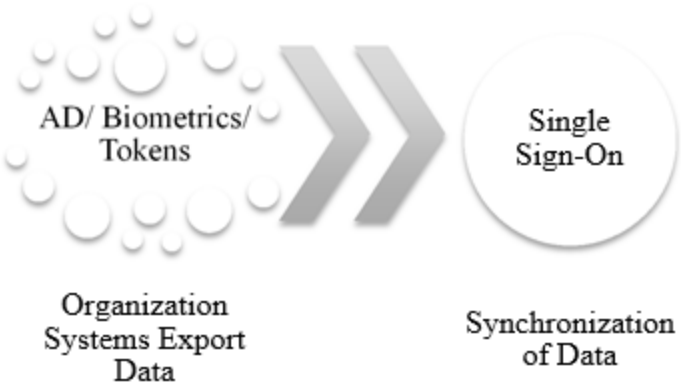
In an investigation of how safely overseen PHI is in clinical research, Billingsley (2019) split the passwords for in excess of 2,000 records in a 24-hour time span. When a common security breach occurs, compromised data such as usernames and passwords are often reset or changed; however, a patient simply change their information, such as their social security number is not available (Brewer, Hejjaji, Ip, Ta, & Wu, 2019; Cardlogix, 2018; Neveux, 2020; Spaniel & Eftekhari, 2020). The documents all contained feeble passwords utilizing area names, creature names, vehicle brands, and number successions (e.g., 123) (Billingsley, 2019). Single-factor authentication includes some innate security worries that managers should represent (Gogan, 2018; Greevy, 2018). System administrators who carry out two-factor authentication apply two elements to affirm the personality of the end client (Chuang et al., 2018). Happa et al. (2019) showed that solid passwords and multifactor authentication are significant strategies to relieve the danger of simple admittance to hackers. Associations keep on permitting the utilization of frail passwords with intricacy decides that just require eight characters and don't need upper and lower case letters, numbers, or unique characters in the secret phrase (Stedman, 2019). To overcome frail passwords, associations generally embrace the Public key framework (PKI) to oversee digital certificates for authentication and encryption (Marciano, 2018). Administrators additionally utilize PKI to help token and key-based confirmation as an option multifaceted system (Lowe, 2018; Marciano, 2018). As indicated by Tariq et al. (2018), NIST Special Publication (SP) 800-53 is a controlled registry coordinated inside control families to be applied in a government data framework (de Vaulx, Simmon, & Bohn, 2018). Inside the data security domain, associations use

biometrics for distinguishing proof supporting validation and access control. Biometric identifiers are the particular, quantifiable attributes used to mark and portray people (Thakkar, 2018). Behavioral biometric authentication is the patterns of behavior that a person establishes naturally, including typing rhythm, gait, walking speed, web-browsing activity, and even voice (Buriro, Crispo, & Conti, 2019). Administration of access management by security managers, gatekeepers can mitigate the risk of data breaches through weak passwords and more easily enforce the National Institute of Standards and Technology (NIST) requirement for stronger and more effective authentication through a biometric Single Sign-On (SSO) security strategy (Madsen, Koga et al. 2005).

SSO is a property of access management of multiple related yet independent software systems which complies with HIPPA and the HIPAA Security Rule. The SSO property for HIPAA-covered entities also complies with Technical Safeguards for Mobile Devices to "Implement technical security measures to guard against unauthorized access to electronically protected health information that is being transmitted over an electronic communications network." With this property, a user is empowered to log in to a workstation by entering a username and secret key toward the start of a move and afterward streamlines all consequent logins amid that move (Gellert et al., 2017). Generally, one piece of information is all that is required for SSO's single-factor authentication. Bigler (2004) attested that SSO could be joined with different advances, for example, biometrics, to improve its capacity to convey more prominent security. For instance, SSO can work with an association's Microsoft Active Directory administrations, biometric gadgets, or potentially tokens (see Figure 1).

Figure 1

SSO Working With Microsoft Active Directory, Biometric Devices, and/or Tokens



The validation idea driving SSO is basic; to rapidly verify to frameworks in the interest of the end-client, paying little heed to whether it keeps running on a server, workstation, or web as expressed by Murphy (2006) and Roesch and Henry (1997). SSO ought to dispose of the requirement for recording passwords, as the specialist just requires the remembrance of one secret key to access assets. Hope and Zhang (2015) analyzed client fulfillment with SSO and PC application meandering inside crisis divisions. The PC application meandering enables doctors and crisis specialists to sign into one PC and utilize an identification to access different PCs in the office (Hope and Zhang, 2015). To remove credential redundancy and prevent fragmented login, a new approach for federating identity management of cloud service providers has been proposed (Intenzer, 2020; Kumar & Goyle, 2019; Mukherjee, 2019). Identity federation involves establishing agreements between cloud service providers to recognize each other's identities in a federated domain. This agreement defines the mapping of a user's identity when they transfer from one administrative domain to another. In this model,

when a user is authenticated to access one service provider's system, their identity is automatically confirmed with SSO two-factor across multiple domains. The SSO, combined with utilizing the second type of validation, ID identifications, expanded the security of patient information and the fulfillment of the clients. SSO utilizes two-factor validation, which utilizes something has known (secret word) and something you have (ID identification). Bigler (2004) stated that both biometrics and SSO technology could be leveraged to achieve two-factor authentication.

Two-factor authentication is a property of identity management**.** At the point when a client signs into a PC framework with a solitary secret key, get to is conceded to every one of the assets, including touchy information. Notwithstanding the additional layer of safety given by 2FA to build the framework of the framework's assault opposition, the 2FA ease of use research discoveries uncovered a combination of qualities and shortcomings in regards to the 2FA cycles and gadgets (Colnago et al., 2018; Das, Dingman, and Camp, 2018). This strategy works for general assets. For instance, a doctor may have a need only a fingerprint reader in his office; as all things considered, the staff member will dependably have the option to give a unique finger impression from any of the enrolled digits. Then again, somebody in the emergency room may need a functioning RFID proximity card. A functioning RFID closeness card would enable a doctor or medical attendant to rapidly get to the framework while never contacting it. This situation would be perfect, as it would permit end-clients to appreciate an enhanced confirmation succession. According to Bigler (2004), not only is this a significant security risk for the organization, but it is also a generator of excessive calls

placed to the IT helpdesk. End-users call requesting assistance to access locked resources, thus causing a loss in productivity due to the inability to access locked systems. In any case, delicate information, for example, electronic wellbeing data, needs a second layer of assurance. Koch and Moslein observed different software vendors offer single-sign-on solutions for intranets, and the solutions are mainly based on (X.500) directory services or are accessible via the lightweight directory access protocol (LDAP). Leveraging services already provided by existing Identity Provider (IdP) practices are more efficient and cost-effective than attempting to replicate this infrastructure on a per-application basis. With two-factor confirmation, clients must give another verification factor outside of their secret key. A second confirmation strategy can be a password that changes frequently or a unique biometric finger impression per user. Two-factor verification secures delicate information by driving somebody to know both the secret word and the second validation strategy. Furthermore, steps like taking out shared passwords, halfway login all client movement, and allocating legitimate benefit level to clients is fundamental. Once biometric data has been appropriately gathered, a trust is set up.

Trust connections are a key part of SSO innovation. Numerous parties can accomplish a trust connection because of appropriate coordinated effort, just as correspondence. For instance, client A trusts another (client B) is the consequence of time spent watching, client A comprehends and recognizes communicated conduct by client B (Lin, Vullings, and Dalziel, 2010). As indicated by Lin et al. (2010), trust connection evolution can have a huge impact because of observable properties existing in trust connections between parties. SSO basically builds up trust with every one of the clinical

applications for which it is designed. Therefore, unidirectional trust permits SSO to get to every one of these applications for the specific doctor and additionally nurture who is attempting to deal with patient information.

Based on whether wrongdoer, target, and gatekeeper statues played a role as influencing factors in creating clarifications for data breaches within the RAT theory, access and identity management correlates SSO and two-factor authentication as the mechanism the wrongdoer must defeat. In a medical clinic condition where doctors sign into different PCs once a day, two-factor verification utilizes the ID identification as the second type of confirmation. Another verification strategy is to have the confirmation sent to a cell phone, where the doctor taps their gadget to verify. Tipton, Forkey, and Choi (2016) caution that if a malignant client accessed the cell phone, that client could get too persistent graphs and individual data. While two-factor identification functions admirably inside corporate dividers, Schneier (2005) trusts two-factor confirmation does not work or is powerless to assaults on remote frameworks. Schneier (2005) additionally trusts two-factor validation can be assaulted utilizing a man-in-the-center assault, where the assailant shows a phony site that traps the client into entering their qualifications to access data. Another assault is a trojan assault, where the assailant introduces a trojan on the injured individual's PC. Trojans enables the assailant to piggyback on the session to open the risk to data breaches.

Data Segregation

The virtual environment is seen as one in which there is 'zero distance' between its points that entities and events cannot be meaningfully located in terms of spatial

contiguity, proximity, and separation. Everyone, everywhere, and everything is always and eternally ‘just a click way.’ Access control models give undeniable level, area free, and execution autonomous reference models for the engineering and plan of access systems (Lowe, 2018). The viability of RAT as a role-based access control (RBAC) model for data breaches begins to look decidedly crucial, given the Static Separation of Duty (SSD) and Dynamic Separation of Duty (DSD) model’s aforementioned dependence on convergence and separation to explain the probability of data breaches.

Users can, without much of a stretch, acknowledge information trustworthiness in single frameworks; however, distributed computing requires the utilization of a populous database to store information for various patients; therefore, it is trying to guarantee information respectability (Hong et al., 2018). Information respectability and isolation idea as the stronghold of delicate data against unapproved creation, adjustment, or erasure. Subsequently, approval is critical to ensuring information honesty; it guarantees that just approved staff can get to delicate data. One method of assigning access to delicate data is with role-based access control (RBAC).

RBAC is overseen at a dimension that relates near the association’s structure. Jobs inside the RBAC procedure are appointed to a client dependent on the capacities they have to perform. Jobs are characterized by occupation competency, expert, and obligation. An example of jobs in a medicinal organization may be Customer Service, Claims, Finance, and Legal. Jobs, as per Ferraiolo and Kuhn, are gathering focused, and for every job is a lot of exchanges designated the job kept up. As far as possible, the

insider risk since the client is just ready to get to information for which their job is conceded.

Several role-based access control models have been developed in recent years that have expanded on and standardized the core ideas behind RBAC. One of the most notable is the effort by the National Institute of Standards and Technology (NIST) to create a standardized template for which the majority of RBAC implementations can be based and expanded upon. Rashid et al., (2020) propose a core RBAC map together the five basic elements of a role-based access control system (users, roles, objects, operations, and permissions) to assign users to roles and roles to permissions, where permissions are in turn mapped between operations and objects. User sessions are also present in the Core RBAC model, allowing users to activate a subset of roles they have been assigned in a given session.

Static Separation of Duty (SSD) relations extend the Core RBAC model to enforce simple separation of duty policies during user role assignment. Sets of two or more conflicting roles and the maximum cardinality of the intersection of users ’roles with such a set are maintained in the system to represent an organization’s SSD policy. For example, an organization may create a policy that limits a user to being assigned to at most two of three roles involved in the process of authorizing payments. The NIST model also allows these SSD policies to be applied to Hierarchical RBAC models by having SSD constraints inherited alongside role permissions.

Dynamic Separation of Duty (DSD) relations also extend the core RBAC model to enforce an organization’s separation of duty policies. However, unlike SSD, DSD

constrains the active permissions a user may be indirectly assigned rather than their role assignment by limiting the roles a user may have acted together in a single session. As with SSD, sets of conflicting roles and maximum cardinalities are used to represent the organization's DSD policy. However, in this case, the intersection is between the conflicting roles and the user's active roles in a session rather than their overall role assignment. For example, if a user has both the role of the patient (allowing a user to view their own health record) and the role of doctor (allowing a user to view their patient's health records and update records to approve a treatment), DSD would not allow such a user to activate both their patient role and doctor role at the same time, preventing them from being able to approve treatments on themselves, while still giving the user the flexibility to view their own record and perform their job in regards to their patient's records.

EHR systems have some level of separation of duties; ordinary strategies to keep up information uprightness, for example, hypertext exchange convention, is improbable. In this manner, accomplishing information respectability happens by actualizing it at the Application Programming Interface stage (Hemalatha, Jenis, Donald, and Arockiam, 2014). Then again, understanding this methodology could additionally confound safety efforts by making potential vulnerabilities in the API innovation or the API stack itself. These vulnerabilities give assailants chances to block delicate information and alter it, bringing about further information debasement or burglary (Hemalatha, Jenis, Donald, and Arockiam, 2014).

Based on whether wrongdoer, target, and gatekeeper statues played a role as influencing factors in creating clarifications for data breaches by data leakages within the RAT theory, data segregation correlates a security manager as a gatekeeper overseeing a provisioning team of the health system. The security strategy for EHR administration must almost certainly isolate information from numerous patients by a gatekeeper. Malevolent users or wrongdoers can utilize application vulnerabilities to create parameters that can sidestep security checks and give access to client data (Hemalatha, Jenis, Donald, and Arockiam, 2014). Security managers (gatekeepers) could test and approve information by utilizing evaluations, for example, uncertain capacity, information approval, and SQL infusion injection flaws (Towbin, 2019). Vulnerabilities related to these tests may pick up assailants ʾunapproved access to a customerʾs delicate information. The event of this security issue was because of defects in session designation, and it showed the significance of information isolation to forestall data leakages.

Encryption Management

The third element of RAT is the absence of a capable guardian. The term ‘capable guardian’ is used widely; it may include the owner of the property (in the context of patient record database repositories, the public key account holder) or any other individual that has the potential to discourage offenders. One of the applications of RAT is in situational crime prevention. Although target hardening measures for the property are usually physical, such as the implementation of locks and barriers, target hardening is also used in data breach prevention, for example, the use of encryption.

The encryption management dimension considers the importance of encrypting data to minimize possible data leakage, specifically relevant in the context of patient record database repositories. A necessity of HIPAA for ensuring ePHI is for a medicinal services business to fuse encryption a piece of their security and risk management strategy. The burglary of decoded convenient gadgets, for example, workstations, tablets, and cell phones represented 39% of security occurrences in social insurance, and 78% of the records traded off in security ruptures (Terry, 2015). Convenient gadgets are effectively lost, lost, or stolen, and in spite of the fact that these gadgets are secret phrase secured, the information that lives on them can be seen in clear content should somebody have the apparatuses to extricate the data. Information encryption can be connected to the record/envelope level, parcel level, and entire circle. Every technical strategy has benefits over the other; be that as it may, encryption on any dimension has disadvantages to information get to.

Identity-based encryption (IBE) is a kind of public-key encryption plan utilizing pair-based cryptography (however, a few plans exist which utilize different techniques, for example, quadratic residues (Cocks, 2001), which uses a plain content public key, for example, an email address or space name. In a perfect world, a confided third party, alluded to as the Private Key Generator (PKG), would be entrusted with creating and safely circulating private keys to their proprietors. For instance, a PKG may be doled out to designate private keys relating to a public key comprising of a client's email address upon solicitation.

A few cryptosystems have been based on the idea of IBE, including the Attribute-Based Encryption (ABE) conspire first presented by Sahai and Waters (2005) as a major aspect of their Fuzzy Identity-Based Encryption cryptosystem (Sahai and Waters, 2005). ABE enables an entity to encrypt a file to such an extent that lone clients with a particular arrangement of properties may decrypt the data. For instance, an emergency clinic may wish to constrain access to a record to staff with the arrangement of attributes {“doctor,” “primary-care-provider,” “staff”}. This is made conceivable through ABE by issuing a private key (their “identity”) to every staff member made incompletely out of their attributes of appointed traits so that intrigue between different workers does not allow a key containing a bigger or joined attributes of properties. Medical staff workers are then restricted to decoding just messages encoded with some subset of their attributes.

Modernistic research in ABE has prompted a few improved plans which upgrade the multifaceted nature conceivable in ABE get to attributes including; empowering a restricted type of role-based access control. Key-Policy Attribute-Based Encryption (KP-ABE) (Goyal, Pandey, Sahai, and Waters, 2006) empowers attribute-based policies to be implanted in the client’s private key, enabling them to decrypt files encrypted with attributes coordinating their key’s policy. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) develops ABE to include variable attributes and access policies encapsulated in the ciphertext, which bolster fuzzy Boolean operations including greater than, less than, less than or equals, and greater than or equals, as well as other Boolean statements. For instance, one client might be doled out the attribute “room = 2020” in reference to their office number, while another client “room = 1020” and a file may then be encrypted

with the policy “room ≥ 2000 AND room < 3000” to permit just clients on the second floor (assuming room numbers begin with a story number) to decrypt the data.

Based on whether wrongdoer, target, and gatekeeper statutes played a role as influencing factors in creating clarifications for data breaches by encryption within the RAT theory, encryption management correlates a privacy manager as a gatekeeper which is an indispensable piece of encryption administration and management. Li et al. (2014) called attention to a privacy manager who likewise works as a security instrument for preparing scrambled information. In this specific circumstance, the privacy manager (gatekeeper) utilizes confusion techniques to decrease the individual information in discovery, limiting the danger of data breaches. The thought behind this methodology is to store the patients ’electronically-stored health information in a digital format in an encoded arrangement while as yet permitting handling on this information (Arain et al., 2019). The limitation is that the EHR software-as-a-service vendor must be happy to execute this instrument to ensure the security of delicate data. The privacy manager (gatekeeper) imparts their security methodologies to informal and formal mechanisms with a productive encryption strategy, simple to use by the two patients and human services experts, and ought to be effectively extensible to incorporate new EHR records to ensure the protection of health information management (HIM) data.

Health Information Management

As previously addressed in RAT, there are varying levels of offender motivation that impact a potential data breach occurs. Thus, ‘situational motivation’ plays a significant role in determining criminal activity. HIM is the result that mitigates a

situational motivation of cybercriminals for attacking medical information that is linked to the healthcare organization.

HIM is information management applied to health and health care and is critical to any technology strategy. It is the practice of acquiring, analyzing, and protecting digital and traditional medical information vital to providing quality patient care. There is some proof that EHR can work on the nature of patient consideration and increment patient wellbeing (Cea Soriano et al., 2019; Summers et al., 2019). Kalloniatis et al. (2014) brought up that securing such information happens through the insurance of the physical and virtual systems, information cryptography, information reinforcement, and information isolation and trustworthiness. Kalloniatis et al. (2014) felt that IT security managers ought to think about hearty cryptography, purification, reasonable upkeep of equipment, and powerful calculation techniques while dealing with the existence cycle of electronic data. This strategy is important for tending to different security dangers, including data breaches, through a leadership-driven standard. The HL7 V3 Messaging is a standard that is useful in supporting data exchange between disparate/heterogeneous healthcare systems.

The HL7 V3 Messaging standard use developing web administrations benchmarks, conventions, and technologies to give a stage to electronic trade of clinical data with other healthcare providers. The HL7 V3 Messaging standard is a mature schematic as it gives a stage to health services to catch clinical and managerial data to help medicinal services data trade. The HL7 V3 Messaging standard uses an event-driven protocol, which characterizes the messages and message exchange formats (Spyrou et al.,

2002). The information trade is “performed between correspondence applications with the messages that are started by the source application to the recipient application” (Spyrou et al., 2002, p. 15).

HL7 V3 Messaging is a model-based “next-generation” standard that uses structures and hierarchies encoded in XML syntax. The HL7 V3 Messaging standard uses a model-driven methodology that is based upon the Object Management Group (OMG)’s Unified Modeling Language (UML). It uses Reference Information Model (RIM), Data Types, and Vocabulary Specifications to derive the information component of V3 message specifications. The model-driven methodology ensures consistency in HL7 V3 message specifications and enables mapping to and convergence with other health information standards such as SNOMED-CT, ICD-10, and LOINC.

Based on whether wrongdoer, target, and gatekeeper statues played a role as influencing factors in creating clarifications for data breaches by data transmission within the RAT theory, HIM correlates a security manager as a gatekeeper for HIM operational security strategies. Monitoring is noteworthy so as to give security of information transmission through correspondence channels, recognize any suspicious action and react to any pernicious occasions. The HIM strategy should offer systems to back-up patient information for approved clients to guarantee understanding protection.

Knowledge Gap

Undoubtedly, researchers have led noteworthy research to explore issues around information and data security strategies in distributed computing environments. These studies have excluded security strategies from IT security managers oversite of specified

technologies for electronic health record application infrastructure architectures, however. Subsequently, I recognize a noteworthy gap in knowledge, requiring the stipulation for further studies. This study tried to fill this gap by looking at the issue of data and information security in EHRs from the strategies of IT security managers. Accordingly, I used a case study research design for this study.

Transition and Summary

The primary focus of the literature review was to assess how prior research of IT business professionals who adopted EHR security strategies and addressed barriers. The framework of the discussion provided an explanation of how RAT, such as EHRs, an electronic health record technology, improves products and system performance. Section 1 also addressed the following topics for this research study: Defined the IT problem, Provided the background of the problem, Specified the problem statement, and the purpose statement.

Section 2 focused on the role of the researcher, participants, research method and design, population sampling, ethical research, data collection/ instruments/ techniques, and reliability and validity. Section 3 will examine the research findings and how the conceptual framework is linked to the research findings. Additionally, this section also reviewed the effects of the findings on social change as expressed in terms of tangible improvements to individuals, communities, organizations, institutions, cultures, or societies. Finally, this section discussed future recommendations and actions and a convincing concluding statement.

Section 2: The Project

In Section 2, I provide the rationale for this qualitative case study. I explain the role of the researcher and the strategies for accessing participants. I also describe the research method and design,, the criteria for choosing participants, and the population addressed in the study. I present the method and design, data collection tools, and the consenting process for the research. Finally, I provide the research question and address the trustworthiness of the study.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the security strategies used by information security managers in Midwest United States health care organizations to prevent data breaches within EHRs. The targeted population consisted of information security managers of health care organizations who had implemented strategies to prevent data breaches within their EHRs and who were located in the Upper Midwest United States. The results of this study may impact social change by improving EHR security awareness promoting enhanced identity theft protection for patients to competitive business growth of critical access hospitals. Health care associations' financial development is subject to trust and notoriety of patient care, and enhanced security measures could change ways of life in patients by giving extra-provincial healing facilities by the CMS management of data records.

Role of the Researcher

My role in this qualitative study was to oversee the research, collect data, evaluate the discoveries, and present the outcomes. Eyre et al. (2015) expressed that the researcher

should design a study that focuses on the most capable strategy to create evidence for data-focused practice. Furthermore, Eyre et al. expressed that a project should be arranged cooperatively with stakeholders. I designed the study to allow participants to describe the security strategies used to deter EHR data breaches. I interviewed security managers from health care organizations who had implemented strategies to prevent EHR data breaches.

The Belmont Report includes the moral utilization of human subjects and spotlights the fundamental standards of regard for people, helpfulness, and equity amid the study (Barlow, 2020). Bansal et al. (2018) noted that researchers need to follow moral guidelines to deal with human subjects properly. The moral guidelines clarified in the Belmont Report and the authoritative structures for research dependent on those benchmarks have served society well by providing a steady structure for research development (Califf & Sugarman, 2015). I complied with the standards delineated in the Belmont Report.

When I contacted the health care organization, I led an exploratory telephone exchange with the HR supervisor of IT who provided a list of qualified participants. Moreover, I thought about the three fundamental moral standards of regard for privacy, advantage, and equity underlined in the Belmont Report, in which Barlow (2020) directed the obligation of clarifying the potential risk. Consequently, the moral principles and standards of the Belmont Report on the assurance of human subjects were followed.

Recording and transcription of interviews were steps used to mitigate researcher bias for this study. Baur et al. (2015) disclosed that without total honesty, recognizing

what individual stakes or tendencies reflected in research is hard and that headways have exhibited being clear alone are lacking to moderate predisposition. Also, J. Smith and Noble (2014) noted that researchers must refresh data to moderate predisposition and view information from an objective focal point. To diminish bias, I conducted my study inside a health care organization that was independent of my present work. I was the sole data-gathering instrument. Morals, respectability, and professional competence are crucial for guaranteeing quality research (Baur et al., 2015). To mitigate bias, I remained open to new experiences inside the research.

I used an interview protocol and conducted participant transcript review to mitigate personal bias and view data from an objective perspective. Fusch et al. (2017) asserted that total elimination of bias is impossible, yet a researcher should utilize interview protocols, participant checking, and information immersion to moderate bias. The interview protocol guides the researcher's questioning and provides a structure of inquiry to help the researcher through the data collection process. Qualitative researchers use an interview protocol to ensure consistency of the data collection methods. I used an interview protocol to ensure consistency with the interview questions and to stay on task (see Yeong et al., 2018).

Participants

The participants in the study were information security managers from Midwest United States health care organizations. I conducted a preliminary telephone call with the HR manager of IT of the targeted health care organization to discuss the recruitment of participants, including the criteria for participants' selection related to limiting EHR data

breaches. The qualification criteria included participants at least 18 years of age who understood the EHR implementation inside their organization. Furthermore, the participant needed to have worked at their health care organization for at least 2 years, have a thorough understanding of EHRs, and have a working knowledge of the security strategies used to protect EHRs from data breaches. In addition, the participants were required to have reasonable involvement with apparatuses used to guide the security strategy of EHRs. Research participants were required to have the information needed to answer the research question.

The believability of participants was addressed during the interview, which Weller et al. (2018) expressed was important for credible results. Participants' knowledge of the topic was explored in the study. Yeong et al. (2018) noted that participants' ability to answer the interview questions is a fundamental element of the candidate's selection for the study. Yeong et al. also focused on participants' need to comprehend the research question before taking part in data collection. I screened the participants to ensure they could answer the interview questions.

Participants and research ought to set up compatibility, which I complied with by acquainting myself and making inquiries with the build-up to expert association with the participant. A researcher's clothing could influence the impressions and official choices of an interview. In this way, a working relationship was set up through cooperating and dressing in an expert way.

Building an association with the participant is crucial for how the participant sees the researcher. Yin (2014) expressed that having a clear understanding enables the

researcher to connect with participants so the transferability of the results to different settings can be contemplated. An introduction letter (see Appendix A) expressing the reason for the study was sent by email, and preliminary conversations were used to establish rapport with my participants.

The initial period of developing a working alliance with the participants involves speaking with them. Yilmaz (2013) expressed that the researcher should set the tone for the meeting. Furthermore, people can illuminate how they comprehend their general environment and their experiences through engagements with the open-finished request (Yilmaz, 2013). Qualitative research requires a careful examination of participants' knowledge of the research topic. Open-ended questions are used to collect data, which are analyzed to identify codes, categories, and themes. Open-ended questions allow participants to explain their experiences by the without the researcher predestining those responses (Yilmaz, 2013). I used open-ended questions to obtain inclusive, relevant, and sensible answers.

Participants were reached by means of email with the assistance of the HR administrator of IT of the health care organization. The HR administrator facilitated my access to the participants (see McFadyen & Rankin, 2016; Peticca-Harris et al., 2016). Although gatekeepers may help with giving the authorization to contact potential participants, they do not guarantee that participants will cooperate with the researcher (McFadyen & Rankin, 2016). Moreover, any issues emerging from associations with the participant may undermine gatekeepers' authoritative standing (McFadyen & Rankin,

2016; Peticca-Harris et al., 2016). In the current study, the gatekeeper was contacted, and I clarified the motivation behind my study and objectives for recruiting participants.

Research Method and Design

A qualitative multiple case study was the most fitting methodology because the purpose of the study was to explore the security strategies used to prevent data breaches of EHRs. A multiple case study including numerous participants was chosen to answer the research question. A multiple case study design was suitable to explore the health care organization's security strategy pertaining to proactive security measures against potential EHR data breaches.

Research Method

The qualitative method was used to answer my research question. According to Rutberg and Bouikidis (2018), the qualitative method is not hypothesis driven and helps researchers perceive the participants ʾperceptions. My purpose was not hypothesis driven, which made the qualitative method more appropriate than the quantitative method. Through a qualitative approach, researchers can pass on suggestions that ascent out of the qualitative capability. This technique helped me collect the data needed to answer the research question. The qualitative approach requires a researcher to convey their circumstances and desires and to break down and reveal their assumptions and inclinations (Saunders et al., 2018). As the researcher, my responsibility was to understand participants ʾpoints of view.

A quantitative method was considered but not chosen. The quantitative method is used to quantify a problem and gather numeric data to test a hypothesis (Purohit & Singh,

2013). The purpose of my study was to explore strategies to limit EHR data breaches, not quantify patterns of breaches. Despite the advantages of the quantitative method, it was not chosen for this study because numeric data were not needed to answer the research question.

The mixed-methods approach involves a combination of qualitative and quantitative approaches. The mixed-methods approach requires gathering qualitative and quantitative data to explore an issue with an open-to-end technique (Purohit & Singh, 2013), which C. Green et al. (2014) noted included survey and quantitative-based solicitations. My study comprised the open-finished interview technique, which did not require the use of surveys. Furthermore, mixed-methods research requires the examination of variables and can be helpful in exploring complex research questions. However, quantitative data were not required for my study.

Research Design

To satisfactorily address the research questions, I picked a case study design rather than phenomenology or ethnography. The case study design was best used to convey delineations of the authority phenomenon utilizing subtleties to decide the data and to distinguish the records. Being in an exploratory portrayal, the case study design contributed knowledge to my study. Furthermore, Vaismoradi and Snelgrove (2019) expressed that case study design presents a total and exact showcase of a case. Moreover, the case study design was utilized to research different aspects of a phenomenon and to satisfactorily address the research questions, which the structure bears subtleties not

actually acquired by other designs, which this design is appropriate to the problem studied.

A phenomenology design was a practical alternative for the study. Phenomenology does not have the dimension of adaptability of a case study (Hyett, Kenny, and Dickson-Swift, 2014). A phenomenological design centers around the human subject and permits a verbalization of the shared characteristics of people's events inside proper conditions. Phenomenological research expects the probability of setting their points in a fathomable area so the phenomenology can confirm encounters. Notwithstanding, shared characteristics of people's events were not the focal point, but rather the shared traits of the group were. Also, an adaptable qualitative data information accumulation method for a group was required instead of clarification of an individual affair. Along these lines, phenomenology design was not utilized, which would digress from the research question.

Ethnography was additionally considered; however, it was not utilized. Hudson and Hudson (2013) depicted ethnography as a qualitative design that allows an examination of phenomena that reflect the learning and course of action of suggestions dealing with the life of a get-together. Furthermore, the examination of fitting reports, participant examination, and formal and casual interviews as information gathering apparatuses for ethnography lines up with the utilization of a hypothetical structure as opposed to reason (Coker et al., 2019). Nonetheless, my research plan did not require a hypothetical system, nor did I research a social phenomenon pertinent to the study. Moreover, there is no compelling reason to examine the participants but instead gain an

understanding of the strategies used to counter data breaches within EHR. Along these lines, ethnography was not picked on the grounds that an obscure issue was not being looked for.

Population and Sampling

The population for my study consisted of information security managers of healthcare organizations within the Midwestern United States (or Midwest). Occupational employment statistics for 2019 provided by the United States Department of Labor for Wisconsin announced 1,260 individuals as the population of Information Security Analysts characterized to respond to computer security breaches and viruses. (Bureau of Labor Statistics, 2019). Moreover, the purpose of selecting a population is to identify as much information as possible with the least number of participants. A smaller sample size helps to achieve saturation faster, and failure to achieve data saturation negatively impacts the validity of the study. Instead of random sampling, more appropriate for quantitative studies, the purposeful selection of participants possessing qualifications, expertise, and experiences pertinent to the phenomenon under study is a fundamental requirement for enhancing the trustworthiness of qualitative research findings (Yin, 2014). Since my employer is a member of the leading six Wisconsin-based healthcare organizations in the recently-formed partnership named abouthealth™; I am aware of the partners, who together cover nearly 90 percent of the state's population, leveraging their collective resources and best-in-class practices to improve the lifetime health of people in the communities they serve in Wisconsin and surrounding areas in the Upper Midwest. The number of cases selected for a qualitative

study is dependent on the nature of the study research questions and the number of factors that might influence the study concept. There is evidence that hospitals tend to differ by type and characteristics, which includes sociodemographic organizational structure, availability of resources, location, and scope of services provided. With this in mind, there was a diligent effort to identify similar organizations that utilize corresponding Electronic Health Records for participation in this study in order to avoid any confounding variables that may present from dissimilar hospital types. Yin (2014) stated that the researcher could settle for two or three cases when the theory is straightforward, and the issue under investigation does not demand an excessive degree of certainty. Three cases positioned by large, medium, and small of abouthealth™ healthcare organizations achieved a high-quality multiple case study for literal or theoretical replication in the research question actualizing a security strategy to limit EHR data breaches. I contacted the abouthealth™ partners, and based on the responses received, three healthcare organizations were used in my multiple case study, with the remaining used to strategically incorporate if data saturation has not been achieved. A LinkedIn abouthealth™ partners employee directory search for information security managers provided probable three participant eligibility per case healthcare organization (Bhatia-Lin et al., 2019; Kapoor et al., 2018). A gatekeeper was utilized to help facilitate endeavors for me to interview the participants. The point at which answers to consistent, carefully worded questions result in the same or similar responses from participants indicates data saturation.

I remained attentive to the point of data saturation and prepared to add to the data collection efforts through additional interviews or additional participants if data saturation did not appear to occur with the nine participants who comprised the predefined eligibility criteria sample in this study. Eligibility to participate in this study was a participant must be at least age 18, working as an information security manager within one of the six abouthealth™ healthcare organizations represented in this study, and possess demonstrable experiences with successful EHR implementation in hospital settings. Rowley (2012) believed that a sufficient number of participants in case studies was between one and 10 participants; therefore, census sampling of nine information security managers possessing expertise and experience of having been successful in EHR security strategies fulfilled the requirement in multiple case study designs. Lucas (2014) added that census sampling occurs when the researcher incorporates in the research the whole population that fits the predefined eligibility criteria.

The census sampling procedure was consolidated into the foreordained strategy for choosing participants and has 100% participation. Census sampling is a strategy used to choose the examples and all the qualified employees for a study. Census sampling was utilized from inside the number of populations in the participants who are qualified to take part. I chose to use census sampling because the nine information security managers are a representation of the entire population of information security managers from the chosen three case healthcare organizations. Random sampling was not considered for this study since it isn't appropriate for a subjective case study. Determination of testing methods actualized methodologies that guaranteed quality, credibility, and validity (Roy

et al., 2015). The execution of sampling technique strategies was done through participants' interview reactions by member checking and data triangulation.

Interviews occurred with qualified participants, which included telephone interviews with 45-minute timeslots and in-person interviews in a private gathering for the individuals who favor face-to-face interviews. Also, the interview convention was pursued, which incorporates a similar design and questions for all participants. At last, all participants completed the consent form prior to the interview, which complies that their recognizable identification data was not be unveiled.

Member checking and triangulation were utilized to confirm the exactness and dependability, which guaranteed the validity of my study (Smith and McGannon, 2018). Member checking includes returning and surveying the aftereffects of the study with the participants. Furthermore, member checking and information triangulation are utilized to guarantee the validness of information (Abdalla et al., 2018). Besides, data immersion happens when new data delivers next to zero changes; therefore, member checking was performed post-interview conclusion and a breakdown of the data to guarantee information immersion.

Ethical Research

The moral and ethical contemplations were scrutinized by ensuring participants' protection and disseminating the consent form. Consent is a moral prerequisite that depicts the researcher's commitment to educating the participants with respect to the dangers of the study, the advantage of the study, and their rights as a participant (Check, Wolf, Dame, and Beskow, 2014). Moreover, Dekking, Van der Graaf, and Van Delden

(2014) expressed that the consent ought to be gathered by a target person who likewise shows the deliberate attributes of participation. At last, Dekking et al. (2014) additionally incorporated that educated consent help uphold the privacy of participants' rights. Along these lines, the consent contains dialect to guarantee classification and assurance, which were messaged to every single potential participant before any information accumulation. When the consent was marked, the participant consented to the volunteer to the idea of the study and may quit whenever.

Watchful thought of keeping up ethical standards must be set up while choosing research participants for a research study. Participants may decide not to partake at whenever point, and they were guaranteed that on the off chance that they choose not to take an interest in the study, the information would be erased, and the participant would be educated about the activity. As per Auger (2016), informed consent must be acquired from all participants who agree to take part in the study without coercion deliberately. The informed consent permitted participants the privilege to pull back or stop the recording amid any bit of the interview in the event that they don't feel great without striking back. I collected marked consent from all participants who deliberately consented to take part in the research study, and once they consented to take an interest willfully, a duplicate of the marked consent was given to every participant for their records (Addendum B). Finally, I told the participants that I finished a National Institutes of Health (NIH) internet instructional class to promote trust and guarantee that ethical standards would be clung to amid the research study.

The consent form (Appendix B) gave an alternative to all participants to quit the study. My contact data, including email and phone number, was given to the participants on the off chance that they choose to pull back from the research study consider at whatever point they need to. Artal and Rubenfeld (2017) expressed that total honesty, educated assent, and intentional cooperation are essential in a research study. The participants were educated of any advantages and damage that the research study would present, and their investment in the investigation is intentional. The informed consent form (Appendix B) and letter of participation (Appendix A) were incorporated into the Appendices and the table of contents. Barnard (2016) underlined the significance of informed consent, which addressed the secrecy of the research participants, information stockpiling, and security of reactions of participants. Information put away is being kept in a wellbeing safety deposit box for five years to protect the participant's secrecy. Privacy of the participants was ensured by allocating every association and the participants a remarkable distinguishing identification number, and every one of the information put away would be secret word secured.

There was no incentive for this study. I told the participants that they all have enthusiasm for defending information put away in distributed computing and limiting information ruptures of clients by and by recognizable data. The utilization of inspirational procedures as an incentive force for research participants to willfully take an interest in a research study and effectively recognized these procedures to verify data security strategies was of an incentive to their associations and may have filled in as benchmarks. Moreover, the participants were beneficiaries of the last research study.

Offering their insight to other topic specialists in a research study gave positive reactions and upgraded rich information accumulation since they all offer a typical premium. The final doctoral original copy incorporated the Walden IRB endorsement number 12-24-19-0552901.

Data Collection

In this section, how data was collected and applied during the study is discussed. According to DeJonckheere and Vaughn (2019), semi-structured interviews with open-ended questions allow the researcher the essential information accumulation strategies (see Appendix D), which were utilized in the meeting convened to gather information from the participants (see Appendix C). Furthermore, the meeting convention assisted in capturing basic data, for example, the participant's experience, socioeconomics, a prologue to the study, the individual's situation as it identifies with the medicinal organization. Semi-structured interviews with the structure were utilized to make a general picture of how security information technology managers in medicinal organizations limit EHR data breaches, which was triangulated with authoritative reports acquired from the gatekeeper.

Instruments

As the essential information accumulation instrument, semi-structured interviews were directed by utilizing open-ended questions all through my study. Young et al., 2018 expressed that the researcher is the essential information gathering instrument because the idea of qualitative research information gathering procedure could be affected by the extent of the information accumulation instrument. In addition, techniques that empower

open-ended questions fuse delayed commitment and reflexivity (Steber, 2018), and Shannon and Hambacher (2014) claimed that reflexive diaries increase the validity of information gathering. Interest and reflexivity were increased by investing energy in the participants in their condition, and NVivo was used to record how choices were executed.

My objective was to guarantee the participation of the active researcher. Qualitative research works with compositions, different understandings of individual gatherings, and focused dialogue to measure the importance of the contribution of a study sample. Thus, perceptive questions were asked that let participants know whether their responses to the research questions were understood. Cope (2014) also said that drawn-out commitment builds trust and partiality with sources to help them develop helpful, point-by-point responses, which adds scope and depth to the analysis. Correspondence with the participants was kept up until the end of the study, to keep them locked in.

The main instruments were semi-structured interviews and hierarchical reports, which the gatekeeper administrated. A semi-structured interview was upgraded and reintegrated during the information gathering (Gomez, 2018; Flick, 2018). To keep the interview conditions consistent, all participants were asked similar questions.

Data Collection Techniques

After approval by Walden University's IRB, a semi-structured approach was used for face-to-face and telephone meetings. McIntosh and Morse (2015) argued that the advantage of semi-structured interviews is that they give provide closeness to the interviewer and add structure to the interview. Phone correspondence also improves openness, privacy, productivity, and efficiency, which gives it an advantage in spite of

the lack of eye contact. Subsequently, I made myself constantly available to the participants. McIntosh and Morse (2015) also noted some impediments, for example long-distance charges and participant's lack of access to phones. For this reason, billable calls were permitted during the information collection period.

To gather information from my participants, correspondence with the gatekeeper was facilitated to get their access details, telephone numbers, and email addresses. McRae et al. (2013) said that gatekeepers help in collecting informed assent by guaranteeing that participants adhere to the interests of the institution. Although gatekeepers don't collect specialist assent from participants, they may carry out their choices about support, which implies that gatekeepers must stay away from irreconcilable circumstances (McRae et al., 2013). After their availability, telephone numbers, and email addresses were gathered, every participant was contacted to plan a meeting, either face to face or via phone.

The meeting conventions were used to stay on track. Participants were contacted by email to provide educated consent. O'Malley, Gourevitch, Draper, Bond, and Tirodkar (2015) identified that the reason for interview conventions is to clarify the techniques and strategies used to direct the research and guide the interview. After the completed consent forms were returned (Appendix B), interviews were planned and the participants were reminded that all interviews would be audio-recorded and stored on an encrypted hard drive.

After the interviews, member checking was performed to guarantee the accuracy of the information gathered, information immersion, and correctness of translation.

Member checking has been recognized as an approval method (Kornbluh, 2015; Morse and McEvoy, 2014). Birt, Scott, Cavers, Campbell, and Walter (2016) noted that it is used to explore whether results reverberate with participants' information. Furthermore, member checking offers a way to reduce biases of the researcher by asking for elective viewpoints on the interpretation of the data (Kornbluh, 2015). Hence, I used member checking to ensure the accuracy of the interviews by going over the accumulated data with the participants. The information gathered from the account was electronically transcribed and reviewed with every participant. Interpretation of the information was a convenient procedure, since all participants guaranteed that no information had been lost from what the participants expressed. Member checking interviews occurred until no new information arose.

The preferred information-gathering methods use more narrative-research information sources that contribute to open doors for the legitimacy and dependability of a study (De Vries, 2018). Aldiabat and Le Navenec (2018) said that analyzing an organization's archives can improve interviews. For this reason, the gatekeeper was contacted to obtain extra data that were useful for recognizing the hierarchical record that was helpful for this study. The records of intrigue included strategy manuals, policy and procedure documents, and some other archives about EHR data breaches (Genç et al., 2019).

Data Organization Techniques

The information organization for my study included storing sound accounts, notes, and interpreted information on an encoded hard drive, and marking them for

effective examination (Broman & Woo, 2018). Securing protection of the participants is a basic moral requirement of examination (Colosi, Costache, and Colosi, 2019). Every participant and datum had a unique identifier, with the addition sign (+) used to note that the participant gave extra data (i.e., for participant 1, P1 and P1+; for participant 2, P2 and P2+, and so forth). Carter et al. (2019) used information association for ordering and recovering information on subjects. Transcriptions maximize the protection of the participants and designed for simplicity of review (Fritz & Vandermause, 2018).

Information examination and topics were recorded in NVivo. But though NVivo is a straightforward program, it can't do a large portion of the necessary work (Castleberry, 2014). It has some programmed coding capacities, but the process needs to be analyzed. NVivo provides an easy-to-use configuration for arranging, synthesizing, and displaying data up to the point that the researcher finds the answer to the research question (Castleberry, 2014). Moreover, it enables the researcher to gather, record, and separate different types of information, incorporating Microsoft Excel spreadsheets, Access databases, and Word, PDF, rich text, and plain text files along with most types of sound, photograph, and video documents (Castleberry, 2014). The adaptability of NVivo enabled me to arrange vital records for investigation.

The recorded data were stored on an encrypted hard drive in a safety deposit box for five years, after which printed copies were destroyed and the hard drive was reformatted and granulated into scrap. Handwritten documents and participant reports were stored in a safe and will be destroyed after five years. Information security is important to protecting participants, so the people and the medicinal organization

involved were not revealed to anyone but me.

Data Analysis Techniques

Methodological triangulation was used to analyze the information and discover the answers to the research questions. This approach uses multiple information accumulation systems to fuse points of interest and reveal hindrances (Fusch et al., 2018). Furthermore, methodological triangulation uses at least two data-gathering techniques to break down nearly identical phenomena and improves believability by collecting and approving information from numerous sources. In this way, semantic record collecting was used to identify noteworthy topics using interviews and report examinations to unite important data to the conceptual framework and research question. Finally, my conceptual framework provided a reason for involving the distinctive accentuations of my coding.

Another reason for methodological triangulation was to guarantee information immersion. Yin (2014) said that methodological triangulation helps on reach information immersion and improves the legitimacy of a study. Information immersion was in fact reached, which advanced my study by ensuring enough data to guarantee thoroughness. With adequate information, the findings become less likely to change (Lewin et al., 2015). Information immersion was deemed to be reached on the grounds that every single qualified participant was interviewed. Moreover, the researcher used different methods of data aggregation to gain a full view of the phenomenon, consolidating interviews, observations, and journaling from the research (Cope, 2014). Methodological triangulation was also used to dissect all the information from the interviews and

medicinal organization records.

My triangulation technique included breaking down hierarchical and medicinal organization records, speaking by phone with the gatekeeper, and conducting interviews to remain close to the participants, and analyzing documents from research reports. Inspection of medicinal organizations' records can improve interviews. After being interpreted, the information gathered from the audio recordings and notes were stored in a Microsoft Word file, and all inquiries were put in the "Heading 1" format. NVivo was used to perform a thematic analysis.

Coding depended on the information examination, the research questions, and the conceptual framework. The appropriation of the thematic analysis permitted a superior cognizance of the most effective coding. Thematic analysis is characterized by native descriptive design, which consists of a lot of straightforward and efficient strategies used to break down literary information and translate themes (Deighton-Smith and Bell, 2018). All information gathered from a participant was shared between that participant and me, a fact the participants confirmed by member checking the assembled information. After I characterized the codes, codes depended on words and expression, which helped me set up the themes of the study. By using thematic analysis after coding, I determined the most fundamental topics for information gathering.

The NVivo analysis tool was used to identify evidence-based ramifications of the qualitative research. NVivo is qualitative analysis software that draws results from similarities between the equivalent datasets. It lets researchers code information and make themes or classifications. NVivo has an auto-coding ability that makes it useful for

coding information. It was used to auto-code and check the outcomes along with physically coding, and thematic analysis was used to code subjective information. Afterward, that code was used to distinguish patterns in the informational index about the research question. Thematic analysis was used to recognize patterns in order to code themes and subthemes.

Document clustering was used to assemble the unsupervised records into convincing applications for substance mining and information recuperation. Capable archive bunching is a direct result of the term-level, sentence-level, and thought-level methods in the high-dimensional record (Nagaraj and Kalarani, 2016). The semantic document-clustering calculation used the semantic loads of words to sort the topics in the reports, after which the closeness of sentences was assessed using a program that uses load and similarity for productive grouping (Nagaraj and Kalarani, 2016). NVivo was used as the document-clustering apparatus.

Clustering is an important task in text mining. A consistent test used in document clustering is to choose the number of document clusters (Timande, Chandak, and Kamble, 2014); if the quantity is insufficient, this shows lack of clustering exactness (Timande, Chandak, and Kamble, 2014). When the groups were included in NVivo, the omission of appropriate information was checked.

Reliability and Validity

Reliability

Researchers use reliability and validity to determine the tone of a study so that the quality of the questions can be evaluated by continuous discussion with participants;

otherwise there would be a possibility of faltering. All participants were asked similar questions on multiple occasions. The two criteria of unwavering reliability and validity have been proposed for making qualitative research reliable (Morse, 2015b). All participants were guaranteed that they could believe me after the interviews were over, in light of the fact that no data from past participants would be revealed. Korstjens and Moser (2018) demonstrated that there are four ways to deal with rigor in research on reliability: dependability, credibility, transferability, and confirmability, which were all addressed in my study. Systematic reliability, availability, and integrity are the most important security points (Wang et al., 2019). All participants' secrecy was respected, and the integrity of my study was guaranteed.

Dependability

Dependability is a measure of the reliability and consistency of a research study. It implies that other analysts could use similar information to produce comparable results. Dependability is achieved when a specialist can use similar information to get similar results (McGrath et al., 2019). As the researcher, I guaranteed dependability by using a similar meeting convention to ask every participant similar questions in the same order. The interview conventions (Appendix A), when repeated, led to similar results. Connelly (2016) said that a review trial is one technique used to guarantee steadfastness.

Noble and Smith (2015) implied that the consistency and dependability of a study depend upon the researcher keeping a choice trail. I used NVivo to report problems and choices in the procedure, which guaranteed lucidity and straightforwardness. Keeping a choice trail also helps to guarantee dependability by making the researcher's choices

unmistakable and straightforward (Noble and Smith, 2015). The dependability of a study relies on the participants giving honest and complete answers to questions (McGrath et al., 2019). I ensured this by asking similar questions of the participants in sequence. The participants were allowed to choose where the interview was held, and I disclosed to them why and how the research procedure improved dependability. I also informed them that all their responses were private and would be stored on a memory stick that would be secured in an area accessible only to me. The consistency of the participants' reactions was measured through member checking. Member checking was finished by having the participants survey the transcripts to guarantee that the information gathered in the interview was correct.

Credibility

The credibility of a qualitative research study depends on the researcher protecting the genuineness of their work. Hussein (2015) described data triangulation as a system that uses multiple sources to verify information. I correlated the themes identified from the interviewees and investigated the authoritative records, just as with the field notes and choice trail from NVivo. Using triangulation from numerous sources, including semi-structured interviews, and contrasting these with hierarchical records, I checked the research findings. I let participants audit and assess the interview transcripts to guarantee that my translations were right and to make appropriate changes before proceeding with the interpretation of the rest of the transcripts. Member checking has been described as among the most precise methodologies for legitimating participants' reactions to inquiries. This procedure guarantees that their reactions are honest. Member checking

and data triangulation together are used to guarantee the validity of research studies. Member checking procedures limit individual inclinations and improve the believability of a study. I avoided individual predispositions by keeping a review trail, using NVivo to report problems and choices. This improved the thoroughness of the investigation.

Transferability

Transferability is a type of outside legitimacy that sums up the findings of a study for an alternative setting or gathering (Cope, 2014). I achieved transferability through information accumulation inside and outside the investigation, with rich and extensive data on participants from interviews and hierarchical records. I did this by using similar inquiries in the same order for each participant. Member checking was accomplished by sharing the information uncovered in the interviews with every participant so they could decide whether the transcripts spoke to their own perspectives and encounters. Member checking also improves data saturation, which is achieved when no new information, themes, or codes appear through member checking. The transferability of this study was ensured by creating a rich and extensive set of data connected to an overall setting.

Validity

Validity is characterized using scores on an appraisal instrument. Validity scores are essential for an assessment of a study. The themes acquired using NVivo were used to create a scoring framework. There are two types of validity: statistical conclusion validity and internal validity. Statistical conclusion validity implies exactness in conclusion about the closeness and nature of the connection between two components (Richardson, Hudspeth Dalton, Shafer, and Patterson, 2016). Statistical conclusion validity incorrectly

associates measurements, conflicting treatments, and distinctive differences of assorted varieties into the exploratory setting. Obtaining internal validity requires paying little heed to whether causation could have prompted the verifiable ends (Richardson et al., 2016). The credibility of my study was identified with validity. However, the key isn't the identification of the idea but how the thoughts about reliability are introduced.

Confirmability

Confirmability improves the objectivity of a research study by using a review trail to maintain transparency and validity (McGrath et al., 2019). I monitored all my perceptions, concerns, and choices during the study in NVivo to provide transparency. A review trails fills in as a plan for the study and diagrams the procedure used by the researcher (Auger, 2016). This plan thus made the examination replicable in other settings and populations. The review trail also reflected the participants' reactions, not only the researcher's predispositions and perspectives (Cope, 2014). Ang et al. (2016) portrayed review trails as the key strategy for gauging confirmability. The researcher's notes monitor the means used for the research study and build up objectivity (Connelly, 2016). Furthermore, the notes can be used by future researchers to understand how and why choices were made during the study.

Transition and Summary

The perspective of this study was discussed in this section. The purpose was restated, and the roles of the researcher and participant were addressed. The main data-gathering instrument and the moral guidelines of the study were also discussed. Statistical analysis was used to choose participants and achieve information immersion. Attention

was also drawn to the methods, research design, population, and sampling. The moral conditions required by the IRB were then discussed. Next, the information-gathering and interview procedures were discussed, with attention to the data gathering through telephone and in-person meetings and from medicinal organizations' documents. My data were composed and broken down in NVivo. Methodological triangulation was used to guarantee immersion. Finally, techniques to guarantee reliability and validity were incorporated. Reliability and validity were addressed through member checking.

Section 3: Application to Professional Practice and Implications for Change

This section contains information from the qualitative study. I present the findings and describe how they can be applied to professional practice. Next, I discuss results that might lead to social change and make recommendations for immediate action. Finally, I provide recommendations for further study and personal reflections on this research.

Overview

The purpose of this qualitative multiple case study was to identify security strategies that IT managers use to secure data in EHR systems in the Midwest United States. The data were collected from IT managers through semistructured interviews conducted in three IT health care organizations in the Midwest. I also reviewed organizational documents that were provided. The IT managers all had experience securing data in EHR systems and mitigating data breaches.

Three major themes emerged from the study: (a) requirements based on government and organizational regulations, (b) implementation of the best industry-standard security measures, and (c) emerging interoperability with a security and privacy program. These themes suggested strategies for minimizing EHR data breaches. Section 3 includes a presentation of findings, applications to professional practice, implications for social change, recommendations for action, recommendations for further research, reflections, and the conclusion of the study.

Findings

The overarching research question for my study was this: What strategies do information security managers in health care organizations use to prevent data breaches

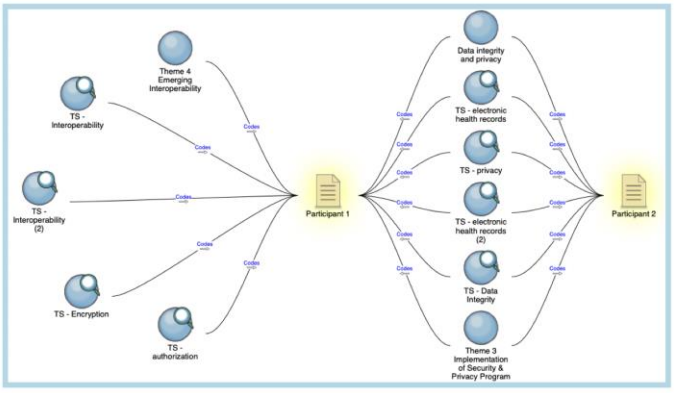
in their organizations ’electronic health record systems? In this section, I present the findings and three major themes I identified after conducting the study. The themes were developed from the nine semistructured interviews about why security strategies for EHR systems are fundamental for health care organizations. The participants were IT security managers with at least 2 years at their health care organization who had thorough experience working with EHR records, including a working knowledge of the security strategies used with the EHR systems (see Ashraf, 2018).

IT security managers prepare and maintain strategic preventive measures to mitigate EHR data breaches (Center for Internet Security, 2018). I asked nine IT security managers to take part in this study. All nine consented to participate in three cases involving large, medium, and small health care organizations. Each participant had 2 years of experience with health care system security strategies and demonstrable experiences with successful EHR systems in hospital settings.

The participants were labeled P1 through P9 and the organizations O1 through O3. Participant 1O1 referred to Participant 1 from Organization 1. After interviewing the third participant from each of the organizations, I reached data saturation as I found no new themes or codes using an NVivo-organized participant-coding cross-analysis (see Figure 2).

Figure 2

1O1 Coding Cross-Reference to 2O1



Organization documents were labeled with O1 through O3 and categorized as policy (P), checklist (C), or guidelines (G), also with sequential numbering. Document O1P1 was Organization 1, Policy 1. Organization 1 provided five documents, O2 provided 12, and O3 provided seven before the interviews, and the documents were member checked to ensure an accurate understanding and to enhance the methodical triangulation process.

Methodological triangulation was used to analyze the data sources, which were semistructured interviews and organizational documents. Three major themes emerged: (a) requirements based on government and organizational regulations, (b) implementation of the best industry-standard security measures, and (c) emerging interoperability with a security and privacy program. These themes suggested strategies for minimizing EHR data breaches.

One essential strategy used by the organization was to place application and work-area virtualization conditions on the EHR environment, which benefits diverse health care geolocation organizations that inherit them from parent organizations while

interpreting and establishing policies, processes, and procedures. This strategy requires familiarity with the arrangements, agreements with merchants and vendors, and apparatuses used to improve EHR modules and interfaces with EHR system updates, releases, and upgrades. The organizations are also building a warehouse of EHR information to help research and improve understanding. Clinical data are not difficult to share using EHRs, and patients ʾdata can be obtained and refreshed as treatment is given (Keshta & Odeh, 2020). Kopel et al. (2019) demonstrated that the benefits of EHRs include the capacity to sort out information for ongoing consideration and the capacity to follow practice data and public principles. The explanatory conditions in a shared health care organization repository included this ported information.

Data saturation was achieved after all the participants were interviewed, as no new themes or codes emerged. All participants referred me to online documents of the HIPAA, the HITECH, the NIST, and HL7 RIM because of regulatory information policies. In addition, I used methodological triangulation to analyze the two major sources of data: the semistructured interviews and organizational documents focused on security policies such as data-breach response, security-incident management, third-party security management, and access control. The reason for the triangulation was to provide a confluence of evidence to increase credibility. Validating findings over the informational index diminished bias through data gathering interviews and documents (J. L. Johnson et al., 2020). I also used member checking to ensure accurate and complete transcription of my findings and secure data saturation.

Theme 1: Requirements Based on Government and Organizational Regulations

The first theme was prerequisites due to governmental and hierarchical guidelines depending on HIPAA, the HITECH, and the methodologies for research and data proposed by the IRB of the association (Mello et al., 2018, Rathert et al., 2019). The methods and terms for measuring and controlling the risk associated with cybersecurity programs have not been standardized (Maglaras et al., 2019; Schmeelk, 2020). HIPAA oversees the security and protection of prosperity record keeping through the Privacy Rule (G. Cohen & Mello, 2018; Graboyes & Bryan, 2018; Woodside & Amiri, 2018). HIPAA regulates how covered entities guarantee and check PHI (ONC, 2016). The association's report showed the conditions in which covered entities are permitted but not required to use and revealed PHI for unequivocal exercises without first confirming an individual's endorsement. Liu et al. (2015) concluded that if 500 individuals are involved in a data breach, a report must include the conditions of the data breach, the name, the type of record, the number of records affected, and whether any external vendors were incorporated using PHI.

Patients face a severe risk of exposure of their personal information because the security and privacy safeguards implemented by EHR custodians provide no guarantee against clandestine exploits (Krisby, 2018). Innovative collaboration in medical services has led to increased intricacy in EHR frameworks and to requirements for IT administration and controls to protect medical services foundations and sensitive patient data. Voluminous EHR collections containing itemized patient records might be looked at with malicious intent as objectives for exploits, such as ransomware assaults or identity

theft (Abouelmehdi et al., 2018). To ensure that patients thrive, strategies for reducing the risk and effects of data breaches are fundamental for health care administration systems and clinicians.

Compliance and breach management are two noteworthy necessities of HIPAA. Compliance involves keeping up security and organization. Breach management strategies include procedures, frameworks, test structures, work process charts, examinations of compliance, and steps for staying in compliance with the law (Downing, 2014). The chief information security officer and the HIPPA office, with the assistance of outside professionals, must use PC criminology and other methods to grasp the purpose of information breaches and eliminate them (Mittal, 2020).

Studies have indicated that lack of access to shared information is one of the main causes of data breaches in health care services (Mohit & Bhararth, 2020). In the underlying period of a data breach, Participant 1O1 reviewed the degree and seriousness of the infringement. In the event that it is an extreme breach, proactive warning is the correct strategy. Next, they determined who and what was affected and tended to the danger quickly. If the matter is as straightforward as resetting passwords, at that point a secret key reset is promptly carried out. After containing the data breach and reestablishing business activities, the difficult work gets started.

Medical services associations must follow HIPAA privacy rules that are presented in government guidelines. HIPAA addresses both the privacy and the security rules of PHI, as they supplement each other (Pussewalage & Oleshchuk, 2016). Elmore (2020) reported that the HIPAA Omnibus Rule came into effect in 2013. Health record

information should be moderately available while security rules are upheld. To protect sensitive information, it is important to know where it is located. The organizational document Privacy and Security and the HIPAA rules present government assurances for understanding patients ’data, and HIPAA addresses patients ’privileges regarding their health information.

HIPAA stated that health care organizations are required by government legislation to actively oversee patients ’data safety, security, privacy, and confidentiality. Sharing of patient data provides protection and security that are in contention with HIPAA principles. The EHR frameworks are instantaneous, an advantage over actual conventional data frameworks (Li et al., 2020).

Participants 2O1, 3O1, and 5O2 said that formal HIPAA continuing training units (CTUs) are a yearly necessity, but participants 1O1 and 402 noted that their preparation was casual. Baumanna et al. (2018) recognized the importance of training to promote ease of use of the EHR system by end users. Continuing education is provided during normal expert daily operations in the field of medical services (Yfanti & Sipitanou, 2016). The essential requirements for instruction are to improve the existing information and the nature of health care; reduce work pressures; improve basic reasoning, self-assurance, and activities; eliminate work errors; improve working conditions; and ensure proficiency and fulfilment (Yfanti & Sipitanou, 2016). CTU should occur whenever new advances arise, and it is essential for improving and guaranteeing the quality of medical services (Yfanti & Sipitanou, 2016).

The current participants accepted that HIPAA’s CTU preparation improved the

congruity and data security of the executives ’inside associations. The associations ’ training programs are thorough. Training must be tailored to specific jobs and should replicate the work tasks that have most successfully increased users ’acceptance of technology (Crowley et al., 2019). The programs ensure that each individual is prepared on privacy and security every year, and that their access is removed if they do not finish the training (Walsh & Cooper, 2018). Using training programs, hierarchical pioneers can unravel the innovative difficulties found in certain associations (Sindhuja, 2014). The pioneers of an association comprehend the importance of having sufficient data security controls inside basic frameworks. However, some fail to complete security training and mindfulness programs in their associations (Ismail et al., 2014).

Data from the Hierarchical Record Newsletter of Organization X indicated that the association used a web-based training, document-sharing, and record-stockpiling administration that allowed staff to collaborate and share data through any device (work PC, telephone, tablet, etc.). The program makes it simple to transfer content, sort out records, share connections to information, and oversee document and envelope consents. Using it, the staff can work with partners inside and outside of the association at any time and place and from any gadget. Every user is prepared in the best way to log in to the document sharing through a web GUI.

The HITECH Act also imposed new requirements on medicinal service associations in regard to meaningful use criteria, which prompt repayments for patient care from the U.S. government (Kruse et al., 2015). The Act included augmentations to HIPAA for assessing the insurance of members, which is the job of the IRB (DeMeo et

al., 2016). In the authoritative record of IRB human subjects, an individual-review case report is expected to create information that can be shared for instructive and clinical objectives. The association's strategy says that a solitary case report is a review examination of one to three clinical procedures; however, this is not looked into, and it must be affirmed by the IRB, and in the event that multiple cases are associated with the diagnostic movement, the action will require examination. Although the association's IRB endorsement is not required, explicit HIPAA Privacy Rule commitments apply to the use and affirmation of PHI for a solitary case report. Researchers who omit HIPAA identifiers from case reports before the information is exposed are not required to obtain marked protection approval for the reports. No delineations or photographs for a situation report should require the identification of the patient. Researchers are also not required to present approval structures to the IRB for surveying.

In the authoritative record, P2O1 noted that operational duties guarantee that exploratory access to clinical information adheres to government requirements to follow the IRB's strategies, desires, and endorsements. For instance, if an IRB affirms that a specialist can distinguish information, then the information group is responsible for conveying only the identified information to that investigator. There is a large group in the association that encourages this procedure. There are also groups of security staff helping and guiding it, and there are groups of individuals producing safe, systematic conditions for investigators to analyze information without being prone to undermining and with solid security and encrypted information. Multiple encryption procedures and components are used to guarantee that information is divided among legitimate clients

(Kaur & Kaur, 2018).

The organization document IRB Compliance Training and the HITECH Act require all data breaches of HIPAA secrecy to be accounted for. Specialists must understand and agree to HIPAA guidelines related to their research. Under the HIPAA Privacy Rule, individuals must meet explicit prerequisites before using or revealing exclusively recognizable patient data for inquiries.

The IRB has a relationship with the information trust for identifying and improving the information that researchers gather from their activity. There are conditions regarding where and how researchers may store that information and limitations on subsequent sharing. Those conditions are generally managed through arrangement and instruction of the users. Nonetheless, the instructional class expects individuals to have an essential comprehension of the HIPAA prerequisites. If individuals are required to finish the course, they should first finish the required essential security seminar on the association's intranet site.

RAT is a theory that forces the investigation of encounters and data (Cohen and Felson, 1979). When estimating the various reactions of the participants, a remarkable differentiation among them became apparent. The research findings on data breaches leading to the theft of patients' data have likewise contradicted the findings detailed by Cascardo (2015), who claimed that a large amount of HIPAA information infringements relate to worker robbery. My review of the organizational documents confirmed the participants' claims that there are government security standards for EHR systems, but internal security strategies will not line up with data-breach management without a key

workforce and ranking IT security managers in the absence of a guardian. When the data breach happened because of a missing component, the senior IT pioneer and conceivably the authorities ought to have been included. Sessions (2019) reported that the most exploited areas of EHRs and electronic health information (EHI) are the users, hardware, software, and networks. HIPAA data breaches have been identified with burglary of workers and with unexpected misfortune. The information about data breaches revealed in this study may add to the more extensive field of break-ins that executives and data security officers look into. This study revealed that a well-defined security strategy developed by IT security professionals is critical to the success of the EHR systems used by organizations.

Table 1

Frequency of First Major Theme

Source of data	Requirements based on government regulations		
	Health Insurance Portability and Accountability Act (HIPPA) (*f*)	Health Information Technology for Economic and Clinical Health (HITECH) (*f)*	Protected Health Information (PHI) (*f*)
Participants	9	4	9
Documents	13	8	9

Note. *f* = frequency

Theme 2: Best Industry-Standard Security Measures

The importance of using the best industry-standard security measures in EHR systems was the second theme to emerge from the data analysis, and it was addressed by

all the participants. Strategic methodologies used in the adoption of EHR differ and can use a hierarchical, government-driven, concentrated framework, a granular perspective that includes new medical-service data frameworks, or a center-out approach in which medical-care suppliers and IT merchants continually change the data frameworks to follow public data norms (Fragidis and Chatzoglou, 2018). Fragidis and Chatzoglou (2018) noted that the U.S. used a granular perspective to advance the cross-country reception of EHR. Medical establishments are responsible for using a record framework that guarantees proficiency, protection, and security, depending on how the providers work (Janchenko, 2020).

One significant area for IT security frameworks is access control, which guarantees that the right authorizations are given to clients in IT frameworks, and that no more access than is required is conceded to each record (Azeez and der Vyver, 2019; Kaušpadienė et al., 2019). The evolution of EHRs and interconnected devices has been identified as one of the biggest contributors to increased concern about data breaches related to healthcare (Coventry & Branley, 2018). Technologies such as EHR can disrupt workflows, increase the time needed to perform tasks, and reduce face-to-face communication with patients, resulting in resistance to EHR systems (Barrett, 2018). The findings showed that IT security professionals implemented the best industry-standard security measures in the EHR structure and architecture, but that the HIPAA security guidelines were not entirely clear and were hard to implement because of terms like “reasonable” (Colquhoun et al., 2020; Cronin, 2020). Other studies have analyzed how associations execute the best practices for advisory alerts (BPAs) in the framework, and

how doctors see the usefulness of these cautions in their work (Chen et al., 2018). According to Chen et al. (2018), users' behavioral intentions (BI) reflect how an innovation will be used and how medical staff will acknowledge it.

This theme included several subthemes mentioned by the participants and the organizational documents. These subthemes are required for IT security managers to verify information in electronic patient record systems. Table 2 shows four critical subthemes of the security techniques introduced by this study and the frequency (number) of participants who executed each to secure data in EHR systems. The table also shows the quantity of supporting records that contain at least one of these security techniques for medical records.

Table 2

Frequency of Second Major Theme

Source of data collection	Importance of well-defined security controls			
	Authentication (*f*)	Authorization (*f*)	Encryption (*f*)	Data integrity and confidentiality (*f*)
Participants	2	1	3	9
Documents	7	7	6	17

Note. *f* = frequency

Authentication

The participants talked about how important authentication was to verifying patient data in EHR systems. A significant part of that data can be sensitive, whether it

involves innovation, monetary or individual data, or other information for which unapproved access or openness could have unfortunate results (Lord, 2018). The goal of authentication is to increase the security of approved clients and prevent unapproved access (Kaur and Mustafa, 2019). Hence, passwords should be long and tangled. All the participants indicated that they had applied verification strategies as the first step to guaranteeing information in patient records. All participants noted that a security authentication procedure followed by IT security managers, guaranteed the security of information and improved its quality. These views of the participants were reliable, according to Sudha (2015). Participants 1O1, 2O1, 4O2, and 5O2 reported using multifaceted confirmation to give users' access to information in modular applications of EHR systems. Multifactor authentication serves as a centralized access-control mechanism to secure data in the cloud (Anakath et al., 2019). It is also more dependable than using the most complex passwords, and this makes it essential for forestalling database break-ins (Simon, 2019).

In critiquing the extensive documentation provided by the IT security managers on behalf of the healthcare systems' information security departments, I found that all the participants in my research pool followed strategies focused on the best way to address particular kinds of security occurrences, including the unplanned revelation of personally identifiable information (PII) to unapproved outsiders. They also described the prerequisites for revealing and reacting to episodes identified with the treatment of sensitive data. In their encounters, participants said that they followed these strategies to verify information in their EHR systems.

The information security documentation given by the participants also showed their insight into and comprehension of the prerequisites for guaranteeing the correctness of information about the users of modular EHR applications. Participants 1O1, 2O1, 3O1, and 4O2 emphasized that IT security managers needed to consent to HIPAA requirements or principles in order to verify PII in EHR systems. These discoveries also upheld the main thesis of this study.

The findings of this study support previous research. Wang et al. (2019) reported that the authentication of users was the primary line of defense for verifying stored electronic information and forestalling data breaches. Zhou, Sun, Song, and Song (2017) cited the significance of authentication in the electronic storage of sensitive data to ensure that PII is not compromised. They argued that authentication conventions stood in for foundational security strategies and have been widely used in electronic banking, web-based shopping, video gathering, and electronic voter registration. Along the same lines, Zhou et al. (2017) aligned with the findings of this study. As far as they could tell, Participants 1O1, 2O1, 3O1, 4O2, and 5O2 had checked the importance of using multifaceted authentication to distinguish the users who had access to information in modular applications in EHR systems.

Current security guidelines such as HIPAA's permit the use of fundamental security controls, such as multifactor authentication to verify information in distributed computing (Gantt, 2014). Participant 1O1 said that the use of multifactor verification follows HIPAA PII guidelines and regulations. Participants further clarified that they each used the Identity Authentication Management (IAM) instrument through Microsoft's

Active Directory (AD) service to permit users to access appropriate modules or embedded applications in the EHR system. Participant 301 said, “We have the lawful rights to ensure the data contained and stored historically is gotten to using multifactor confirmation.” Cresswell et al. (2021) reported that IAM is a security device used for dealing with passwords and authorizing access to specific administrations in a distributed environment. Participant 402 clarified the systems of multifactor authentication by describing HIPAA’s orders and gauges. Participant 502 said that multifactor authentication is done in all frameworks that approve users before granting access to EHR records. Simon (2019) saw multifactor authentication as an attempt at oversight because of security concerns about using unscripted SMS text messages on phones.

Heatherly (2016) highlighted the size of multifactor authentication as a safety effort to protect users ’information. He clarified that validation is accomplished by combining something users know (a password) with something they have (an identifiable electronic token or physical device). The use of known traits and trusted beliefs can influence the complexity of passwords (Alarcon, Lyons, Christensen, Bowers, Klosterman & Capiola, 2018). This authentication instrument also supports the findings of theme 1. Each participant considered the use of multifactor authentication for all users of the EHR system as one of the most significant safety efforts in EHR systems.

These discoveries showed the importance of safety efforts in EHR security strategies and bolstered the RAT framework used in this study. The discoveries were predictable, given how low-end, problematic innovations such as EHRs have forced healthcare organizations to change their business rationales. These changes were

completed by associations improving items and framework execution in a time of constant innovation by abusing the interruptions (Goldstein, 2015; Sultan, 2015). A large number of the participants reported using security strategies such as validation in modular EHR applications to verify electronic records and limit the risk of data breaches. The IT security managers understood RAT and thus implemented security strategies to protect the information in EHR systems and improve the productivity and execution of their embedded applications. The discovery of the significance of such security strategy efforts bolsters RAT. These discoveries have made IT security managers hold onto RAT as an opportunity to lead their associations toward change (Kranz et al., 2016; Osiyevskyy and Dewald, 2015). In addition to building a secured EHR environment, IT security managers noted that verification improves the profitability of electronic data security (Li and Wang, 2019).

Authorization

Heatherly (2016) characterized authorization as the right given to users to access electronic records. He underlined the significance of fluctuating authorization levels for verifying information (Heatherly, 2016). Participants 1O1 and 2O1's responses upheld this view. Both clarified the importance of authorization as an all-around security measure in EHR systems. The participants and the organizational documents both implied that authorization limited human data breaches. Cusack and Ghazizadeh (2016) said that authorization depends on configuration of users' access. Participant 1O1 said that authorization is a layered way to deal with security concentrated on jobs and consent. Participant 2O1 repeated the claim that authorization provides consent for jobs in order to

control internal dangers. Participant 5O2 likewise stressed that authorization depends on perusing and composing to get consent for jobs.

Companies should evaluate rules of least privilege and role-based privileges and leverage machine learning to confirm normality (Novinson, 2020). The participants' reactions showed that a powerful approval instrument secures the information in electronic records. This finding was predictable in light of the writings of Foresti, Paraboschi, Pelosi, and Samarati (2018). Foresti et al. (2018) said that authorization is provided by way of administrative access rights, which permit users to access fluctuating information while maintaining protection and privacy. For instance, Participant 1O1 said "If Person A needs to get to the information from my application, I will give it a security template that concedes its entrance to do a particular capacity, and in the event that they need more than one sort of access, I will give it various security templates dependent on that consent level." Participant 2O1 said, "User approval might be made sure about by Active Directory. Each time a user signs into the EHR system, Active Directory deals with the confirmation and authorization rules." Participant 3O1 said that they gave the least privileged access and composed access to users just for determined application modules.

These discoveries bolster the RAT framework used in this study, in that IT security managers ought to create strong character-identity management foundations to guarantee that authorization rights are granted or denied depending on users 'jobs and relationships to the health-system organization (Jathanna and Jagli, 2015). This theme is consistent with RAT, the motivation behind this study, and answers the research

question. The participants claimed that authorization is the best security strategy for forestalling data breaches in EHRs by shielding patient information. The health-system documentation examined included approaches and systems concentrated on consent rights for approval of information to limit data breaches in EHRs (Foresti et al., 2018). Past research led to the discovery of access rights, such as cancellation, provisioning, and crippling of records depending on the association's endorsement procedure.

Encryption

The third subtheme was encryption, a security strategy used to scramble or unravel information through access approaches (Hidayat and Mahardiko, 2020). When asked what the IT security managers 'involvement was with EHR security, Participants 1O1, 3O1, 4O2, 5O2, and 6O3 reported that encryption was a significant system used to forestall unapproved access to EHR database tables.

The method of encryption used differed among the participants. Participant 1 said, "Encryption is a single direction hash or can be used as a reversible hash contingent upon the undertaking's seriousness." He added that, "Encryption is used for information that is very still or in transport when it leaves the secured zone." Participant 3O1 said that encryption was one of the means of assurance against information breaches. Participant 3O1 demonstrated how the use of encryption is important for verifying information but worried that complex encryption might restrict this. This agrees with my findings and comparable results by Hadavi, Jalili, Damiani, and Cimato (2015), who found that perplexing encryption can be tested while storing information electronically and looking after security. In addition, encryption protects information veracity, yet its multifaceted

design has limited its practical use (Hadavi et al., 2015). Participant 4O2 portrayed the encryption of information as an unpredictable procedure for scrambling information using an encryption key. Participant 5O2 implied that the encryption of information is one of the first steps taken by IT security managers secure PII and limit data breaches. Jho, Chang, Hong, and Seo (2016) confirmed these findings about the main subject, and Jho et al. (2016) said that another system of maintaining information security and protection is to use encryption. These findings about complete encryption justify information privacy, which was predictable given the reactions of Participants 1O1, 301, 402, and 5O2.

I analyzed and criticized the health-system policy and procedural documentation in order to verify that it upheld the participants ’reactions to the use of encryption. All participants verified that IT security managers followed good procedures and strategies for encoding information in transport and still made sure that information was private in EHR records. These findings likewise supported the principal topic of this study. The participants confirmed that their strategies for encryption were guided by the NIST Cryptographic Algorithm and Module Validation Programs (Gordon et al., 2020). These findings were upheld by Lankford (2019), who said that Federal Information Processing Standards (FIPS) 140-2 is the proper way to ensure an encryption calculation. Mug (2017) affirmed the findings in the authoritative reports that all PII in EHR databases should be encoded to prevent information breaches. EHR innovation has improved framework execution, leading it to be engaged by huge associations that at first saw it as unremarkable (Crockett et al., 2013). Accordingly, encryption is an urgent security

strategy used by IT security managers to limit breaches of EHR databases.

As identified with the RAT framework, the findings of this study suggest that the business procedure of the whole health system makes information secure and progressively more open to associations at any place and time, which underpins the findings of Goldstein (2015). With all-around security strategies like encryption, IT security managers can verify databases in EHR systems, and this will improve the execution of their frameworks. The first theme underpins one of King and Baatartogtokh (2015) four key components of the idea that "officeholders in a market are improving in the way of supporting advancement. These findings are attached to the use of encryption as a system for continuing development by verifying information in the EHR systems, which limits data breaches.

Data Integrity and Privacy

The fourth subtheme was data integrity and confidentiality. With the rise of electronic medical records for patients, the integrity and privacy of patients' sensitive data, or PII, is currently significant (Dhasarathan, Thirumal, and Ponnurangam, 2015). Two of the nine participants stressed the importance of the integrity and privacy of PII. Babrahem and Monowar (2018) argued that healthcare organizations should ensure high confidentiality of patient records, and this is a standard requirement for the development of the EHR system. Clinical data might be by the physician first, but as this might be excessively tedious during clinical consultations, physicians might also use scribes to enter patients' data into EHRs during consultations, and this has exacerbated worries about tolerant security (Kroth et al., 2019; Tutty, Carlasare, Lloyd, & Sinsky, 2019).

According to Van Dyke (2019), changes caused by EHR have included additional work for providers, mostly due to documentation and other administrative tasks that are peripheral to caring for patients (Yates, 2020). Duty to the patient is a unique professional responsibility that regularly challenges physicians' time management (Pitre et al., 2018). Participant 1O1 said that "information protection in EHR systems is a significant worry of patients." He added that he agreed to orders for activities or got them by relying on government or medicinal-services information. Participant 2O1 reported that information trustworthiness and protection was maintained through adherence to HIPAA rules and guidelines for verifying PII. A survey of the three system policy and procedural documents confirmed that the security approaches of their health systems were based on HIPAA and NIST protection prerequisites to maintain information respectability and security using safety efforts such as multifactor authentication, encryption, and authorization (Kayser et al., 2019). Sudha (2015) confirmed the participants' experiences, noting that sensible security prerequisites that tend toward confirmation, information obscurity, and patient protection improve the integrity and privacy of patients' PII. Gootman (2016) reported that a multifactor authentication procedure, such as a solid secret phrase and a personal identification verification (PIV) card, will limit the risk of programmers accessing PII.

These findings line up with the aftereffect noted by Christensen (1997), that the use of distributed computing by associations has reached its present position because of the disturbance of IT space. Notwithstanding all the security challenges, this study shows that associations have made efforts to shield the information in EHR systems. The

significance of these safety efforts prompted that disturbance, which researchers have noted happens when distributed computing items spread widely and are embraced by customary associations (Christensen, 1997; Surya, Mathew, and Lehner, 2014). Storing information through distributed computing has disturbed the business rationales of associations, which generally store data in physical server farms, bringing about new specialty units that perform exercises of different value (Christensen, 2011).

The second theme emphasized the need to use security devices and encryption. Participant 4O2 said that their association maintains the security of its EHRs with sixty to seventy classes of instruments. I discovered acknowledgment of a portion of these apparatuses in the association documents. A few instruments were referenced in the associated documentation; Right Tool was viewed as phenomenal. In any case, as a result of security concerns, the association restricts its use of them. It uses only a few suggested inside instruments with EHR databases, keeping a safe domain through constant, coordinated effort.

According to Participant 4O2, the security of the framework is maintained through inspecting and auditing. Unauthorized users can take advantage of weaknesses to get unapproved access or favored control of working frameworks, end-client applications, venture applications (in the cloud or on the premises), programs, network gadgets, and servers (Cavalancia, 2020). Compensating controls should incorporate limited organization access and impaired network administration or programming parts to secure weaknesses that could be taken advantage of through network access (Vigna, 2019). Participant 4O2 said that every server requires patches at the operating system level. The

EHR must be fixed for both security and usefulness. Outsider or vendor EHR-integrated application software is fixed. Patches are applied within a fixed time period after being recognized. The normally secure boundary of confinement by detachment from the system when something isn't vital is traded off when the security group is sent to the location to secure the equipment on which the EHR is stored. Participant 4O2 recognized the need to shield the environment from phishing and malware. The documentation from Know Cybersecurity shows that it investigated the impact of malware and procedures to address it.

Mirsa et al. (2019) reported that considerable and growing threats exist for medical information stored in cloud environments. The organizational document titled "Medical Record System" indicated that the private cloud option requires cryptography, which promotes the encryption and decryption of data storage (Kiruthika & Laxmi Sree, 2014). The participants and the document "Self Protection" stated that cloud-based EHRs are typically encrypted at the transport level. Because patient data is governed by privacy regulations regardless of storage method, the participants noted that cloud-based EHR encryption is less expensive than on-premise encryption, whereas "Self Protection" stated that decryption is more expensive but includes the benefits of secure implementation and remote accessibility. All nine participants said that the organization's EHR was on premise, and that its hot backup was provided via a third-party commercial organization, although the organization owned and managed the hardware. Therefore, Participant 2O1 said, when a patient's EHR must be obtained from private cloud storage by a healthcare professional, the decryption must be approved by the hospital before the files can be

accessed.

Seh et al. (2020) found that health care records were susceptible to both internal and external threats, such as hacking, data loss, and improper disposal of sensitive information. Participant 4 said in the organizational document “Medical Record System” that breaches attract expensive lawsuits, which cause the information security department to be on alert. They developed a set of networking and system support tools with a centralized IT service. The traffic on the VPN in the private cloud was fully encrypted. All access to the cloud has been integrated into the active directory system.

In the literature, vulnerabilities in a system may be uncovered by an agent through analytics and by understanding patterns and trends in the data (Jouini et al., 2014). Standard encryption methods today provide insufficient means to operate on encrypted data without decrypting it first. But encryption restricts the likelihood of outsourcing externally stored information (Bos, Lauter, & Naehrig, 2014). According to Participant 3O1, the amount of time that data is in the clear is relatively short. It is only when the organization is doing analytic views in the cloud that the data is dynamically decrypted.

Encryption is a tool for ensuring the privacy of medical data. It restricts the functionality of actions performed on such data. The encryption that is used today provides insufficient opportunities to act on encrypted data without decrypting it first (Bos et al., 2014). The data is partitioned so that if a partition is compromised, it is isolated or insulated. People can penetrate only so far into a data environment before hitting a firewall on another layer of decryption.

Online performance is one way of recognizing malicious activity, indicating

through the RAT propositions the ubiquity of a target and the absence of protection (Pyrooz, Decker, & Moule, 2015). From all the participants ’responses, it was evident that all their senior IT leaders understood that their organizations were targets of potential cyberattacks (Yarachi & Gopal, 2018). Through testing, each senior IT leader had confirmed that there was protection within their organization. However, clinicians in public health settings reported greater dissatisfaction with EHR due to difficulties with documentation and interface navigation and with variation in processes and terminology (Crowley et al., 2019). Jackson (2015) said that vulnerability is not an issue of exploitation but of a motivated offender. This position takes the burden off the victim and places it on the shoulders of the offender. However, few definitions place constraints on offenders ’situations, presumably to encompass as many types of offenders as possible.

The RAT aligns with patch management and testing because if you eliminate patch management, you become a suitable target. The RAT attempts to define the minimum conditions necessary for a crime and then to focus on the elements of the crime depending on the offender. Whereas the RAT produces characteristics of situations, targets, and victims of crime, it only holds that the offender must be motivated to seize the opportunity.

The RAT and LRAT are aligned with the theme of protection of infrastructure because both are correlated to victimization. Although the RAT accounts for criminality when possible offenders and victims are in the same environment at the same time without a capable guardian, it does not satisfactorily address victimization and offenses in non-physical areas (Choi & Lee, 2017). This is because the theory assesses the physical

confluence of space and time between the victim and offender. Another aspect of the LRAT is that it is used mainly to assess crimes that can be carried out online, and for which individuals can end up in places where they become suitable targets for victimization (Choi & Lee, 2017). In relation to the RAT, senior IT leaders of an organization are depicted as targets while implementing cybersecurity strategies and as remaining targets while protecting their EHR system from data breaches.

Protection of the environment is aligned with the tenets of the RAT. Participant 4O2 said that their organization investigated twenty to thirty security incidents daily, and the firewall blocked millions of incidents. The RAT includes visibility, accessibility, and guardianship. According to Cisco Systems (2018), numerous medical services suppliers have embraced network division to add extra safety controls and confine admittance to basic frameworks and patient information. Medical-service suppliers have adopted division based on isolating various frameworks or capacities into more modest portions while controlling traffic inside sections. Organizations are increasingly implementing security controls, but often not enough (Brown et al., 2019; Stein et al., 2020). RAT's approach to crime depends on the ability to surround offenders and targets in the absence of a capable guardian. Participant 2O1 said that their organization used a private cloud and had a security team that focused on eliminating threats such as cyberattacks and hacking of sensitive information. RAT accounts for criminality when possible offenders and victims are in the same environment without a capable guardian, but it does not sufficiently address victimization in other locales. This is because the theory is focused on the physical proximity of the victim and the offender (Choi & Lee, 2017).

According to the RAT approach to crime, the absence of guardianship by EHR cybersecurity can result in increased cyberattacks. The RAT can be mapped onto information security and includes recommendations of vulnerabilities and resolutions for IT security (Elmaghraby & Losavio, 2014). Senior IT leaders should consider using the private cloud to for security to minimize EHR cyberattacks because this compensates for the shortcomings of the RAT. Senior IT leaders might also head off cyber attacks by focusing on criminals ’motivations. Cohen and Felson (1979) argued that the RAT is primarily a theory of victimization focused on individuals who are suitable targets for motivated offenders. In the protection of infrastructure, however, the RAT is used to specify the conditions necessary for a crime to occur and to focus attention on the factors that are independent of the offender. At the same time, it specifies components of situations, targets, or victims and notes that offenders must be motivated to take advantage of them.

Suitable targets include people who require protection to prevent attacks. The LET was the rival theory used for this study. It is aligned with the theme of patch management and testing. Research based on the LET has shown that the position of a victim should be brought to attention when victimization is studied, as the victim’s behavior may have increased their chance of being victimized (Kokkinos & Saripanidis, 2017).

The literature contains insights into cyberattacks in healthcare and aligns with the data from my own interviews and organizational documents. Healthcare is a prime target of cyber attackers, as the impact on it is unprecedented. IT has an enormous effect on

social well-being and national security (Kruse, Frederick, Jacobson, & Monticone, 2017). Cybersecurity has become an integral part of every organization, and the mass usage of networked systems has given rise to critical threats and vulnerabilities with significant social impacts (Kruse et al., 2017).

Theme 3: Emerging Interoperability With a Security and Privacy Program

Another theme was research into advances in reliably assessing security angles and improving the security. “Interoperability” has been characterized by the Institute of Electrical and Electronics Engineering (IEEE) as describing at least two frameworks or components with the capacity to trade and use data (Bates and Samal, 2018). Interoperability is one of the most notable and well-examined subjects in the medical services (Thompson and Graetz, 2018; World Health Organization [WHO], 2018), and businesses expect future interoperability arrangements to improve care for patients increase usefulness (Kuiler and McNeely, 2018).

Studies have shown that new technologies create uncertainty and put pressure on organizations (Holotiuk & Moormann, 2018). EHR configuration problems have also been hard to evaluate where there are framework impediments, for example large records that create adaptability problems, perception difficulties of with total information, and a lack of framework to-framework interoperability (Sultanum et al., 2018).

Legislative acts such as the ACA and 21st Century Cures have led the federal government to accept a larger role in the progress of interoperability, through legislative rules and an educational plan for accountable care organizations and health information organizations associated with the Office of the National Coordinator for Health

Information Technology (ONC) and the Centers for Medicare and Medicaid Services (CMS) interoperability motivation programs (Atkinson et al., 2018; Kondylakis et al., 2018). Although they provide important benefits, EHR systems also introduces new problems for providers, such as the lack of interoperability between systems from different vendors (Courtis et al., 2018) .

Medical care regularly engages in rational rearrangements that are necessary for data security (Ismail and Yusof, 2018). The ubiquity of internet access coupled with the increasing adoption of mobile phones and the internet of things (IoT) has created a foundation for approaches that can handle unprecedented amounts of health information records (Chernyshev et al., 2019). The HEI standards, for example FHIR, are empowering frameworks to trade information and support information access, and the reception of technical interoperability guidelines is expanding, but the foundations for information liquidity are still lacking (Heyde, 2018; Offodile and Ho, 2018).

Reflecting on current work methods and looking for ways to improve them encourages staff members to think outside the box (Rashkovits, 2019). In a study conducted by Gibson (2020), the three key elements identified by a security program were an understanding of the threat landscape, the establishment of operational objectives and priorities, and security infrastructure and design. Moreover, various authors have asserted that a big part of all breaks are brought about by workers' absence of information on close-to-home information and rebelliousness against association data security strategies (Chua et al., 2018).

The medical-services industry has directed a lot of work toward specialized

interoperability, also known as structural interoperability (Braunstein, 2018; Lane et al., 2018; Wang, 2018). One such development consolidated the use of data loss prevention (DLP) programming. DLP is a procedure for guaranteeing that clients of an affiliation don't send sensitive or fundamental information outside the framework. EHRs' resource limitations also inhibit their ability to provide intrusion protection, rendering devices vulnerable to hacking (Rathore, Mohamad, Al-Ali, Du, & Guizani, 2018; Sun et al., 2018). Participant 5 said that DLP devices are used to recognize regions of sensitive data in databases, servers, and record shares. Sensitive data is correctly recognized as alphanumeric data that follows the arrangement of a clinical record number, a patient number, a social security number, and charge card numbers. Upon unmistakable verification, the system reviews ahead to determine whether the zone containing the sensitive data is reasonable. Du and Wang (2019) highlighted how intrusion detection systems have numerous asset necessities and can devour trillions of bytes each second. Through the use of honeypots, the traffic would be made insignificant because information would be caught from sources that claim to be authentic. Therefore, a security strategy for identifying pretend resources could consume the time and resources of the attacker (Du & Wang, 2020).

According to Anderson (2018), a security program should address procedures, personnel, and training in order to provide an approach that is organized and methodical (Kakucha and Buya, 2018). Electronic clinical records present multiple points of interest and seem to create novel risks for restorative administration affiliations concerning protection and security. It is important for electronic clinical record programming

merchants to see dangers and stresses straightforwardly and adequately. Barrett (2018) noted that the intricacy of the medical-care industry keeps expanding as services conveyance becomes more tolerant and focused and the innovations in patient care become more deterministic. Nonetheless, contemporary professionals have claimed that improved interoperability is required for EHR access, and a shift is needed in data-sharing worldviews to improve patients' and administrators' access to health information (Essen et al., 2018; Finset, 2018). For this reason, medical-services suppliers and clients of EHR frameworks keep open lines of communication with EHR merchants, educating them about the restrictions of the EHR to aid future advancements (Barrett, 2018).

The Authoritative Record Newsletter says that an understanding of the spread of information electronically can be gotten from tablets or personal computers, however provisory, in a particular area or on a particular server. A balance must be struck between security measures and the usability of healthcare systems (Dameff et al., 2019). For patients who visit multiple offices for medical services, openness of data starting between the organizations is beneficial. Participant 5 said that the adaptability of electronic records and documents allows specialists, patients, clients, and arrangement areas to be included rapidly and productively at low cost. Researchers have suggested that this puts patients at risk, because the IT systems do not communicate with one another, making cross-referencing difficult and potentially leading to errors (Foster, 2020). Although changing from a hard-copy paper framework to an electronic framework may be scary at the outset, it lets the health system increase its monetary gains and spare time (Willard-Grace et al., 2019).

Protected medical information (PMI) includes patient data, such as comparative information that can be followed back to people, and health, insurance, and payment data. New medical devices and cell phones that screen patient data and interact through the web are particularly helpless against the extensive scope of digital dangers (Meng et al., 2018). Workstations, smartphones, and USB sticks are not permitted to hold private information in many health systems' policies. Participant 3O1 said that the PMI could verify a patient's consent remotely during clinical treatment. The health system is committed to making legitimate strides toward only discharging vital data. The inability to implement these measures will lead to fines and repayments. Atluri (2018) indicated that both before and after the move to EHRs, there have been dangers to address, and there ought to be clear jobs and obligations for dealing with those risks.

According to Participant 2O1, gadgets designed to debilitate insider dangers make use of checking, recognition, moderation, and discouragement. DLP apparatuses might be used to identify and alleviate insider dangers and screen information use. Participant 3O1 said that measures to discourage the abuse of inside frameworks focus on four components: security strategies, checking, preventive programming, and preparation. Observation alone isn't acceptable for keeping up with insider dangers. It secures the goal but not the inspiration, and it is hard to perceive examples of abuse.

Participant 1O1 had a firewall and a security group responsible for guaranteeing the protection of hierarchical and patient information. The hierarchical archive Considerations for Unified Communications, which contains information recorded and put away, requires security. The security is provided by documenting the information on

servers and using DLP items to control access to it. The association has division firewalls in its framework that guarantee its most significant applications remain secure. Division firewalls help to stop threats by providing an extra layer of security where it is generally needed. The main role of the firewalls is to authenticate traffic inside the system. The association uses the firewall to give extra protection to sensitive, high-risk parts of the system.

Participant 2O1 said that the healthcare system attempts each step of asking the question, providing information, and examining it to guarantee that it is in a safe and auditable condition. The healthcare system no longer allows examiners to download information to their work areas and possibly bargain with that information, regardless of whether it would be a worthwhile trade-off. There is no alternative to destroying the chain of authority for information on the executives, which remains in a protected domain through each step of the procedure.

Participant 2O1 said that information was leaving the organization, in transit, and entering electronically shared status. At that point, obviously, there could be frontal assaults on the customer themselves. Each of those stages represents a potential security danger. The oversimplified approach to managing information leaving an association that is the best in its class is to encode it before going sending it into shared electronic status. The health system uses start-to-finish encryption of information, and the information isn’t decoded until it is securely in a trusted domain. At that point, the information can be unscrambled on request so that when the healthcare system must investigate or use it, it will be decoded and then encrypted again afterward.

The advantage of constant improvement in avoiding information mishaps was a major theme in the interviews and documentation reviews. Rosenbloom et al. (2019) pointed out that hospitals are hesitant to commit to data sharing across networks. Healthcare system data frameworks include numerous advances necessary for maintaining and sharing patients' information electronically. Machine learning and artificial intelligence are among the major innovations for healthcare organizations to consider (Yu et al., 2018; Yu & Qian, 2018), so as interoperability arrangements foster development, new advances such master data management and white space data should be investigated to build respectable security arrangements (Zhang et al., 2018). Interoperability is fundamental to medical services, as strong value-based consideration becomes the standard and no single element can deliver content at will, and it results in cycle support that is reasonable for the best clinical and specialized proofs and requires universal healthcare that further develops the wellbeing of the populace (Rajkomar et al., 2018).

According to Luna et al. (2016), data breaches are a larger danger to medicinal-services associations. Hackers use malware to structure relationships outside of the frameworks that hold the stolen information (Manworren et al., 2016). In a reasonable structure, the RAT is appropriate for exploring means of data-loss prevention. The RAT lines up with DLP in that it provides a framework for avoiding misfortune and taking care of problems in an organized manner. Wrongdoers' activities can be taken care of by changing natural signs. With these data in position, data loss can be anticipated if the costs are made to be higher than the advantages of carrying out the wrongdoing. The

RAT helps senior IT stakeholders by reminding them that they remain targets and should use security strategies to limit EHR cyberattacks and shield their frameworks from information breaches. Obstructions can't provide insight into real insider dangers. The RAT presents more thoughtfulness about society at large.

Table 3

Third Major Theme

Source of data collection	Organizational documentation		
	Small Organization I (*f*)	Medium Organization II (*f*)	Large Organization III (*f*)
Authentication		2	
Authorization	3	3	
Data integrity and confidentiality	2	4	1
Encryption	3	3	
PHI	3	6	
Policy		12	4
HIPPA	2	8	1

Note. *f* = frequency

Applications to Professional Practice

This study implies that senior IT pioneers in the medical-services industry should use security procedures to prevent EHR data breaches. In the medical industry, securing patient data is the first concern of leaders (Peterson et al., 2018). This study is critical because this issue involves many medical-services associations where concerns about

patients' wellbeing and risks are pervasive (Green, Brandt, and Miller, 2018; Priestman et al., 2018).

There are many advantages to EHRs, including the availability of enormous amounts of health information, which is greatly improving healthcare services (Techapanupreed and Kurutach, 2020). One IT consequences, however, is that organizations might benefit from EHR security strategies. Aceto et al. (2020) reported that cloud-based architectures are being adopted by healthcare providers largely because they improve the efficiency, simplicity, development, and deployment of health information systems for gathering, processing, and transferring EHRs. EHR architectures also support medical activities by providing apparatus and assets for conveying a variety of data, including perceptions, expectations, dashboards, cautions, and backup for crisis administration (Wang et al., 2019). Conversations about interoperability in the medical industry and regarding state and federal regulations stress the need for medical offices to use EHR strategies effectively.

Participants 1O1 through 5O2 focused on the need to continuously protect patients' PII to prevent intrusions and maintain privacy. Data privacy is an increasing concern of leaders, and privacy issues affect all types of stakeholders (Brauer & Wiersema, 2018; David & Dhillon, 2019; Hemsley et al., 2018; Mullings & Ngwenyama, 2018; Tavares et al., 2018; Tubaishat, 2018; Vitari & Ologeanu-Taddei, 2018). The hesitancy of medical-services organizations to carry out EHR strategies for interoperability could allow people to effectively share and decipher patients' information in heterogeneous frameworks (Blackman, 2017). Researchers may benefit from the

findings of this study by learning to develop strategies for reducing data breaches, unapproved access, and abuse of patient information. The controls set up by the strategies allow IT staff and management to control the movement of sensitive PHI. Preferably, the main individuals who should see the data are patients, insurance agencies, and physicians (Levine, Linder, & Landon, 2018). If the data move beyond that range, the internal IT security staff must research and fix the problem, which prevents them from doing other jobs, so controls to assist with this can help the IT division work more productively.

Implications for Social Change

According to Reeler (2015), social change doesn't happen simply due to circumstances and their logical results. It is set off by inward and external impacts considered by society. There are monetary and other reasons that medical organizations are focused on so forcefully by hackers (Tao et al., 2019). According to Tao et al. (2019), the assaults on medical associations are numerous, and the IT frameworks in medical services are infamous for using obsolete equipment and poorly defended software. Taking active measures to keep hackers out of EHRs is substantially less expensive than data breaches in which information is compromised (Kamiya et al., 2019). Furthermore, a large number of medical services associations use obsolete frameworks (Branch et al., 2019).

According to Barosy (2019), social change can be seen emphatically when people remembers a climate free from danger in which businesses' and buyers' certainty are reinforced by safe and private data. All IT industries could profit from the research in this study as it could help associations identify strategies for obtaining different kinds of

confidential and sensitive data (Henriques de Gusmão et al., 2018). Black Book Research (2019) reported that 93% of medical-care systems had suffered data breaches in the three most recent years, with 57% suffering more than five, leading to more than 300 million records being stolen since about 2015. Data breach emergencies set the stage for groundbreaking change by prompting novel ideas for removing imposters' influence (Reeler, 2016), fight data breaches, possibly the most shocking crime, and forestall any monetary or other benefits to the imposters. Genuine social change is predicated on restored attitudes, sound government intercession, and holding lawbreakers responsible for their activities by reacting to the clamor from survivors of data breaches.

Scholarly findings could have a profound effect on healthcare delivery by reducing the profits of medical facilities, which would have a great impact on society as a whole. This study might also effect social change by reducing the fraudulent use of individually recognizable data and individual health data in EHR systems. The theft of patient data can have a long-term impact on medical organizations and patients. EHR security strategies might influence the way doctors practice by allowing productive private access to records by approved clinical workforces. In the HIT context, medical-care associations should create opportunities for representatives to upgrade both the breadth and the depth of information obtained from external entities.

A few models incorporate joint efforts among colleges, research organizations, legislatures, clients, and providers to acquire outside data and information (Xie et al., 2018). Keshta and Odeh (2020) pointed out that security breaches create concern for healthcare providers. EHR systems allow access by both the clinical workforce and the

patients, something security strategies might take into account, for instance in the correspondence among health systems in the treatment of patients. Controlling access to information in multiple frameworks requires levels of granularity from single patients to whole populations (Demurjian et al., 2014). Without a systematic approach, medical-services suppliers and patients might face legal repercussions because of either lawful prerequisites or the unlawful release of data into public channels.

With regards to wasteful spending in medical services, Participant 1O1 argued that the federal government should dole out more severe punishments to reduce these crimes. A powerful measure for countering data breaches in medical care is to recognize the dangers that lead to information loss (Tu, Spoa-Harty, and Xiao, 2015). Moving medical data to the cloud quickly could prompt significant improvements to EHR security strategies, preventing data breaches and leveraging financial plans for future medical service administrations while reducing the impacts across the clinic's business. The findings of this study could ameliorate these effects and contribute to social change through improved healthcare services and reduced medical costs, leading to more affordable healthcare.

Recommendations for Action

This study's findings revealed three key security strategies IT security professionals can use in IT security awareness training and implementation. Powerful security strategies are important for preventing data breaches but present new difficulties that should be addressed by IT security managers, particularly with new technologies. A strong security strategy to prevent data breaches will pay for itself (Hausfeld &

Zimmerman, 2018). Strategies that have been demonstrated to be powerful in this review by IT experts include the following:

- Meeting requirements based on government and organizational regulations.
- Implementing the best industry-standard security measures.
- Implementing a security and privacy program.

These findings are valuable and support recent work on data security strategies for EHRs, just as the organizational documents do. The findings are vital for all health systems that store patient data locally, in warehouses, or in the cloud.

Pierre-Francois and Guzman (2020) reported that small and medium-sized healthcare facilities experience more difficulty complying with HIPAA's Security Rule. The participants in this study stressed the importance of security strategies for EHRs, and IT security experts should recognize as technology ceaselessly advances, new security problems will arise that must be addressed. When IT leaders rethink their strategies, they discover new and useful ideas for improving products and services while pursuing goals (Le Cong, 2019). With these advances in threats, security strategies cannot be relied on to continue as before. IT security experts should think about how to keep EHR end users, either internal or external, such as patients, educated and mindful of the development of security strategies to limit information breaches.

The findings of this review will be distributed after a CAO endorsement is obtained for this study. A two-page outline of the results will be sent to each of the nine participants. The results will also be distributed through scholarly networks such as ProQuest to undergraduates and researchers.

Recommendations for Further Study

This study revealed strategies used by IT security professionals to prevent EHR data breaches. The limitations were that the work focused primarily on the Midwestern United States. Repeating the study in other regions of the U.S. in light of their regulations and security requirements, and using a different conceptual framework and methodology, will benefit organizations and IT professionals.

This study adds to the security-strategies literature, but further research is warranted due to the small sample size and the use of qualified IT security professionals. Gao and Sunyaev (2019) noted that the adoption of cloud service models improves one are in which the healthcare sector suffers: the lack of health IT professionals. It may also be significant for primary care physicians' mandatory use of EHR systems, as enforced by industry and regulatory groups (Wani & Malhotra, 2018). Future research might explore of security strategies using larger samples or organizations.

Telehealth intensified in 2020 due to the coronavirus. Therefore, nurse managers recognized the importance of telehealth EHR because most of their patients are high-risk or elderly (Jason, 2020). Future interoperability arrangements should use normalized catch documentation, following chain-of-guardianship for information sources and information changes and upgrades (Kharrazi et al., 2018).

Finally, this study contributes to the body of literature on security strategies for EHR systems and may prove beneficial for security strategies in the areas of auditing and compliance, and to the legal departments of healthcare organizations.

This study included some important recommendations based on the literature

review and the collected data that must be addressed in EHR security strategies:

- Researchers should explore multiple approaches to encryption to identify the those that deliver the best data security.
- Further research is needed to explore the barriers preventing leaders from taking active security measures and investing in innovative strategies to keep their organizations relevant and prevent data breaches.
- Researchers should explore the key components of medical care, including telehealth, to understand the motivations and triggers of behavior changes that will minimize external and internal data breaches in organizations.

Reflections

During this study, my understanding of doctoral-level examinations grew extensively. I was tested and astonished by the degree of detail and organization that the study required, and I felt overwhelmed during the analysis stage. At times I wanted to stop, as I couldn't keep writing.

In 2014, I became more interested in being an information security professional when I started working for a nonprofit healthcare organization for the first time. As the information security specialist senior, I was aware of the importance of healthcare's reputation for using the best security strategies to prevent breaches of patient data. The personal, professional, and government requirements gave me the energy to pursue this study. As an IT professional with more than twenty years in the industry, I had some interest beforehand in IT security frameworks, standards, and strategies. But I limited my bias by allowing the participants to speak without expressing my own impressions and

used open-ended, semi-structured interviews to obtain rich, far-reaching information based on the participants ʼown experiences.

I was ignorant of how wide-ranging and deep a qualitative study is until I dove into the analysis stage during a pandemic. Enlisting participants for my study was a test, and all nine of my participants were inaccessible for extended conversations by either phone or email to plan meetings. Member checking was difficult to plan, yet on the basis of my colleagues ʼexperience, I learned that having the interviews auto-transcribed and having a five- to ten-minute overview afterward was the most useful under the time constraints.

Finding software to produce richer insights and produce clearly articulated, defensible findings backed by rigorous evidence was also a laborious procedure, since I needed to figure out how to use it appropriately for my study. In general, I was delighted with the interviews and how willing the participants were to impart their knowledge to me. This study identified well-characterized strategies that IT security experts can use to forestall database breaches in EHRs.

Through this work, I learned to design a qualitative research study. My academic and creative writing capacities have also improved since I enrolled at Walden University, and I hope to continue developing them. I now have the academic skills to confidently move on and further develop security strategies for electronic health record systems.

Summary and Conclusions

Maintaining the security of sensitive EHR data is essential to healthcare organizations and increases trust in users such as patients. The purpose of this qualitative

multiple case study was to explore strategies used by information security managers in Midwest healthcare organizations to prevent data breaches in EHRs. The specific IT problem is that some information security managers in these organizations lack strategies for preventing data breaches in their organizations ’EHR systems. I investigated strategies used to securing data in EHRs and answered the following research question: “What strategies do information security managers in healthcare organizations use to prevent data breaches in electronic health record systems?” Nine information security managers from three healthcare organizations, large, medium, and small, provided details on their a strategies, which included the following:

- Requirements based on government and organizational regulations.
- Implementation of the best industry-standard security measures.
- Pursuing interoperability with a security and privacy program.

There is an ongoing need for information security in EHRs because of the growing danger of sensitive data being compromised. Until security vulnerabilities are mitigated, organizations must be wary and gauge their security risks against the upsides of EHRs by using obvious controls and strategies. EHRs might be much more welcome if all these strategies were followed to secure data and protect the reputation of the healthcare system for building trust and certainty.

One constraint on this study was the minimal scope, involving only information security managers in the Midwestern U.S. healthcare organizations and data breaches in EHRs. The findings are nonetheless critical and supported by organizational documents, scholarly literature, and ongoing work on EHR security strategies consistent with the DIT

framework of this study. According to the DIT framework, EHRs are a troublesome invention because of their security problems, which must be fixed. The findings of this study are pertinent to information security managers in the Midwest and to other healthcare organizations that need successful security strategies to collaborate and increase confidence in the sharing of the sensitive data in their EHRs.

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), 1–18. https://doi.org/10.1186/s40537-017-0110-7

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons*, 62(4), 539–548. https://doi.org/10.1016/j.bushor.2019.03.010

Abu, S., Rahayu, S. S., Ariffin, A., & Robiah, Y. (2018). Cyber threat intelligence: Issue and challenges. *Indonesian Journal of Electrical Engineering and Computer Sciences*, *10*, 371–379. https://doi.org/10.11591/ijeecs.v10.i1.pp371-379

Aceto, G., Persico, V., & Pescapé, A. (2020). Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0. *Journal of Industrial Information Integration*, *18*, 100–129.

Agana, M. A., & Wario, R. (2018). A multi-level evidence-based cybercrime prosecution information system. *International Journal of Engineering & Technology*, *7*, 39–48. https://www.researchgate.net/profile/Ruth_Wario/publication/326905155_A_Multilevel_Evidencebased_Cyber_Crime_Prosecution_Information_System/links/5b6

b5781a6fdcc87df6dcce3/A-Multi-levelEvidence-based-Cyber-Crime-Prosecution-Information- System.pdf

Ahmed, Y., Naqvi, S., & Josephs, M. (2019). Cybersecurity metrics for enhanced protection of healthcare IT systems. *2019 13th International Symposium on Medical Informationand Communication Technology (ISMICT). 2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)*, (pp. 1–9). https://doi.org/10.1109/ismict.2019.8744003

Alarcon, G. M., Lyons, J. B., Christensen, J. C., Bowers, M. A., Klosterman, S. L., & Capiola, A. (2018). The role of propensity to trust and the five factor model across the trust process. *Journal of Research in Personality*.

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

Alder, S. (2019). 82% of Healthcare organizations have experienced a cyberattack on their IoT devices. *HIPAA Journal*.

Aldiabat, K. M., & Le Navenec, C. L. (2018). Data saturation: The mysterious step in grounded theory methodology. *Qualitative Report*, *23*(1), 245–261. https://nsuworks.nova.edu/tqr/vol23/iss1/18

Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). Ehealth cloud security challenges: A survey. *Journal of Healthcare Engineering*, 2019. https://doi.org/10.1155/2019/7516035

Alohali, M., Clarke, N., Li, F., & Furnell, S. (2018). Identifying and predicting the factors

affecting end-users' risk-taking behavior. *Information & Computer Security*. https://doi.org/10.1108/ICS-03-2018-0037

Ambre, A., & Shekokar, N. (2015). Insider threat detection using log analysis and event correlation. *Procedia Computer Science*, *45*, 436–445. doi:10.1016/j.procs.2015.03.175

Anakath, A. S., Rajakumar, S., & Ambika, S. (2019). Privacy preserving multi factor authentication using trust management. *Cluster Computing*, *22*(5), 10817-10823. https://doi.org/10.1007/s10586-017-1181-0

Anderson, D., Burleson, W., Vogel, J., O'Leary, C., Eshaya-Chauvin, B., & Flahualt, A. (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Med Inform Decis Mak*, *20*, (art.146.) https://doi.org/10.1186/s12911-020-01161-7

Anderson, R. E., Jr. (2018). Low-cost strategies to strengthen cybersecurity: Low-cost strategies can help healthcare organizations avoid the high price of a data breach. *Healthcare Financial Management, 72*. https://www.hfma.org/topics/hfm/2018/march/59656.html

Ang, C. K., Embi, M. A., & Yunus, M. M. (2016). Enhancing the quality of the findings of a longitudinal case study: Reviewing trustworthiness via ATLAS. *The Qualitative Report*, *21(*10), 1855-1867. Retrieved from https://nsuworks.nova.edu

Angraini, Alias, R. A., & Okfalisa. (2019). Information security policy compliance: Systematic literature review. *Procedia Computer Science*, *161*, 1216–1224. https://doi.org/10.1016/j.procs.2019.11.235

Anthem BCBS. (2015, February 4). *Anthem Blue Cross Blue Shield*. (Anthem, Producer) Retrieved February 18, 2016, from Anthem Blue Cross Blue Shield: https://www.anthem.com/health-insurance/about-us/pressreleasedetails/WI/2015/1813/statement-regarding-cyber-attack-against-anthem

Applied Risk (2019). *The state of industrial cyber security 2019.* Amsterdam, The Netherlands: Applied Risk BV. Retrieved from https://appliedrisk.com/assets/uploads/whitepapers/The_State_of_Industrial_Cyber_Security_2019_Applied_Risk.pdf

Arain, M., Tarraf, R., & Ahmad, A. (2019). Assessing staff awareness and effectiveness of educational training on IT security and privacy in a large healthcare organization. *Journal of Multidisciplinary Healthcare*, *12*, 73-81. doi:10.2147/JMDH.S183275

Arapi, K. (May 2018). *The healthcare industry: Evolving cyber threats and risks* (Master's Thesis). Retrieved from ProQuest Dissertations and Thesis database. (UMI No. 10814836)

Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D., Valentine-Florin, M., Calcavecchia, F., Artal, R., & Rubenfeld, S. (2017). Ethical issues in research. *Best Practice & Research Clinical Obstetrics & Gynaecology*, *43*, 107-114. doi:10.1016/j.bpobgyn.2016.12.006

Ashraf, A. (2018). Security awareness for healthcare professionals. Retrieved from http://resources.infosecinstitute.com/category/healthcare-information-

security/security- awareness-for-healthcare-professionals/

Atasoy, H., Greenwood, B. N., & Scott McCullough, J. (2019). The Digitization of Patient Care: A Review of the Effects of Electronic Health Records on Health Care Quality and Utilization. *Annual Review of Public Health*, *40*, 487. https://doi-/10.1146/annurev-publhealth-040218-044206

Atkinson, P., Jahromi, S., Kongsansatean, P., & Chan, L. (2018). Technology assessment:patient-centric solutions for transfer of health information. In *Infrastructure and Technology Management* (pp. 245-269). Springer, Cham.

Atluri, I. (2018). Smarter cyber risk governance for health care in a digital transformation age. *ISSA Journal, 16,* 27–31. https://mydigitalpublication.com/publication/?m=1336&i=517151&p=26

Auger, M. D. (2016). Cultural continuity as a determinant of indigenous peoples' health: A metasynthesis of qualitative research in Canada and the United States. *International Indigenous Policy Journal, 7*(4), 1-24. doi:10.18584/iipj.2016.7.4.3

Azeez, N. A., & der Vyver, C. V. (2019). Security and privacy issues in e-health cloud-based systems: A comprehensive content analysis. *Egyptian Informatics Journal, 20*, 97–108. https://doi.org/10.1016/j.eij.2018.12.001

Babrahem, A. S., & Monowar, M. M. (2018). Preserving confidentiality and privacy of the patient's EHR using the OrBAC and AES in cloud environment. *International Journal of Computers and Applications*, 1-12. doi:10.1080/1206212X.2018.1505025

Bae, J., Ford, E. W., Kharrazi, H. H. K., & Huerta, T. R. (2018). Electronic medical

record reminders and smoking cessation activities in primary care. *Addictive Behaviors, 77*,203-209. doi:10.1016/j.addbeh.2017.10.009

Balozian, P., Leidner, D., & Warkentin, M. (2019). Managers' and employees' differing responses to security approaches. *Journal of Computer Information Systems, 59*(3), 197–210. https://doi.org/10.1080/08874417.2017.1318687

Barlow, C. (2020, April). Human subjects protection and federal regulations of clinical trials. In *Seminars in Oncology Nursing* (p. 151001). WB Saunders. https://doi.org/10.1016/j.soncn.2020.151001

Barosy, W. (2019). Successful operational cybersecurity strategies for small businesses. Walden University. https://scholarworks.waldenu.edu/dissertations/6969/

Baumanna, L. A., Baker, J., & Elshaug, A. G. (2018). The impact of electronic health record systems on clinical documentation times: A systematic review. *Health Policy, 122*, 827-836. doi:10.1016/j.healthpol.2018.05.014

Braunstein, M. L. (2018). Health care in the age of interoperability: The potential and challenges. *IEEE Pulse, 9*(5), 34-36.

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

Barrett, A. K. (2018). Electronic health record (EHR) organizational change: Explaining resistance through profession, organizational experience, and EHRcommunication quality. *Health Communication, 33*, 496-506. doi:10.1080/10410236.2016.1278506

Bates, D. W., & Samal, L. (2018). Interoperability: what is it, how can we make it work forclinicians, and how should we measure it in the future?. *Health services research*.

Baur, X., Budnik, L. T., Ruff, K., Egilman, D. S., Lemen, R. A., & Soskolne, C. L. (2015). Ethics, morality, and conflicting interests: how questionable professional integrity in some scientists supports global corporate influence in public health. *International Journal of Occupational and Environmental Health*, *21*(2), 172-175. doi:10.1179/2049396714y.0000000103

Bennington, C. (2020). HHS OCR announces results of most recent round of HIPAA audits. Retrieved from https://www.jdsupra.com/legalnews/hhs-ocr-announces-results-of-most- 50654.

Berkeyheiser, L. (2019). HIPAA challenges: Balancing policy and technology. *For the Record (Great Valley Publishing Company, Inc)*, *31*(9), 6-7. http://reddog.rmu.edu.2060/login.aspx?direct=true&db=ccm&AN=139123981&site=eho st-live&scope=site

Bhatia-Lin, A., Boon-Dooley, A., Roberts, M. K., Pronai, C., Fisher, D., Parker, L., Engstrom, L., Ingraham, D., & Darnell, D. (2019). Ethical and regulatory considerations for using social media platforms to locate and track research participants. *The American Journal of Bioethics*, *19*(6), 47-61. https://doi.org/10.1080/15265161.2019.1602176

Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S.,Levy, M., Kedia, S., Dasgupta, D. and Dobalian, A. (2020). Transforming

healthcare cybersecurity from reactive to proactive: Current status and future recommendations.*Journal of Medical Systems,* (44(5). doi: 10.1007/s10916-019-1507-y

Bigler, M. (2004). Single sign-on. *The Internal Auditor, 61*(6), 31-34.

Blijleven, V., Koelemeijer, K., & Jaspers, M. (2019). SEWA: A framework for sociotechnicalanalysis of electronic health record system workarounds. *International Journal of Medical Informatics, 125,* 71-78.

Billingsley, L. (2019). Cybersmart: Protect the patient, protect the data. *Journal of RadiologyNursing.* Vol. 38. pp 261-263. https://doi.org/10.1016/j.jradnu.2019.09.010

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

Black Book Research. (2019, November 4). *Healthcare data breaches costs industry $4 billion by year's end, 2020 will be worse reports new black book survey.* Company Newsroom of Black Book Market Research.https://blackbookmarketresearch.newswire.com/news/healthcare-databreaches-costs-industry-4-billion-by-years-end-2020-21027640

Blue, J. & Furey, E. (2018). A novel approach for protecting legacy authentication databases in consideration of GDPR. *International Symposium on Networks, Computers and Communications,* Rome, Italy: IEEE.

Branch, L. E., Eller, W. S., Bias, T. K., McCawley, M. A., Myers, D. J., Gerber, B. J., &

Bassler, J. R. (2019). Trends in malware attacks against United States healthcare organizations, 2016-2017. *Global Biosecurity, 1*(1), 15–27. https://doi.org/http://doi.org/10.31646/gbio.7

Brauer, M., & Wiersema, M. (2018). Analyzing analyst research: A review of past coverage and recommendations for future research. *Journal of Management, 44*(1), 218-248. https://doi.org/10.1177/0149206317734900

Brewer, J., Hejjaji, V., Ip, L., Ta, B., & Wu, Z. (2019). An insight into the current securityposture of healthcare IT: A national security concern. *Institute for Critical Infrastructure Technology*. Retrieved from https://icitech.org/an-insight-into-the- current-security-posture-of-healthcare-it-a-national-security/concern/.

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

Brown, A., Awasthi, D., Dhaval, R., Rowe, J., Zonooz, P., & Ma, S. (2019). HIPAA compliancein the AWS cloud. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-hippa-compliance-in-the-aws-cloud.pdf.

Bui, Q. N., Hansen, S., Liu, M., & Tu, Q. (2018). The productivity paradox in health information technology. *Communications of the ACM, 61*(10), 78-85.

Bunch, J., Clay-Warner, J., & Lei, M. (2015). Demographic characteristics and victimization risk: Testing the mediating effects of routine activities. *Crime & Delinquency, 61*(9), 1181-1205. doi:10.1177/0011128712466932

Bunch, J., Clay-Warner, J., & Mcmahon Howard, J. (2014). The effects of victimization

on routine activities. *Criminal Justice and Behavior*, *41*(5), 574-592. doi:10.1177/0093854813508286

Bureau of Labor Statistics. (2019, August 12). *Bureau of Labor Statistics.* Retrieved January 1, 2019, from United States Department of Labor: https://www.bls.gov/oes/current/oes113021.htm

Buriro, A., Crispo, B., & Conti, M. (2019). AnswerAuth: A bimodal behavioral biometric-based user authentication scheme for smartphones. *Journal of Information Security and Applications*, *44*, 89-103. doi:10.1016/j.jisa.2018.11.008

Cea Soriano, L., Zong, J., & García Rodríguez, L. A. (2019). Feasibility and validity of The Health Improvement Network database of primary care electronic health records to identify and characterize patients with small cell lung cancer in The United Kingdom. *BMC Cancer*, *19*(1), 1–9. https://doi.org/10.1186/s12885-019-5305-1

Califf, R. M. & Sugarman, J. (2015). Exploring the ethical and regulatory issues in pragmatic clinical trials. *Clinical Trials, 12*(5), 436-441. doi:10.1177/1740774515598334

Campbell, J. (2019). Enhancing healthcare cybersecurity through legacy system retirement and data archiving. Retrieved from https://www.healthcareittoday.com/2019/09/26/enhancing-healthcare-cybersecurity- through-legacy-system-retirement-and-data-archiving/.

Capece, G., & Lorenzi, F. (2020). Blockchain and healthcare: Opportunities and prospects forEHR. *Sustainability*, *12*(22), 9693.

https://doi.org/10.3390/su12229693.

Cardlogix. (2018). Why hackers seek electronic protected health information (ephi), more so than credit cards. Retrieved from https://www.cardlogix.com/education/why-hackers- target-electronic-protected-health-information/.

Carter, D. D., Robinson, K., Forbes, J., Walsh, J. C., & Hayes, S. (2019). Exploring the perspectives of stroke survivors and healthcare professionals on the use of mobile health to promote physical activity: A qualitative study protocol. *HRB Open Research*, *2*. https://doi.org/10.12688/hrbopenres.12910.1

Cascardo (2015). Physician challenges in 2015. *Journal of Medical Practice Management: 30*(6), 395-398. Retrieved from https://www.greenbranch.com/store/index.cfm/product/4_31/the-journal-of-medical-practice-management.cfm

Castleberry, A. (2014). NVivo 10 [software program]. Version 10. QSR International; 2012. *American Journal of Pharmaceutical Education*, *78*(1), 25. doi:10.5688/ajpe78125

Cavalancia, N. (July 2, 2020). Vulnerability management explained. Retrieved from https://cybersecurity.att.com/blogs/security-essentials/vulnerability-management-explained

Cegielski, C. G., Bourrie, D. M., & Hazen, B. T. (2013). Evaluating adopting of emerging IT for corporate IT strategy: Developing a model using qualitative method. *Information Systems Management*, *30,* 235-249. doi:10.1080/10580530.2013.794632

Centers for Disease Control and Prevention. (2020). Public health and promoting interoperabilityprograms. Retrieved from https://www.cdc.gov/ehrmeaningfuluse/introduction.html

Center for Internet Security. (2018). Cyber attacks: in the healthcare sector. Retrieved from https://www.cisecurity.org/cyber-attacks-in-the-healthcare-sector/

Charles, D., Gabriel, M., & Searcy T. (2015). *Adoption of electronic health record systems among U.S. non-federal acute care hospitals: 2008-2014 ONC Data Brief, No. 23.* Washington, DC: Office of the National Coordinator for Health Information Technology, Government Printing Office.

Chen, H., Butler, E., Guo, Y., George Jr, T., Modave, F., Gurka, M., & Bian, J. (2018). Facilitation or hindrance: physicians' perception on best practice alerts (BPA) usage in anelectronic health record System. *Health Communication*, 1-7.

Chen, Q. (2019). Toward realizing self-protecting healthcare information systems: Design andsecurity challenges. *Advances in Computer*, (Vol. 114, 2019, pp. 113-149). doi:10.1016/bs.adcom.2019.02.003

Chernyshev, M., Zeadally, S., & Baig, Z. (2019). Healthcare data breaches: Implications for digital forensic readiness. *Journal of Medical Systems, 43*(1). https://doi.org/10.1007/s10916-018-1123-2

Choi, K., Cronin, S., & Correia, H. (2016). The assessment of capable guardianship measures against bullying victimization in the school environment. *Police Practice and Research*, 17(2), 149-159. doi:10.1080/15614263.2015.1128161

Choi, K., Kyungseok C., & Yong S., (2016). Demographic variables and risk factors in

computer-crime: An empirical assessment. *Cluster Computing*, *19*(1), 369-377. https://doi.org/10.1007/s10586-015-0519-8

Chua, H., Wong, S., Low, Y., & Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. *Telematics and Informatics*, *35*(6), 1770-1780. doi:10.1016/j.tele.2018.05.005

Chuang, Y., Lo, N., Yang, C., & Tang, S. (2018). A lightweight continuous authenticationprotocol for the internet of things. *Sensors*, *18*, 1104. doi:10.3390/s18041104.

Cisco Systems. (May 2018). SD-Access Segmentation Design Guide. Retrieved from https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Software-Defined-Access-Segmentation-Design-Guide-2018MAY.pdf

Coker, Z., Widder, D. G., Le Goues, C., Bogart, C., & Sunshine, J. (2019). A qualitative study on framework debugging. In *2019 IEEE International Conference on Software Maintenance and Evolution (ICSME)* (pp. 568-579). IEEE. https://doi.org/10.1016/j.ienj.2019.01.005

Cocks, C. (2001). An Identity Based Encryption Scheme Based on Quadratic Residues. *In Proceedings of the 8th IMA International Conference on Cryptography and Coding*, (pp. p. 360-363).

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588-608. doi:10.2307/2094589

Cohen, G., & Mello, M. M. (2018). HIPAA and protecting health information in the 21st century. *JAMA, 320*(3), 231-232. doi:10.1001/jama.2018.5630

Colicchio, T.K., Cimino, J.J., & Del Fiol, G. (2019). Unintended consequences of nationwide electronic health record adoption: Challenges and opportunities in the post-meaningful use era. *Journal of Medical Internet Research, 21*(*6*). doi:10.2196/13313

Collier, R. (2018). EHR access and training still lacking for medical trainees. *Canadian Medical Association Journal, 190*(35), E1054. http://dx.doi.org.contentproxy.phoenix.edu /10.1503/cmaj.109-5650

Colnago, J., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Cranor, L., & Christin, N. (2018).“It’s not actually that horrible”: Exploring adoption of two-factor authentication at a university. *Proceedings of the 2018 CHI Conference on Human Factors in ComputingSystems,* ACM, 1-11. doi: 10.1145/3173574.3174030

Colosi, H. A., Costache, C., & Colosi, I. A. (2019). Informational privacy, confidentiality and data security in research involving human subjects. *Applied Medical Informatics, 41,* 16. Retrieved from https://ami.info.umfcluj.ro

Colquhoun, D. A., Shanks, A. M., Kapeles, S. R., Shah, N., Saager, L., Vaughn, M. T., Buehler,K., Burns, M. L., Tremper, K. K., Freundlich, R. E., Aziz, M., Kheterpal, S., & Mathis, M. R. (2020). Considerations for Integration of Perioperative Electronic Health Records AcrossInstitutions for Research and Quality Improvement: The Approach Taken by the MulticenterPerioperative Outcomes

Group. *Anesthesia and analgesia*, *130*(5), 1133–1146. https://doi.org/10.1213/ANE.0000000000004489.

Connelly, L. (2016). Understanding research. Trustworthiness in qualitative research. *MedSurg Nursing*, *25*(6), 435-436. Retrieved from http://www.medsurgnursing.net

Cope, D. G. (2014). Methods and meanings: Credibility and trustworthiness of qualitative research. *Oncology Nursing Forum*, *41*(1), 89-91. doi:10.1188/14.ONF.89-91+A178:A179A178:A180

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats, and ways forward. *Maturitas*, *113*, 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008

Creswell, J.W., & Guetterman, T.C. (2019). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (6th ed.). Saddle River, NJ: Pearson.

Cresswell, K., Williams, R., & Sheikh, A. (2021). Using cloud technology in health care during the covid-19 pandemic, *3*(1), 5. https://doi.org/10.1016/S2589-7500(20)302910

Cronin, C. (2020). What lawyers mean by ‘reasonable’ cyber security controls. *CyberSecurity: A Peer-Reviewed Journal*, *3*, 315–329. https://www.ingentaconnect.com/content/hsp/jcs/2020/00000003/00000004/art00004

Crowley, K., Mishra, A., Cruz-Cano, R., Gold, R., Kleinman, D., & Agarwal, R. (2019).

Electronic health record implementation findings at a large, suburban health and human services department. *Journal of Public Health Management & Practice, 25*, 11-16. doi:10.1097/PHH.0000000000000768

Curtis, J. R., Sathitratanacheewin, S., Starks, H., Lee, R. Y., Kross, E. K., Downey, L., … Lindvall, C. (2018). Using electronic health records for quality measurement and accountability in care of the seriously ill: Opportunities and challenges. *Journal of Palliative Medicine, 21*(S2), S-52. doi:10.1089/jpm.2017.0542

Dalal, A. K., Fuller, T., Garabedian, P., Ergai, A., Balint, C., Bates, D. W., & Benneyan, J.(2019). Systems engineering and human factors support of a system of novel EHR-integrated tools to prevent harm in the hospital. *Journal of the American Medical Informatics Association*, *26*(6), 553-560.

Dameff, C., Pfeffer, M. A., & Longhurst, C. A. (2019). Cybersecurity implications for hospital quality. *Health Services Research, 54*(5), 969–970. https://doi.org/10.1111/1475-6773.13202

Danielson, L. (2021). HIPAA cybersecurity incentivized in new safe harbor law. *Corsica Technologies*. https://www.corsicatech.com/blog/hipaa-cybersecurity-incentivized-in-new-safe-harbor-law/

David, L. C., & Dhillon, G. (2019). Cloud privacy objectives a value based approach. *Information and Computer Security, 27*(2), 189-220. doi:10.1108/ICS-05-2017-0034

Davis, J. (2021). HIPAA safe harbor bill becomes law; Requires HHS to incentivize security. *Health IT Security*. https://healthitsecurity.com/news/hipaa-safe-harbor-

bill- becomes-law-requires-hhs-to-incentivize-best-practice-security

Deighton-Smith, N., & Bell, B. T. (2018). Objectifying fitness: A content and thematic analysis of# fitspiration images on social media. *Psychology of Popular Media Culture*, *7*(4), 467. https://doi.org/10.1037/ppm0000143

DeJonckheere, M., & Vaughn, L. M. (2019). Semistructured interviewing in primary care research: a balance of relationship and rigour. *Family Medicine and Community Health*, *7*(2), e000057. https://doi.org/10.1136/fmch2018-000057

Dekking, S. A., Van der Graaf, R., & Van Delden, J. J. (2014). Strengths and weaknesses of guideline approaches to safeguard voluntary informed consent of patients within a dependent relationship. *BMC Medicine*, *12*(1),12-52. doi:10.1186/1741-7015-12-52

de Vaulx, F., Simmon, E., & Bohn, R. (2018). *Cloud computing service metrics descriptions.* (NIST Special Publication 500-307). National Institute of Standards and Technology. Gaithersburg, MD: U.S. Government Printing Office.

De Vries, B. (2018). Resonating with reflexive design: On participatory design, narrative research and crystallization. *EDeR. Educational Design Research*, *2*(1). https://doi.org/10.15460/eder.2.1.1184

De Waal, M. M., Christ, C., Dekker, J. J., Kikkert, M. J., Lommerse, N. M., van den Brink, W., & Goudriaan, A. E. (2018). Factors associated with victimization in dual diagnosis patients. *Journal of Substance Abuse Treatment*, *84*, 68-77. https://doi.org/10.1016/j.jsat.2017.11.001

DHHS. (2014, March 28). *Department of Health and Human Services.* Retrieved January

1, 2019, from Department of Health and Human Services Website: http://www.hhs.gov/about/news/2014/03/28/hhs-releases-security-risk-assessment-tool- to-help-providers-with-hipaa-compliance.html

DHHS. (2010, July 12). *Department of Human and Health Services*. Retrieved January 1, 2019, from HHS.Gov: http://www.hhs.gov/sites/default/files/small-practice-security-guide- 1.pdf

DHHS-Office of Secretary. (2009, October 30). HIPAA Adminstrative Simplication: Enforcement. *45 CFR Part 160 Section 13410(d) , 74* , 56124. Washington, DC, US: Federal Register.

Das, S., Dingman, A., & Camp, L. J. (2018). Why Johnny doesn't use two factor a two-phaseusability study of the FIDO U2F security key. *Proceedings of the International Conference on Financial Cryptography and Data Security*. doi: 10.1007/978-3-662- 58387-6

Doerner, W. G. & Lab, S. P. (2015). *Victimology* (7th ed.). Philadelphia, PA: Taylor & Francis.

Du, M., & Wang, K. (2020). An SDN-enabled pseudo-honeypot strategy for distributed denial of service attacks in industrial Internet of things. *IEEE Transactions on Industrial Informatics, 16*(1), 648-657. doi:10.1109/tii.2019.2917912

Ebnehoseini, Z., Tara, M., Tabesh, H., Dindar, F., & Hasibian, S. (2020). Understanding key factors affecting on hospital electronic health record (EHR) adoption. *Journal of Family Medicine & Primary Care, 9*(8), 4348–4352. https://doi.org/10.4103/jfmpc.jfmpc_109_20

Ehrenfeld, J. M., & Wanderer, J. P. (2018). Technology as friend or foe? Do electronic health records increase burnout? *Current Opinion in Anesthesiology*, 31(3), 357-360. doi:10.1097/ACO.0000000000000588

Elhoseny, M., Abdelaziz, A., Salama, A. S., Riad, A. M., Muhammad, K., & Sangaiah, A. K. (2018). A hybrid model of internet of things and cloud computing to manage big data inhealth services applications. *Future Generation Computer Systems, 86*, 1383-1394. https://doi.org/10.1016/j.future.2018.03.005

Elmaghraby, A. S. & Losavio, M. M. (2014). Cyber security challenges in smart cities: Safety, security and privacy. *Journal of Advanced Research*, 5(4), 491-497. doi:10.1016/j.jare.2014.02.006

Elmore, B. (2020, October 14). *All about the hipaa omnibus rule*. Accountable. https://www.accountablehq.com/post/the-hipaa-omnibus-rule

Everson, J., Rubin, J. C., & Friedman, C. P. (2020). Reconsidering hospital ehr adoption at the dawn of hitech: implications of the reported 9% adoption of a "basic" ehr. *Journal of the American Medical Informatics Association: JAMIA,27*(8), 1198–1205. https://doi.org/10.1093/jamia/ocaa090

Excellus BCBS. (2015, September 9). *Excellus Blue Cross Blue Shield*. Retrieved February 26, 2016 , from Excellus Blue Cross Blue Shield Website: http://www.excellusfacts.com

Eyre, L., George, B., & Marshall, M. (2015). Protocol for a process-oriented qualitative evaluation of the Waltham Forest and East London Collaborative (WELC) integrated care pioneer programme using the Researcher-in-Residence model.

BMJ Open, 5(11), 1-10. doi:10.1136/bmjopen-2015-009567

FBI. (2009, April 1). *Federal Bureau of Investigation*. (FBI, Producer) Retrieved March 1, 2016, from Federal Bureau of Investigation: https://www.fbi.gov/news/stories/2009/april/spearphishing_040109

Finset, A. (2018). Among the topics of this issue: Health literacy and interpreter-mediated communication. *Patient Education and Counseling, 101*(1), 1. https://doi.org/10.1016/j.pec.2017.11.005

Forero, R., Nahidi, S., De Costa, J., Mohsin, M., Fitzgerald, G., Gibson, N., & Aboagye-Sarfo, P.(2018). Application of four-dimension criteria to assess rigour of qualitative research in emergency medicine. *BMC Health Services Research, 18*(1), 120. https://doi.org/10.1186/s12913-018-2915-2

Foster, S. (2020). Digital can make a difference. *British Journal of Nursing, 29,*75. https://doi.org/10.12968/bjon.2020.29.1.75

Flick, U. (2018). *An introduction to qualitative research*: Sage Publications Limited.

Fragidis, L. L., & Chatzoglou, P. D. (2018). Implementation of a nationwide electronic health record (EHR): The international experience in 13 countries. *International Journal of Health Care Quality Assurance, 31,* 116-130. doi:10.1108/IJHCQA-09-2016-0136

Fritz, R. L., & Vandermause, R. (2018). Data collection via in-depth email interviewing: Lessons from the field. *Qualitative health research, 28*(10), 1640-1649. https://doi.org/10.1177/1049732316689067

Fusch, P. I., Fusch, G. E., & Ness, L. R. (2017). How to conduct a mini-ethnographic

case study: A guide for novice researchers. *Qualitative Report, 22*(3), 923-941. Retrieved from http://nsuworks.nova.edu/tqr/vol22/iss3/16

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

Gagnon, M. L., & Stephen, G. (2018). A pragmatic solution to a major interoperability problem: using blockchain for the nationwide patient index. *Blockchain in Healthcare Today*.

Ganiga, R., Pai, R. M., Pai, M., & Sinha, R. K. (2020). Security framework for cloud based electronic health record (EHR) system. *International Journal of Electrical and ComputerEngineering*, 10(1), 455-466.

Gao, F., & Sunyaev, A. (2019). Context matters: A review of the determinant factors in the decision to adopt cloud computing in healthcare. *International Journal of InformationManagement, 48*, 120-138. https://doi.org/10.1016/j.ijinfomgt.2019.02.002

Gellert, G. A., Crouch, J. F., Gibson, L. A., Conklin, G. S., Webster, S. L., & Gillean, J. A. (2017). Clinical impact and value of workstation single sign-on. *International Journal of Medical Informatics, 101*(Supplement C), 131–136. doi.org/10.1016/j.ijmedinf.2017.02.008

Genç, Z., Masalimova, A. R., Platonova, R. I., Sizova, Z., & Popova, O. V. (2019).Analysis of documents published in scopus database on special education learning through mobile learning: A content analysis. *International Journal of*

Emerging Technologies in Learning (iJET), *14*(22), 192-203. https://doi.org/10.3991/ijet.v14i22.11732

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., & Baker, T. (2018). Security threats to critical infrastructure: the human factor. *The Journal of Supercomputing*, *74*(10), 4986-5002. Springer Link. https://link.springer.com/article/10.1007/s11227-018-2337-2

Gibson, G. (2020). *A comprehensive strategy for cybersecurity implementation within the department of defense: A Delphi study*. https://www.proquest.com/openview/cdc6908b80ed4e795f6c6e92551012bb/1?pq-origsite=gscholar&cbl=18750&diss=y

Gogan, M. (2018). *10 Best practices to secure and protect passwords*. Retrieved from https://techspective.net/2018/05/23/10-best-practices-to-secure-and-protectpasswords/

Gomez, A. (2018). Self As Instrument. Retrieved from selfasinstrument.me/sai/

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *Journal of Cybersecurity*, *6*(1), tyaa005, Oxford Academy. https://doi.org/10.1093/cybsec/tyaa005

Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of the 13th ACM conference on Computer and communications security (CCS '06)* (p. p. 89).

Graboyes, R. F., & Bryan, D. (2018). From electronic health records to digital

biographies. Retrieved from https://www.mercatus.org/publications/electronic-health-records-ehr-digital-health-biographies

Green, R., Brandt, R., & Miller, A. (2018, September). A Framework for Integrating Safety inUsability Engineering for Electronic Health Records. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 62, No. 1, pp. 499-502). Sage CA: Los Angeles, CA: SAGE Publications.

Green, C., Duan, N., Gibbons, R., Hoagwood, K., Palinkas, L., & Wisdom, J. (2014). Approaches to mixed methods dissemination and implementation research: Methods, strengths, caveats, and opportunities. *Administration and Policy in Mental Health and Mental Health Services Research*, 1-16. doi:10.1007/s10488-014-0552-6

Greevy, H. (2018). The fine print on two-factor authentication. *Medical Economics*, 95(18), 17-18. Retrieved from https://search.proquest.com/docview/2120615693?accountid=28902

Gue, D. (2019). *The health IT staffing shortage is a problem morphing into crisis*. Health IT consultants. https://hitconsultant.net/2019/10/16/health-it-staffing-shortage-crisis/

Guhr, N., Lebek, B., & Breitner, M. H. (2019). The impact of leadership on employees' intended information security behavior: An examination of the full-range leadership theory. *Information Systems Journal*, *29*(2), 340–362.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2018). Understanding non-malicious security violations in the workplace: A composite behavior model.

Journal of Management Information Systems, 28(2), 203–236.

Haqaf, H., & Koyuncu, M. (2018). Understanding key skills for information security managers. *International Journal of Information Management, 43*, 165–172.

Haimes, Y. Y., Horowitz, B. M., Guo, Z., Andrijcic, E., & Bogdanor, J. (2015). Assessing systemic risk to cloud computing technology as complex interconnected systems of systems. *Systems Engineering*, *18*, 284–299. doi:10.1002/sys.21303

Happa, J., Glencross, M., & Steed, A. (2019). Cyber security threats and challenges in collaborative mixed-reality. *Frontiers in ICT*. https://doi.org/10.3389/fict.2019.00005

Hausfeld, J., & Zimmerman, R. (2018). Your organization can and should be cyber secure. *The Journal of Medical Practice Management, 33*(6), 389–391. https://www.proquest.com/openview/ffe7397237d815ea98d0126e3029afd7/1?pq-origsite=gscholar&cbl=32264

Harmon, E. (2018). *Strategies used by cloud security managers to implement secure accessmethods* (Doctoral Dissertation). Retrieved from ProQuest Central; ProQuest Dissertations & Theses Global (UMI No.10743323).

Harrington, L. (2019). Quality of electronic health record data on which we stand. *AACN Advanced Critical Care*, *30*(2), 105–109. https://doi.org/10.4037/aacnacc2019556

Hatef, E., Weiner, J. P., & Kharrazi, H. (2019). A public health perspective on using electronic health records to address social determinants of health: The potentialfor a national system of local community health records in the United States.

International Journal of Medical Informatics, *124*, 86–89. https://doi.org/10.1016/j.ijmedinf.2019.01.012

He, H., & Yan, Y. (2014). Design of hospital EMR management system. *International Journal of U-and E-Service, Science and Technology*, *7*, 341-348. doi:10.14257/ijunnesst.2014.7.5.30

HealthIT. (2020, June 26). *HealthIT.gov*. Retrieved May 4, 2020, from HealthIT.gov: https://www.healthit.gov/providers-professionals/security-risk-assessment-tool

Hedda, M., Malin, B. A., Yan, C., & Fabbri, D. (2018). Evaluating the effectiveness of auditing rules for electronic health record systems. *AMIA . Annual Symposium proceedings. AMIA Symposium*, *2017*, 866–875.

Hemsley, B., Rollo, M., Georgiou, A., Balandin, S., & Hill, S. (2018). The health literacy demands of electronic personal health records (e-PHRs): An integrative review to inform future inclusive research. *Patient Education and Counseling*, *101*(1), 2-15. https://doi.org/10.1016/j.pec.2017.07.010

Herwono, I., & El-Moussa, F. A. (2018). Automated detection of the early stages of cyber killchain. *In Proceedings of the 4th International Conference on Information Security Systems and Privacy*(pp. 182-189). doi: 10.5220/0006543301820189

Henriques de Gusmão, A. P., Silva, M. M., Poleto, T., Camara e Silva, L., & Cabral Seixas Costa, A. P. (2018). Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. *International Journal of Information Management*, *43*, 248–260. https://doi.org/10.1016/j.ijinfomgt.2018.08.008

Hertzog, R., Johnson, J., Smith, J., McStay, F. W., da Graca, B., Haneke, T., ...

Couchman, G. R. (2019). Diagnostic accuracy in primary care e-visits: Evaluation of a large integrated health care delivery system's experience. *Mayo Clinic Proceedings*, *94*(6),976-984. doi:10.1016/j.mayocp.2019.02.011

Heyde, S. M. (2018). Primary care practices' progress of using electronic health information exchange (hie). *Primary Care*.

Hidayat, T., & Mahardiko, R. (2020). A Systematic literature review method on aes algorithmfor data sharing encryption on cloud computing. *International Journal of Artificial Intelligence Research*, *4*(1), 49-57.

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization: An empirical foundation for a theory of personal victimization*. Cambridge, MA: Ballinger.

HIMSS (2019). *2019 HIMSS cybersecurity survey*. Chicago, IL: Healthcare Information and Management Systems Society Inc. Headquarter. Retrieved from https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_ Final_Report.pdf

Holotiuk, F., & Moormann, J. (2018). Organizational adoption of digital innovation: The case of blockchain technology. In *Proceedings of the European conference on information systems*.

Holt, T. J. & Bossler, A. M. (2013b). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice*, *29*(4), 420-436. doi:10.1177/1043986213507401

Hong, L., Luo, M., Wang, R., Lu, P., Lu, W., & Lu, L. (2018). Big data in health care:

Applications and challenges. *Data and Information Management, 2*(3), 175-197. https://doi.org/10.2478/dim-2018-0014

Hope, P., & Zhang, X. (2015). Examining user satisfaction with single sign-on and computer application roaming within emergency departments. *Health Informatics Journal, 21*(2), 107–119. https://doi.org/10.1177/1460458213505572

Houghton, C., Murphy, K., Shaw, D., & Casey, D. (2015). Qualitative case study data analysis: An example from practice. *Nurse Researcher, 22*(5), 8. doi:10.7748/nr.22.5.8.e1307

Howe, J. L., Adams, K. T., Hettinger, A. Z., & Ratwani, R. M. (2018). Electronic health record usability issues and potential contribution to patient harm. *JAMA, 319*(12), 1276–1278. DOI:10.1001/jama.2018.1171

Howe, R. C., Sharma, S., & Murray, M. (2019). Practice intervention activities to improve population health: A case study using electronic health records (EHR) for chronic disease management. *Texas Public Health Journal, 71*(1), 24–30. Retrieved from https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=a9h&AN=133970076&site=eds-live&scope=site

HRSA. (2014, March 14). *Health Resources and Services Administration*. Retrieved January 1, 2019, from HRSA website: http://www.hrsa.gov/healthit/toolbox/RuralHealthITtoolbox/Collaboration/whatishie.html

Hsieh, M., & Wang, S. K. (2018). Routine activities in a virtual space: A Taiwanese case

of anATM hacking spree. https://doi.org/10.5281/zenodo.1467935

Hu, X., Qu, H., Houser, S. H., Chen, H., Zhou, J., & Yu, M. (2020). Hospital characteristics associated with certified ehr adoption among US psychiatric hospitals. *Risk Management and Healthcare Policy, UME 13*, 295–301. http://doi.org/10.2147/RMHP.S241553

Hudson, S. & Hudson, R. (2013). Engaging with consumers using social media: a case study of music festivals. *International Journal of Event and Festival Management, 4*(3), 206-223. doi:10.1108/ijefm 06 2013 0012

Huerta, T. R., Thompson, M. A., Ford, E. W., & Ford, W. F. (2013). Electronic health record implementation and hospitals' total factor productivity. *Decision Support Systems, 55*, 450-458. doi:10.1016/j.dss.2012.10.004

Hughbanks, F. A. (August 2018). *Cybersecurity within the healthcare industry and electronichealth records.* (Master's Thesis). Retrieved from ProQuest Dissertations and Thesisdatabase. (UMI No. 10930168)

Hussein, A. (2015). The use of triangulation in social sciences research: Can qualitative and quantitative methods be combined? *Journal of Comparative Social Work, 4*(1), 1-12. Retrieved from https://doaj.org/article/a76dfb64227a46d3b7878af4c5b2d52e?

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

Ilievski, A. (2016). An explanation of the data breaches victimisation: Self-control and

lifestyle/routine activity theory. *Innovative Issues and Approaches in Social Sciences, 9*(1), 30-47. doi:10.12959/issn.1855 0541.iiass 2016 no1-art02

Intenzer. (2020). Migrating to the cloud: Compliance issues when transitioning from a traditionaldata center. Retrieved from https://cloudsecurityalliance.org/blog/2020/12/16/migrating- to-the-cloud-compliance-issues-when-transitioning-from-a-traditional-data-center/.

International Organization for Standardization. (2005, October). *International Organization for Standardization ISO 27001*. (International Organization of Standardization ISO Central Secretariat) Retrieved April 16, 2016, from ISO.org: http://www.27000.org/iso- 27001.htm

Ismail, W. B. W., & Yusof, M. (2018). Mitigation strategies for unintentional insider threats on information leaks. *International Journal of Security and Its Applications, 12*(1), 37–46. https://doi.org/10.14257/ijsia.2018.12.1.03

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. *Journal of Medical Internet Research, 20*(5). https://doi.org/10.2196/10059/

James, K., Schank, C., Downing, K. K., Misasi, J., Miner, M., Mulloy, J., & Mikal, M. (2018). Pediatric palliative physician and nurse mentorship training program: A personalized didactic and experiential training curriculum developed to enhance access to care in non-metropolitan communities. Retrieved from https://pediatrics.aappublications.org/content/142/1_MeetingAbstract/656

Janchenko, G. (2020). The impact of electronic health record systems on physician

productivity. *Issues In Information Systems*, *21*(4), 1–8. https://doi.org/10.48009/4_iis_2020_1-8.

Jason, C. (2020). How EHR telehealth integration evolved patient care duringCOVID-19. *EHR Intelligence-xtellingent Healthcare Media.* www.ehrintelligence.com

Johnson, A. M., & Lederer, A. L. (2013). IS strategy and IS contribution: CEO and CIO perspectives. *Information Systems Management, 30,* 306-318. doi:10.1080/10580530.2013.832962

Johnson, J. L., Adkins, D., & Chauvin, S. (2020). A review of the quality indicators of rigor in qualitative research. *American Journal of Pharmaceutical Education*, *84*(1), 138–146. https://doi.org/10.5688/ajpe7120

Joseph, S., Sow, M., Furukawa, M. F., Posnack, S., & Chaffee, M. A. (2014). HITECH spurs EHR vendor competition and innovation, resulting in increased adoption. *American Journal of Managed Care, 20,* 734-740. doi:10.1016/j.hjdsi.2013.12.004

Joshi, A., Bollen, L., Hassink, H., De Haes, S., & Van Grembergen, W. (2018). Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategicrole. *Information and Management, 55,* 368-380. doi:10.1016/j.im.2017.09.003

Kadam, A.W. (2007). Information security policy development and implementation. *Information Systems Security. 16,* 246-256. doi.org/10.1080/10658980701744861

Kakucha, W., & Buya, I. (2018). Information System Security Mechanisms in Financial Management. *Journal of Information and Technology*, *2*(1), 1-16. Stratford.

https://stratfordjournals.org/journals/index.php/Journal-of-Information-and-Techn/article/view/115

Kalloniatis, C., Mouratidis, H., Vassilis, M., Islam, S., Gritzalis, S., & Kavakli, E. (2014). Towards the design of secure and privacy-oriented information systems in the cloud: Identifying the major concepts. *Computer Standards & Interfaces, 36,* 759–775. doi:10.1016/j.csi.2013.12.010

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2019). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*. https://doi.org/10.1016/j.jfineco.2019.05.019

Kapoor, K. K., Tamilmani, K., Rana, N. P., Patil, P., Dwivedi, Y. K., & Nerur, S. (2018). Advances in social media research: Past, present and future. *Information Systems Frontiers, 20*(3), 531-558. https://doi.org/10.1007/s10796-017-9810-y

Kaur, A., & Kaur, R. (2018). Cloud computuing: A focus on security issues in cloud computing region. *International Journal of Advanced Research in Computer Science, 9*(2), 267-269. doi:10.26483/ijarcs.v9i2.5556

Kaur, A.A, & Mustafa, K.K. (2019). A critical appraisal on password based authentication. *I.J. Computer Network and Information Security, 1,* 47-61. doi:10.5815/ijcnis.2019.01.05

Kaušpadienė, L., Ramanauskaitė, S. & Čenys, A. (2019). Information security management framework suitability estimation for small and medium enterprise. *Technological and Economic Development of Economy*.

https://doi.org10.3846/tede.2019.10298

Kayser, C. S., Ellen Mastrorilli, M., & Cadigan, R. (2019). Preventing cybercrime: A framework for understanding the role of human vulnerabilities. *Cyber Security: A Peer-Reviewed Journal*, *3*(2), 159-174. Ingenta. https://www.ingentaconnect.com/content/hsp/jcs/2019/00000003/00000002/art00007

Kern, C. (2015, September 28). *Heath IT Outcomes*. (C. Kern, Producer) Retrieved March 6, 2016, from Health IT Outcomes: http://www.healthitoutcomes.com/doc/excellus-data- breach-undetected-nearly-two-years-0001

Keshta, I., & Odeh, A. (2020, August 4). Security and privacy of electronic health records:Concerns and challenges. *Egyptian Informatics Journal*. doi:https://doi.org/10.1016/j.eij.2020.07.003

Kharrazi, H., Gonzalez, C. P., Lowe, K. B., Huerta, T. R., & Ford, E. W. (2018). Forecasting thematuration of electronic health record functions among US hospitals: Retrospective analysis and predictive model. *Journal of Medical Internet Research*, 20(8).

Kim, E., Rubinstein, S. M., Nead, K. T., Wojcieszynski, A. P., Gabriel, P. E., & Warner, J. L.(2019). The Evolving Use of Electronic Health Records (EHR) for Research. In *Seminars in Radiation Oncology* (Vol. 29, No. 4, pp. 354-361). WB Saunders.

Koch, M., & Moslein, M. (2005). Identities management for e-commerce and collaboration applications. *International Journal of Electronic Commerce*, 9(3),

11-29.

Kocher, R. P. (2021). Reducing Administrative Waste in the US Health Care System. *JAMA*, *325*(5), 427–428. https://doi-/10.1001/jama.2020.24767.

Kondylakis, H., Koumakis, L., Tsiknakis, M., & Kiefer, S. (2018). The vision of personallymanaged health data: Barriers, approaches and roadmap for the future. *Journal of Biomedical Informatics, 81*, 131–132.

Kooienga, S. (2018). Rural patients' and primary care clinic staffs' perceptions of ehr implementation: An ethnographic exploration. *The Journal of Ambulatory Care Management, 41*(1), 71-79. DOI:10.1097/JAC.0000000000000199

Kopel, J., Hier, D., & Thomas, P. (2019). Electronic health records: Is mindfulness the solution? *Baylor University Medical Center. Proceedings, 32*(3), 459–461. https://doi.org/10.1080/08998280.2019.1588839

Kornbluh, M. (2015). Combatting challenges to establishing trustworthiness in qualitative research. *Qualitative Research in Psychology*, *12*(4), 397-414. doi:10.1080/14780887.2015.1021941

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

Krisby, R. M. (2018). Health care held ransom: Modifications to data breach security & the future of health care privacy protection. *Health Matrix, 28*(1), 365-401. Retrieved fromhttps://scholarlycommons.law.case.edu

Kroning, M. (2018). 59 clicks in the EHR. *Nursing Management (Springhouse), 49*(5),

10–14. doi:10.1097/01.NUMA.0000532337.74937.a1

Kroth, P. J., Morioka-Douglas, N., Veres, S., Babbott, S., Poplau, S., Qeadan, F., … Linzer, M.(2019). Association of electronic health record design and use factors with clinician stress and burnout. *JAMA Network Open*, *2*(8), e199609-e199609. doi:10.1001/jamanetworkopen.2019.9609

Kuo, A. M.-S., Thavalathil, B., Elwyn, G., Nemeth, Z., & Dang, S. (2018). The Promise of Electronic Health Records to Promote Shared Decision Making: A Narrative Review and a Look Ahead. *MEDICAL DECISION MAKING*, *38*(8), 1040–1045. https://doi-org /10.1177/0272989X18796223.

Kuiler, E. W., & McNeely, C. L. (2018). Federal big data analytics in the health domain: Anontological approach to data interoperability. *In Federal Data Science* (pp. 161-176).Academic Press.

Kumar, R., & Goyal, R. (2019). Assurance of data security and privacy in the cloud: A three-dimensional perspective. *Software Quality Professional*, *21*(2), 7–26.

Kwon, J., & Johnson, M. E. (2013). Health-care security strategies for data protection and regulatory compliance. *Journal of Management Information Systems, 30*, 41–66. doi:10.2753/MIS0742-1222300202

Landi, H. (2015, September 10). *Healthcare Informatics*. (M. Hagland, Editor, H. Landi, Producer, & Vendome Group, LLC) Retrieved February 21, 2018, from Vendome Healthcare Media: http://www.healthcare-informatics.com/news-item/excellus-bluecross-blueshield-hacked-more-10m-affected

Landi, H. (2015, September 22). *Healthcare Informatics*. (H. Landi, Editor) Retrieved

June 1, 2018, from Vendome Healthcare Media: http://www.healthcare-informatics.com/news- item/study-hitech-act-boosted-ehr-use-misses-mark-interoperability

Lane, S. R., Miller, H., Ames, E., Garber, L., Kibbe, D. C., Schneider, J. H.… & DirectTrustClinicians' Steering Group. (2018). Consensus statement: feature and function recommendations to optimize clinician usability of direct interoperability to enhance patient care. *Applied Clinical Informatics*, *9*(01), 205-220.

Lanier, C., Dao, M. D., Hudelson, P., Cerutti, B., & Perron, N. J. (2018). Learning to use electronic health records: can we stay patient-centered? A pre-post intervention study with family medicine residents. *BMC Family Practice, 18*, 1–10. https://doi.org/10.1186/s12875-017-0640-2

Le Cong, T. (2019). Motivating follower creativity by offering intellectual stimulation. *International Journal of Organizational Analysis, 28*(4), 817-829. https://doi.org/10.1108/ijoa-06-2019-1799

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263-280. https://doi.org/10.1080/01639625.2015.1012409

Levine, D. M., Linder, J. A., & Landon, B. E. (2018). Characteristics and disparities among primary care practices in the united states. *Journal of General Internal Medicine*, *33*(4), 481-486. doi:10.1007/s11606-017-4239-z

Levitt, H. M., Bamberg, M., Creswell, J. W., Frost, D. M., Josselson, R., & Suárez-Orozco, C. (2018). Journal article reporting standards for qualitative primary,

qualitative meta-analytic, and mixed methods research in psychology: The APA Publications and Communications Board task force report. *American Psychologist, 73*(1), 26. https://psycnet.apa.org/fulltext/2018-00750-003.html

Li, Y., Rao, S., Roberto, J., Solares, R. A., Hassaine, A., Ramakrishnan, R., … & Salimi-Khorshidi., G. (2020). BEHRT: Transformer for Electronic Health Records. *Scientific Reports*, *10*(1), 1–12. https://doi:10.1038/s41598-020-62922-y

Longhurst, C. A., Davis, T., Maneker, A., Eschenroeder Jr, H. C., Dunscombe, R., Reynolds, G., ... & Adler-Milstein, J. (2019). Local Investment in Training Drives Electronic Health Record User Satisfaction. *Applied clinical informatics*, 10(02), 331-335. doi:10.1055/s-0039-168875. Retrieved from https://www.thieme-connect.com/products/ejournals/html/10.1055/s-0039-1688753

Lopez, C. A., Omizo, R. K., & Whealin, J. M. (2018). Impact of a tailored training on advanced electronic medical records use for providers in a Veterans Health Administration Medical System. *JAMIA Open, 1*, 142-146. doi:10.1093/jamiaopen/ooy031

Lord, N. (2018). What is Cyber Security? Retrieved from https://digitalguardian.com/blog/what-cyber-security

Lowe, D. (2018). *Networking all-in-one for dummies* (7th ed.). Hoboken, NJ: JohnWiley and Sons.

Lucas, S. R. (2014). Beyond the existence proof: Ontological conditions, epistemological implications, and in-depth interview research. *Quality & Quantity*, *48*(1), 387-408. doi:10.1007/s11135-012-9775-3

Madsen, P., Koga, Y. & Takahashi, K. (2005), Federated Identity Management for Protecting users from Id theft, in 'Proceedings of the 2005 workshop on Digital Identity management'. doi:10.1145/1102486.1102500

Maglaras, L., Ferrag, M. A., Derhab, A., Mukherjee, M., Janicke, H., & Rallis, S. (2019). Threats, protection and attribution of cyber attacks on criticalinfrastructures. *arXiv preprint arXiv:1901.03899*. https://arxiv.org/abs/1901.03899

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2014). Juveniles and cyber stalking in the United States: An analysis of theoretical predictors of patterns of online perpetration. *International Journal of Cyber Criminology*, *8*(1), 47-56. Retrieved from http://www.data breachesjournal.com/marcumetalijcc2014vol8issue1.pdf

Marciano, A. (2018). Reframing biometric surveillance: From a means of inspection to a form ofcontrol. *Ethics and Information Technology*, *3,* 102-110. doi:10.1007/s10676-18-9493-1/ISSN 1572-8439

Martin, J., Dubé, C., & Coovert, M. D. (2018). Signal Detection Theory (SDT) is effective for modeling user behavior toward phishing and spear-phishing attacks. *Human factors*, *60*(8), 1179-1191. https://doi.org/10.1177/0018720818789818

Mayer, A. H., da Costa, C. A., & Righi, R. da R. (2019). Electronic health records in a Blockchain: A systematic review. *Health Informatics Journal*, *26*(2), 1273–1288. https://doi.org/10.1177/1460458219866350

Mazzoli, R. (2021). Health insurance portability and accountability (HIPAA) & HITECH acts. Retrieved from https://docs.microsoft.com/en-us/compliance/regulatory/offering-hipaa- hitech

McAlearney, A. S., Hefner, J. L., Sieck, C. J., & Huerta, T. R. (2015). The journey through grief: Insights from a qualitative study of electronic health record implementation. *Health Services Research, 50*, 462-488. doi:10.1111/1475-6773.12227

McFadyen, J., & Rankin, J. (2016). The role of gatekeepers in research: Learning from reflexivity and reflection. *GSTF Journal of Nursing and Health Care (JNHC), 4*(1), 82-88. doi:10.5176/2345-718X_4.1.135

McGee, M. K. (2015, September 21). *Data Breach Today*. Retrieved February 26, 2016, from Data Breach Today Web Site: http://www.databreachtoday.com/excellus-faces-breach- related-lawsuit-a-8539

McGlade, D., & Scott-Hayward, S. (2019). ML-based cyber incident detection for electronic medical record (EMR) systems. *Smart Health*, 12, 3–23. doi: 10.1016/j.smhl.2018.05.001

McGrath, C., Palmgren, P. J., & Liljedahl, M. (2019). Twelve tips for conducting qualitative research interviews. *Medical teacher*, *41*(9), 1002-1006. https://doi.org/10.1080/0142159X.2018.1497149

McIntosh, M. J., & Morse, J. M. (2015). Situating and constructing diversity in semi-structured interviews. *Global Qualitative Nursing Research, 2*, 233339361559767. doi:10.1177/2333393615597674

McGuire, M. J. (2019). Building learning health care systems in primary care. *Quality Management in Healthcare, 28(4),* 252-253. doi: 10.1097/QMH.0000000000000230. Retrieved from

https://journals.lww.com/qmhcjournal/Citation/2019/10000/Building_Learning_Health_Care_Systems_in_Primary.9.aspx

McKillop, N., Reynald, D. M., & Rayment-McHugh, S. (2020). (Re) conceptualizing the role ofguardianship in preventing child sexual abuse in the home. *Crime Prevention and Community Safety*, *23*, 1-18. https://doi.org/10.1057/s41300-020-00105-7

McRae, A. D., Bennett, C., Brown, J. B., Weijer, C., Boruch, R., Brehaut, J., … Taljaard, M. (2013). Researchers' perceptions of ethical challenges in cluster randomized trials: a qualitative analysis. *Trials*, *14*(1), 1. doi:10.1186/1745- 6215-14-1

Mello, M. M., Adler-Milstein, J., Ding, K. L., & Savage, L. (2018). Legal barriers to the growthof health information exchange—Borders or pebbles? *The Milbank Quarterly*, *96*(1), 110-143. doi:10.1111/1468-0009.12313

Meng, W., Li, W., Wang, Y., & Au, M. H. (2018). Detecting insider attacks in medical cyber–physical networks based on behavioral profiling. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2018.06.007

Microsoft. (n.d.). Windows XP end of support. Retrieved from https://www.microsoft.com/en- us/windowsforbusiness/end-of-xp-support

Miethe, T. D. & Meier, R. F. (1990). Opportunity, choice and criminal victimization rates: A theory of a theoretical model. *Journal of Research in Crime & Delinquency*, *27*, 243-266. doi.org/10.1177/0022427890027003003

Mikeal, A. (2019). From patient to population. *2019 ACM SIGUCCS Annual Conference on –SIGUCCS '19. 2019 ACM SIGUCCS Annual Conference*, (pp.155-159). doi:

10.1145/3347709.3347779

Miranda, M. J. (2018). Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. *International Management Review, 14*(2), 5-10. http://www.imrjournal.org/uploads/1/4/2/8/14286482/imr-v14n2art1.pdf

Misra, S. C., Kumar, A., & Munnangi, A. K. (2019). Cloud-based healthcare management: identifying the privacy concerns and their moderating effect on the cloud-based healthcare services. Security and Privacy, 2(3). https://doi.org/10.1002/spy2.63

Misto, K., Padula, C., Dame, L., Molloy, P. A., & Nimmagadda, J. (2020). Interprofessional Evidence-Based Strategies to Enhance Provider and Patient Interactions During Electronic Health Record Use. *Journal for Nurses in Professional Development*, *36*(3), 134–140.

Mittal, A. (2020). Digital health: Data privacy and security with cloud computing. *Issues in Information Systems, 21*(1), 227-238. https://iacis.org/iis/2020/1_iis_2020_227-238.pdf

Mohajan, H. K. (2018). Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment, and People, 7*(1), 23-48. MPRA. https://mpra.ub.unimuenchen.de/85654/1/MPRA_paper_85654.pdf

Mohammadi, F., Panou, A., Ntantogian, C., Karapistoli, E., Panaousis, E., & Xenakis, C. (2019). CUREX: Secure and private health data exchange. *IEEE/WIC/ACM International Conference on Web Intelligence on - WI '19 Companion. IEEE/WIC/ACM International Conference on Web Intelligence* (pp.263-268). doi:

10.1145/3358695.3361753

Mohit, G. S., & Bhararth C, S. (2020). Investigation of inter vlan routing and deploying accesscontrol list for corporate network. *International Journal of Electrical Engineering and Technology*, *11*(3).

Moir, E., Hart, T. C., Reynald, D. M., & Stewart, A. (2018). Typologies of suburban guardians: Understanding the importance of responsibility, opportunities, and routine activities in facilitating surveillance. *Crime Prevention & Community Safety*. https://doi.org/ 10.1057/s41300-018-0057-4

Monson, M. C. (2019). *Securing legacy medical devices*. (Master's Thesis). Retrieved fromProQuest Dissertation and Theses database. (UMI No. 22619189)

Moon, B., Morash, M., Jeong, S., & Yoon, H. S. (2015). Gender differences in the routine activities associated with risks for larceny in south korea. *International Journal of Offender Therapy and Comparative Criminology, 60,* 1327. doi:10.1177/0306624x15578631

Moore, W., & Frye, S. (2020). Review of HIPAA, part 2: limitations, rights, violations, and rolefor the imaging technologist. *Journal of nuclear medicine technology*, *48*(1), 17-23.

Morse, J. M. (2015b). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative Health Research*, *25*(9), 1212-1222. doi:10.1177/1049732315588501

Morse, A., & McEvoy, C. (2014). Qualitative research in sport management: Case study as a methodological approach. *Qualitative Report, 19*(17), 1-13. Retrieved from

http://nsuworks.nova.edu/tqr/vol19/iss31/3/

Mues, K. E., Bogdanov, A. N., Monda, K. L., Yedigarova, L., Liede, A., & Kallenbach, L. (2018). How well can familial hypercholesterolemia be identified in an electronic healthrecord database? *Clinical Epidemiology, 10,* 1667-1677. doi:10.2147/CLEP.S176853

Mukherjee, S. (2019). Cloud-based security solutions. *IUP Journal of Computer Sciences, 13*(4), 72–78. https://dx.doi.org/10.2139/ssrn.3408882

Muller, S. R., & Lind, M. L. (2020). Factors in information assurance professionals' intentions to adhere to information security policies. *International Journal of Systems and Software Security and Protection (IJSSSP), 11*(1), 17-32. https://doi.org/10.4018/IJSSSP.2020010102

Mullings, C., & Ngwenyama, O. (2018). Factors that Drive Successful Electronic Health Record Implementation Among Aging Nurses. In *International Conference on HCI inBusiness, Government, and Organizations* (pp. 626-644). Springer, Cham.

Mun, H. J., Hong, S., & Shin, J. (2018). A novel secure and efficient hash function with extra padding against rainbow table attacks. *Cluster Computing*, *21*(1), 1161-1173. https://doi.org/10.1007/s10586-017-0984-3

Munro, D. (2015, December 31). *Forbes Pharma & Healthcare*. (D. Munro, Producer, & Forbes) Retrieved February 22, 2016, from Forbes: http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total- over-112-million-records-in-2015/#685b5afe7fd5

Nagaraj, R., & Kalarani, X. A. (2016). Semantically document clustering using

contextual similarities. *International Journal of Applied Engineering Research, 11*(1), 71-76. Retrieved from https://www.ripublication.com/ijaer16/ijaerv11n1_13.pdf

Näsi, M., Oksanen, A., Keipi, T., & Räsänen, P. (2015). Data breaches victimization among young people: a multi nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention, 16*(2), 203-210. doi:10.1080/14043858.2015.1046640

Nass, L., Levit, L., & Gostin, L. (2009). Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. *National Center of Biotechnology Information*. doi.org/10.17226/12458

National Health Care Anti-Fraud Association. (2020). *The U.S. healthcare system and the challenge of fraud*. Retrieved from NHCAA: https://www.nhcaa.org/media/164614/challenges_of_healthcare_fraud.pdf

Newman, L. (2019). A plan to stop breaches with dead simple database encryption. Retrievedfrom https://www.wired.com/story/field-level-encryption-databases-mongobd/

Neveux, E. (2020). Healthcare data: The new prize for hackers. Retrieved from https://www.securelink.com/blog/healthcare-data-new-prize-hackers/

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-Based Nursing, 18*(2), 34-35. doi:10.1136/eb-2015-102054

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. Holistica, 9(3), 71–88. https://doi.org/10.2478/hjbpa-2018-0024

Novinson, M. (2020). 12 biggest cloud threats and vulnerabilities in 2020. Retrieved from CRN:https://www.crn.com/slide-shows/security/12-biggest-cloud-threats-and-vulnerabilities-%20in-2020/5

Offodile, A. C., & Ho, V. (2018). Making “cents” for the patient: improving health care through consumerism. *Issue Brief, 3*.

O’Donnell, A., Kaner, E., Shaw, C., & Haighton, C. (2018). Primary care physicians’ attitudesto the adoption of electronic medical records: A systematic review and evidence synthesis using the clinical adoption framework. *BMC Medical Informatics and Decision Making, 18*. doi:10.1186/s12911-018-0703-x

Offner, K. L., Sitnikova, E., Joiner, K., & MacIntyre, C. R. (2020). Towards understanding cybersecurity capability in Australian healthcare organisations: A systematic review of recent trends, threats and mitigation. *Intelligence and National Security*, 35(4), 556–585.doi: 10.1080/02684527.2020.1752459

Open Web Application Security Project. (2020). *OWASP top ten*. https://owasp.org/www-project-top-ten/

Patel, N. (2020). Social engineering as an evolutionary threat to information security in healthcare organizations. *Jurnal Administrasi Kesehatan Indonesia*, (8(1), 56). doi.org/10.20473/jaki.v8i1.2020.56-64

Patil, A. P., & Chakrabarti, N. (2020). A review into the evolution of hipaa in response to evolving technological environments. *Journal of Cybersecurity and Information Management*, 5(2), 5-15. https://doi.org/10.5281/zenodo.4014219

Pescatore, J. (2019). How to optimize security operations in the cloud through the lens of

theNIST framework. *SANS Information Security Reading*. SANS Institute.

Peterson, D. C., Adams, A., Sanders, S. & Sanford, B. (2018). Assessing and addressing threats and risks to cybersecurity. *Frontiers of Health Services Management, 35*(1), 23–19. https://doi.org/10.1097/HAP.0000000000000040

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

Petrescu, M., Gironda, J. T., & Korgaonkar, P. K. (2018). Online piracy in the context of routine activities and subjective norms. *Journal of Marketing Management*, *34*(3-4), 314-346. https://doi.org/10.1080/0267257X.2018.1452278

Pierre-Francois, W., & Guzman, I. (2020). Factors that influence hipaa secure compliance in small and medium-size health care facilities. 2020 KSU Conference on Cybersecurity.

Pitre, C., Petit, K., Ladd, L., Chisholm. C., & Welch, J. (2018). Physician time management. *MedEdPORTAL*. https://doi.org/10.15766/mep_2374-8265.10681

Ponemon Institute. (2019). *The State of Risk-based Security Management, US & UK 2019.* Ponemon Institute. Tripwire, Inc.

Pratt, T. C. & Turanovic, J. J. (2015). Lifestyle and routine activity theories revisited: The importance of "risk" to the study of victimization. *Victims & Offenders, 11*(3), 335-354. doi:10.1080/15564886.2015.1057351

Priestman, W., Sridharan, S., Vigne, H., Collins, R., Seamer, L., & Sebire, N. J. (2018). What toexpect from electronic patient record system implementation: lessons

learned from published evidence. *Journal of Innovation in Health Informatics*, *25*(2), 92-104.

Pritchard, S. (2018). Compliance in the cloud: Avoiding the cloud compliance trap. Retrievedfrom https://www.computerweekly.com/news/252441643/Compliance-in-the-cloud- Avoiding-the-cloud-compliance-trap

Privacy Rights Clearinghouse. (2019, February). *Privacy Rights Clearinghouse*. Retrieved January 1, 2019, from Privacy Rights Web site: https://www.privacyrights.org/content/health- privacy-hipaa-basics#not%20required%20to%20comply%20HIPAA

Purohit, B. & Singh, P. P. (2013). Data leakage analysis on cloud security. *International Journal of Engineering Research and Applications*, *3*(3), 1311-1316. doi:10.1.1.418.9020&rep=rep1&type=pd

Pyrooz, D. C., Decker, S. H., & Moule Jr, R. K. (2015). Criminal and routine activities in online settings: Gangs, offenders, and the Internet. *Justice Quarterly*, *32*, 471–499. doi:10.1080/07418825.2013.778326

Ragan, S. (2015, February 9). *CSO*. (J. Goodchild, Ed.) Retrieved March 3, 2016, from CSO Online: http://www.csoonline.com/article/2881532/business-continuity/anthem-how- does-a-breach-like-this-happen.html?page=3

Rajaram, A., Hickey, Z., Patel, N., Newbigging, J., & Wolfrom, B. (2020). Training medical students and residents in the use of electronic health records: a systematic review of the literature. *Journal of the American Medical Informatics*

Rajkomar, A., Oren, E., Chen, K., Dai, A. M., Hajaj, N., Hardt, M., & Sundberg, P.

(2018). Scalable and accurate deep learning with electronic health records. *npj Digital Medicine,1*(1), 18. Retrieved from https://www.nature.com/articles/s41746-018-0029-1

Rashid, M., Parah, S. A., Wani, A. R., & Gupta, S. K. (2020). Securing e-health iot data oncloud systems using novel extended role based access control model. In *Internet of Things (IoT)* (pp. 473-489). Springer, Cham.

Rashkovits, S. (2019). The importance of the nurse leader's proactivity and intellectual stimulation in the nursing team workload-learning relationship: A cross-sectional study. *Journal of Advanced Nursing, 75*(11). 2647-2658. https://doi.org//10.1111/jan.14047

Raths, D. (2020). OCR HIPAA audit report highlights risk management shortcomings. Retrievedfrom https://www.hcinnovationgroup.com/cybersecurity/hipaa/article/21203246/ocr-hipaa-audit-report-highlights-risk-management-shortcomings

Rathert, C., Porter, T. H., Mittler, J. N., & Fleig-Palmer, M. (2019). Seven years after Meaningful Use: Physician's and nurses' experiences with electronic health records. *Health care management review, 44*(1), 30-40. doi:10.1097/HMR.0000000000000168

Rathore, H., Mohamed, A., Al-Ali, A., Du, X., & Guizani, M. (2018). A review of security challenges, attacks and resolutions for wireless medical devices [paper presentation]. The *13th International Wireless Communications and Mobile ComputingConference*, Valencia, Spain (pp. 1495-1501). IEEE.

doi.1109/IWCMC.2017.7986505

Reuters. (2017). Anthem to Pay Record $115M to Settle Lawsuits Over Data Breach. Retrieved from https://www.nbcnews.com/news/us-news/anthem-pay-record115m-settle-lawsuits-over-data-breach-n776246

Reynald, D. M., Moir, E., Cook, A., & Vakhitova, Z. (2018). Changing perspectives on guardianship against crime: an examination of the importance of micro-level factors. *Crime Prevention and Community Safety*, *20*(4), 268-283. https://doi.org/10.1057/s41300-018-0049-4

Reyns, B. W., & Scherer, H. (2018). Stalking victimization among college students: The role of disability within a lifestyle-routine activity framework. *Crime & Delinquency*, *64*(5), 650-673. https://doi.org/10.1177/0011128717714794

Reyns, W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216-238.

Reyns, W. (2015). A routine activity perspective on online victimisation. *Journal of Financial Crime, 22*(4), 396-411. doi.org/10.1108/JFC-06-2014-0030

Reyns, B. W., & Henson, B. (2015). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology*, *60*(10), 1119-1139. doi:10.1177/0306624x15572861

Reyns, B. W., Henson, B., & Fisher, B. S. (2015). Guardians of the cyber galaxy: An empirical and theoretical analysis of the guardianship concept from routine 140

activity theory as it applies to online forms of victimization. *Journal of Contemporary Criminal Justice, 32*(2), 148-168. doi:10.1177/1043986215621378

Richardson, J. D., Hudspeth Dalton, S. G., Shafer, J., & Patterson, J. (2016). Assessment fidelity in aphasia research. *American Journal of Speech-Language Pathology, 25*(4S), S788-S797. doi:10.1044/2016_ajslp-15-0146

Rosenbloom, T. S., Smith, J. R., Bowen, R., Burns, J., Riplinger, L., & Payne, T. H. (2019). Updating hipaa for the electronic medical record era. *Journal of the American MedicalInformatics Association, 26*(10), 1115-1119. https://doi.org/10.1093/jamia/ocz090

Rouse, M. (2019a). *Network protocols*. Retrieved from https://searchnetworking.techtarget.com/definition/protocol

Rouse, M. (2019b). *Best practice*. Retrieved from https://searchsoftwarequality.techtarget.com/definition/best-practice

Rowley, J. (2012). Conducting research interviews. *Management Research Review, 35*, 260-271. doi:10.1108/01409171211210154

Rubin, A., & Babbie, E. (2016). Empowerment Series: *Research Methods for Social Work* (9th ed.). Boston, MA: Cengage Learning.

Rutberg, S., & Bouikidis, C. D. (2018). Focusing on the fundamentals: A simplistic differentiation between qualitative and quantitative research. *Nephrology Nursing Journal, 45*(2), 209-213. CNE. http://www.homeworkgain.com/wp-content/uploads/edd/2019/09/20181009143525article2.pdf

Sabillon, R., Serra-Ruiz, J., & Cavaller, V. (2019). An effective cybersecurity training

model to support an organizational awareness program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. *Journal of Cases on Information Technology (JCIT), 21*(3), 26-39. https://doi.org/10.4018/JCIT.2019070102

Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organizations. *Journal of information security and applications*, *40*, 247-257. https://doi.org/10.1016/j.jisa.2017.11.001

Sahai, A., & Waters, B. (2005). Fuzzy Identity-Based Encryption. *Advances in Cryptology – EUROCRYPT 2005*, (pp. vol. 3494, pp. 457-473).

Salwei, M. E., Carayon, P., Hoonakker, P., Hundt, A. S., Novak, C., Wang, Y., & Patterson, B. (2019, November). Assessing workflow of emergency physicians in the use of clinical decision support. In *Proceedings of the Human Factors and Ergonomics Society AnnualMeeting* (Vol. 63, No. 1, pp. 772-776). Sage CA: Los Angeles, CA: SAGE Publications.

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

Savas, A., Smith, E., & Hay, B. (2019). EHR quality indicator tracking: A process improvementpilot project to meet MACRA requirements. *The Nurse Practitioner, 44*(4), 30-39. doi:10.1097/01.NPR.0000554084.05450.0e.

Schmeelk, S. (2019). Where is the risk? Analysis of government reported patient medical databreaches. *IEEE/WIC/ACM International Conference on Web Intelligence on - WI '19, Companion Volume*, (pp.269-272). doi: 10.1145/3358695.3361754

Schmeelk, S. (2020). Creating a standardized risk assessment framework library for healthcare information technology. *Hawaii International Conference on System Sciences,* 3881–3890. https://scholarspace.manoa.hawaii.edu/bitstream/10125/64216/0384.pdf

Schneier, B. (2005). Two-Factor authentication: Too little, too late. *Communications of the ACM*, *48*(4), 1. doi.org/10.1145/1053291.1053327

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare data breaches: insights and implications. *MDPI Healthcare*, *8*(133), 118. https://doi.org/10.3390/healthcare8020133

Sessions, C. L. (2019). *Exploring Personal Protection Strategies of Cybersecurity Specialists inSocial Media*. Doctoral dissertation, Colorado Technical University l, ProQuest Dissertations Publishing, 2019. 13884061

Serova, E., & Guryeva, I. (2018). Health Care Information Technologies Innovation. In *ECMLG 2018 14th European Conference on Management, Leadership and Governance* (p. 245). Academic Conferences and publishing limited.

Shackelford, S. J.; Mattioli, M.; Myers, S.; Brady, A.; Wang, Y.; Wong, S. (2018). Securing the internet of healthcare. *Minnesota Journal of Law, Science and Technology,* 19(2), 405-454.

Shannon, P. & Hambacher, E. (2014). Authenticity in constructivist inquiry: Assessing an

elusive construct. *Qualitative Report, 19*(52), 1-13. Retrieved from http://nsuworks.nova.edu/tqr/vol19/iss52/3

Sheffer, J., Domas, S., Finn, D, Larson, J.P., Upendra, P., Wirth, A. (2019). How effectively are we protecting protected health information? *Biomedical Instrumentation & Technology, 53*(2), 128–135. doi:10.2345/0899-8205-53.2.128.

Sieck, C., Pearl, N., Bright, T., & Po-Yin Yen, P., (2020). A qualitative study of physician perspectives on adaptation to electronic health records. *BMCMedical Informatics and Decision Making*, *20*(1), 1–8. https://doi-/10.1186/s12911-020-1030-6

Silverman, R. D. (2013). EHRs, EMRs, and health information technology: To meaningful use and beyond. *Journal of Legal Medicine*, *34*(1), 1-6. doi:10.1080/01947648.2013.768134

Silvius, G. A. J., & Stoop, J. (2013). Relationship between strategic information systems planning situational factors, process configuration and success. *Journal of International Technology and Information Management, 22*(1), 1-17. doi:10.1109/hicss.2013.536

Singh, M. M., & Bakar, A. A. (2019). A Systemic cybercrime stakeholders architectural model. *Procedia Computer Science*, *161*, 1147-1155. https://doi.org/10.1016/j.procs.2019.11.227

Shackleford, D. (2019). How to build a security visibility strategy in the cloud. *SANS Information Security Reading.* SANS Institute.

Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K.-K. R. (2020). Applicationsof

blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & Security*, *97*. https://doi-/10.1016/j.cose.2020.101966.

Sidhu, S. S. (November 9th, 2018*). Information security in the healthcare system.* (Master's Thesis). California State Polytechnic University. Retrieved from Bronco Scholar Thesis,Dissertation and Student Research database. (URI No. 10211.3/206613)

Sittig, D. F., Belmont, E., & Singh, H. (2018). Improving the safety of health information technology requires shared responsibility: It is time we all step up. *Healthcare*, *6*(1), 7–12. https://doi.org/10.1016/j.hjdsi.2017.06.004

Smith, J., & Noble, H. (2014). Bias in research. *Evidence Based Nursing, 17,* 100-101. doi:10.1136/eb-2014-101946

Smith, P. R. (2018). Collecting sufficient evidence when conducting a case study. *The Qualitative Report*, *23*(5), 1054-1048. https://nsuworks.nova.edu/tqr/vol23/iss5/2/

Snell, E. (2015, November 18). *HeathIT Security.* Retrieved February 21, 2018, from HeathIT Security: http://healthitsecurity.com/news/reviewing-hipaa-compliance-enforcement-actions

Snell, E. (2015, February 26). *HeatlhIT Security*. (E. Snell, Producer, & Xtelligent Network Media) Retrieved March 05, 2018, from HealthIT Security: http://healthitsecurity.com/news/top-tips-on-healthcare-byod-best-practices-mobile-security

Spaniel, D., & Eftekhari, P. (2020). The healthcare research security pandemic: Threats

to patient care, national security, and the economy. Retrieved from https://icitech.org/the- healthcare-research-security-pandemic-threats-to-patient-care-national-security-and-the- economy/

Spyrou, S. S., Bamidis, P., Chouvarda, I., Gogou, G., Tryfon, S. M., & Maglaveras, N. (2002). Healthcare information standards: Comparison of the approaches. *Health Informatics Journal, 8*(1), 14-19. doi:10.1177/146045820200800103

Steber, C. (2018). What's the Difference Between Key Informant Interviews and In-Depth Interviews? Retrieved from cfrinc.net/cfrblog/key-informant-versus-in-depth-interviews

Stedman, A. (2018). *Healthcare is under attack: Investigating the importance of cybersecurity to protect patients and organizations.* (Master's Thesis). Retrieved fromProQuest Dissertations and Theses database. (UMI No. 2042846930)

Stein, M., Campitelli, V., & Mezzio, S. (2020). Managing the impact of cloud computing: Perspectives on vulnerabilities, ERM, and audit services. *The CPA Journal*, 20–27.

Stern, A. D., Gordon, W. J., Landman, A. B., & Kramer, D. B. (2019). Cybersecurity features of digital medical devices: an analysis of FDA product summaries. *BMJ open*, *9*(6), e025374. doi:10.1136/bmjopen-2018-025374

Summers, J. F., O'Neill, D. G., Church, D., Collins, L., Sargan, D., & Brodbelt, D. C. (2019). Health-related welfare prioritization of canine disorders using electronic health records in primary care practice in the UK. *BMC Veterinary Research*, *15*(1), 163. https://doi-org.ezp.waldenulibrary.org/10.1186/s12917-019-1902-0

Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G. (2018). Security and privacy in the medical internet of things: a review. *Security and Communication Networks, 2018.* https://doi.org/10.1155/2018/5978636

Sultanum, N., Brudno, M., Wigdor, D., & Chevalier, F. (2018). More text please! understanding and supporting the use of visualization for clinical text overview. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (p.422). ACM.

Tafreshi, S. (May 2018). *Privacy and security of health information: A novel user-centric approach.* (Master's Thesis). Retrieved from ProQuest (Pub. No. 10744816)

Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. *Future Generation Computer Systems, 98,* 660-671. https://doi.org/10.1016/j.future.2019.03.042

Tariq, M. I., Tayyaba, S., Ashraf, M. W., Rasheed, H., & Khan, F. (2018). Risk base NIST effectiveness analysis for cloud security. *Bahria University Journal of Information & Communication Technology, 10,* 1. https://www.researchgate.net/publication/326414860_Risk_Based_NIST_Effectiveness_Analysis_for_Cloud_Security

Tavares, J., Goulão, A., & Oliveira, T. (2018). Electronic health record portals adoption: empirical model based on UTAUT2. *Informatics for Health and Social Care, 43*(2), 109- 125.

Techapanupreed, C., & Kurutach, W. (2020). Enhancing transaction security for handling

accountability in electronic health records. *Security & Communication Networks*, 1–18. https://doi.org/10.1155/2020/8899409

Terfas, H., Suryn, W., Roy, J., & Eftekhar, S. M. (2018). Extending ISO/IEC 19086 Cloud Computing SLA standards to support cloud service users with the SLA negotiation process. *SQM XXVI*, 127.

Terry, K. (2015). HIPAA breach: Secure data and prevent fines now. Retrieved from http://medicaleconomics.modernmedicine.com/medical-economics/news/hipaa-breach- secure-data-and-prevent-fines-now

Thakkar, D. (2018). *Top 5 biometric devices for your organization*. Retrieved from https://www.bayometric.com/biometric-security-devices-organization/*Management Journal*, *26*(3), 3-12. doi:10.1080/10429247.2014.11432015

Thomas, L.M., & Ingargiola, S. (2021). Learning from the mistakes of others: OCR releasesaudit report. *The National Law Review*, *XI*(19).

Thompson, M. P., & Graetz, I. (2018, December). Hospital adoption of interoperability functions. In *Healthcare*. Elsevier.

Timande, N., Chandak, M. B., & Kamble, M. (2014). Document clustering with feature selection using Dirichlet process mixture model and Dirichlet multinomial allocation model. *International Journal of Engineering Research and Applications*, 10-16. Retrieved from https://pdfs.semanticscholar.org/6a0f/2d593688780a73e12e171ee157bb94b037cc.pdf

Tipton, S. J., Forkey, S., & Choi, Y. B. (2016). Toward proper authentication methods in electronic medical record access compliant to HIPAA and C.I.A. Triangle. *Journal of Medical Systems; New York*, *40*(4), 1–8. doi.org/http://dx.doi.org/10.1007/s10916- 016-0465-x

Towbin, R. S. (2019). *A protection motivation theory approach to healthcare cybersecurity: Amultiple case study* (Doctoral dissertation). Retrieved from ProQuest Dissertation and Theses database. (UMI No. 13809084)

Tubaishat, A. (2018). Perceived usefulness and perceived ease of use of electronic health recordsamong nurses: application of technology acceptance model. *Informatics for Health and Social Care, 43*(4), 379-389.

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.

Tyler, L. B. (2018). Exploring the implementation of cloud security to minimize electronic health records cyberattacks. Walden University. https://scholarworks.waldenu.edu/dissertations/5281/

Vaismoradi, M., & Snelgrove, S. (2019, September). Theme in qualitative content analysis and thematic analysis. In *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research* (Vol. 20, No. 3). https://doi.org/10.17169/fqs-20.3.3376

Van Dyke, M. (2019), *Battling clinician burnout: fighting the epidermic from within. Healthcareexecutives 34* (1), 11-12

Van Galen, L. S., Wang, C. J., Nanayakkara, P. W. B., Paranjape, K., Kramer, M. H. H., & Car, J. (2019). Telehealth requires expansion of physicians' communication competencies training. *Medical teacher, 41(6),* 714-715. https://doi.org/10.1080/0142159X.2018.1481284

Van Kesteren, J. (2016). Assessing the risk and prevalence of hate crime victimization in Western Europe. *International Review of Victimology, 22*(2), 139-160. doi:10.1177/0269758015627046

Vasileiou, I., & Furnell, S. (2019). *Cybersecurity education for awareness and compliance*. IGI Global. https://kevincurran.org/papers/insiderthreats.pdf

Vecchio, J. M. (2013). Once bitten, thrice wise: The varying effects of victimization on routine activities and risk management. *Deviant Behavior, 34*(3), 169-190. doi:10.1080/01639625.2012.726167

Vidich, S. (2021). HIPAA (US). Retrieved from Microsoft: https://docs.microsoft.com/en-us/azure/compliance/offerings/offering-hipaa-us

Vigna, G. (2019). Confusing Patch Management with Vulnerability Management Could Have Dire Results. Just ask Equifax!. https://www. lastline.com/blog/confusing-patch-management-with-vulnerability-management- could-have-dire-results-just-ask-equifax/

Vitari, C., & Ologeanu-Taddei, R. (2018). The intention to use an electronic health record and its antecedents among three different categories of clinical staff. *BMC health services research, 18*(1), 194.

Walker, D. M. (2018). Does participation in health information exchange improve

hospitalefficiency? *Health Care Management Science*, 21(3), 426-438.

Wang, K. C. (2018). Standard lexicons, coding systems and ontologies for interoperability andsemantic computation in imaging. *Journal of Digital Imaging, 31*(3), 353-360.

Wang, L., Wang, Y., Shen, F., Rastegar-Mojarad, M., & Liu, H. (2019). Discovering associations between problem list and practice setting. *BMC Medical Informatics andDecision Making, 19*(Suppl 3*).* doi:10.1186/s12911-019-0779-y

Wang, Y., Kung, L., Wang, W. Y. C., & Cegielski, C. G. (2018). An integrated big data analytics-enabled transformation model: Application to health care. *Information& Management, 55*, 64-79. doi:10.1016/j.im.2017.04.001

Wani, D., & Malhotra, M. (2018). Does the meaningful use of electronic health records improvepatient outcomes? *Journal of Operations Management, 60*(1), 1-18. doi:10.1016/j.jom.2018.06.003

Walsh, R., & Cooper, M. M. (2018). Who provides phishing training? Facts, stories, and peoplelike me. Retrieved from https://bitlab.cas.msu.edu/papers/phishing-stories.pdf

Ward, C., Banks, J., & Pritam, N. (2018, April 10). Ransomware still a top cybersecurity threat,warns Verizon 2018 data breach investigations report. Retrieved from Verizon.com: https://www.verizon.com/about/news/ransomware-still-topcybersecurity-threat-warns- verizon-2018-data-breach-investigations-report

Weisburd, D., Groff, E. R., & Yang, S.-M. (2014). The importance of both opportunity and social disorganization theory in a future research agenda to advance criminological theory and crime prevention at places. *Journal of Research in*

Crime and Delinquency, 51, 499–508. doi:10.1177/0022427814530404

Weller, S. C., Vickers, B., Bernard, H. R., Blackburn, A. M., Borgatti, S., Gravlee, C. C., & Johnson, J. C. (2018). Open-ended interview questions and saturation. *PloS one, 13*(6), e0198606. https://doi.org/10.1371/journal.pone.0198606

Wencheng S., Zhiping C., Yangyang L., Fang L., Shengqun F., & Guoyan W. (2018). Data Processing and Text Mining Technologies on Electronic Medical Records: A Review. *Journal of Healthcare Engineering, 2018*. https://doi-10.1155/2018/4302425.

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime, 26*(1), 277-292. https://doi.org/10.1108/JFC-10-2017-0095

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security, 88,* 101640. https://doi.org/10.1016/j.cose.2019.101640

Willard-Grace, R., Knox, M., Huang, B., Hammer, H., Kivlahan, C., & Grumbach, K. (2019). Burnout and health care workforce turnover. *The Annals of Family Medicine, 17*(1), 36-41.

Williams, M. L. (2015). Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology, 56*(1), 21-48. doi:10.1093/bjc/azv011

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities theory. *Deviant Behavior, 40*(9), 1119-1131.

https://doi.org/10.1080/01639625.2018.1461786

Woodside, J. M., & Amiri, S. (2018). Healthcare hyperchain: Digital transformation in thehealthcare value chain. Retrieved from https://www.aisnet.org

World Health Organization (WHO). (2018). *Classification of digital health interventions v1. 0: ashared language to describe the uses of digital technology for health*. Retrieved from https://apps.who.int/iris/bitstream/handle/10665/260480/WHO-RHR-18.06- eng.pdf?sequence=1

Xie, X., Zou, H., & Qi, G. (2018). Knowledge absorptive capacity and innovation performance in high-tech companies: A multi-mediating analysis. *Journal of Business Research, 88*, 289-297.

Yaokumah, W., Walker, D. O., & Kumah, P. (2019). SETA and Security Behavior: MediatingRole of Employee Relations, Monitoring, and Accountability. *Journal of Global Information Management (JGIM), 27*(2), 102-121.

Yarachi, N., & Gopal, R. D. (2018). The role of HIPAA omnibus rules in reducing the frequency of medical data breaches: Insights from an empirical study. *The MilbankQuarterly, 96*(1), 144-166. doi:10.1111/1468-0009.12314

Yates, S. W. (2020). Physician stress and burnout. *The American Journal of Medicine, 133*(2), 160-164.

Yen, H. (2009, January 28). VA agrees to pay $20 million to veterans in 2006 data breach. Retrieved from http://archive.boston.com/news/nation/articles/2009/01/28/va_agrees_to_pay_20_million _to_veterans_in_2006_data_breach/

Yeong, M. L., Ismail, R., Ismail, N. H., & Hamzah, M. (2018). Interview protocol refinement: Fine-tuning qualitative research interview questions for multi-racial populations in Malaysia. *The Qualitative Report, 23*(11), 2700-2713. https://nsuworks.nova.edu/tqr/vol23/iss11/7/

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education, 48*(2), 311-325. doi:10.1111/ejed.12014

Yin, R. K. (2014). *Case study research: Design and methods* (5th ed). Thousand Oaks, CA: Sage.

Young, J. C., Rose, D. C., Mumby, H. S., Benitez-Capistros, F., Derrick, C. J., Finch, T., . . . Mukherjee, N. (2018). A methodological guide to using and reporting on interviews inconservation science research. *Methods in Ecology and Evolution, 9*(1), 10-19. doi:10.1111/2041-210x.12828

Yu, K. H., Beam, A. L., & Kohane, I. S. (2018). Artificial intelligence in healthcare. *NatureBiomedical Engineering*, *2*(10), 719.

Yu, P., & Qian, S. (2018). Developing a theoretical model and questionnaire survey instrument to measure the success of electronic health records in residential aged care. *PloS one*, *13*(1), e0190749.

Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). Fhirchain: applyingblockchain to securely and scalably share clinical data. *Computational and Structural Biotechnology Journal*, *16*, 267-278.

Zhou, J., Sun, L., Song, M., & Song, J. (2017). Anonymous limited-use-proof entity

authentication protocol. *Wireless Personal Communications, 96*(1), 1065–1082. doi:10.1007/s11277-017-4221-4

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: a comparative study. *Journal of Computer Information Systems,* 1-16. https://doi.org/10.1080/08874417.2020.1712269

Appendix A: Introductory Email to Participants

Date: `Introductory E-mail to Participants`

Dear Potential Research Participant,

I'm working on my doctorate degree in information technology at Walden University. I'm studying "Security Strategies of Electronic Health Record Systems." According to Cascardo (2015), the 2013 Redspin Breach Report indicated that more than 800 patient data breaches have occurred since 2009, with 29 million patient records affected by Health Insurance Portability and Accountability Act of 1996 (HIPPA) violations. Data breaches in health care can potentially upset the trust of the facility in perspective to the relationship with the patient.

I'm searching for an organization with an information security staff of at least 4-10 people to participate in my study. These people could be a combination of managers or directors within the organization. The study would involve a short one-on-one interview with each person and a review of any documentation involving security strategies of electronic health record systems. All information about the organization and participants is confidential and not made public in any way. My study would simply refer to "the organization," "participant 1", etc. A confidentiality agreement can be provided. A copy of my study results will be provided to the organization.

Sincerely,

Benjamin Thomas Gerke

Appendix B: Interview Protocol

Interviewee (Title): _____

Interviewer: Benjamin Thomas Gerke

Background:

_____ A: Interviewee Background

_____ B: Demographics

Other Topics Discussed: _____

_____

Documents Obtained: _____

_____

Post Interview Comments or Leads:

_____

Introductory Protocol

To facilitate our note-taking, we would like to audiotape our conversations today. For your information, only researchers on the project will be privy to the tapes, which will be eventually destroyed after they are transcribed. Essentially, this document states that: (1) all information will be held confidential, (2) your participation is voluntary, and you may stop at any time if you feel uncomfortable, and (3) we do not intend to inflict any harm.

Thank you for your agreeing to participate. I have planned this interview to last no longer than 45 minutes. During this time, I will have several questions that I would like to cover.

Introduction

You have been identified as someone who has a great deal to share about data security—my research project as a whole focuses on the implementation to minimize EHR data breaches. My study does not aim to evaluate your techniques or experiences. Rather, I am trying to learn more about your strategies against EHR data breaches.

A. Interviewee

Background

How long have you been …?

_____ in your present position?

_____ at this medical facility?

B. Demographics

Post Interview Comments and/or Observations:

Appendix C: Interview Questions

Demographic Questions

1. What is your role within your organization, and do you have a team whose focus is primarily on data breaches?
2. Describe the architecture of your EHR. Include if you have your cloud or use the third-party vendor. Describe the responsibility of a third-party vendor if applicable. What is your role in keeping EHR secure from data breaches?

Interview Questions

1. What is your IT background, such as education, work experience, etc.?
2. What is your role in respect to database security measures for the EHR?
3. What security measures does your organization use to prevent EHR breaches?
4. What solutions does your organization provide with regards to preventing EHR breaches?
5. What lessons learned do you have regarding preventing EHR data breaches?
6. With your experience as an IT professional, what obstacles does your organization face with regards to implementing EHR security measures, and why?
7. In terms of EHR, are there any concerns in implementing security measures, and if so, what has the organization done to rectify these concerns?