A NARRATIVE REVIEW OF ADVANTAGEOUS CYBERSECURITY FRAMEWORKS AND REGULATIONS IN THE UNITED STATES HEALTHCARE SYSTEM

by

Mustafa Farouk Abo El Rob

B.S., University of Jordan, 2006
M.S., Colorado Technical University, 2008
M.B.A., Regis University, 2013

A Research Paper Submitted to the School of Computing Faculty of

Middle Georgia State University in

Partial Fulfillment of the Requirements for the Degree

DOCTOR OF SCIENCE IN INFORMATION TECHNOLOGY

MACON, GEORGIA
2023

A narrative review of advantageous cybersecurity frameworks and regulations in the United States healthcare system

Mustafa Abo El Rob, *Middle Georgia State University, mustafa.aboelrob@mga.edu*

Abstract

As the healthcare industry continues to thrive competitively, organizations hold a great dependency on data, especially with the increase in cybersecurity regulations and potential privacy threats. When operating with electronic health information, the United States' healthcare sector bears a significant amount of responsibility in order to ensure adequate cybersecurity protection. Organizations ought to ratify comprehensive cybersecurity frameworks and relevant standards that encompass the industry's compliance needs and particular organizations' security requirements. Health organizations are culpable and required by US law to enforce all necessary security measures and policies to safeguard patient data. This research study presents a narrative review of opportune cybersecurity frameworks, regulations, and their corresponding comparisons based on existing peer-reviewed papers in the healthcare cybersecurity landscape. The study further analyzes the selection of cybersecurity frameworks that sufficiently adhere to healthcare regulatory compliance and privacy conditions. The study examines how cybersecurity frameworks can be transformed to drive security enhancements in the healthcare sector. In consonance with the present research analysis, healthcare organizations can acquire significant advantages from the integration of HITRUST and NIST cybersecurity frameworks. In conclusion, the research demonstrates the detailed strategies that assist organizations to comply with US cybersecurity regulations and standards to ensure effective data privacy.

Keywords: Cybersecurity, frameworks, regulations, standards, compliance, healthcare

Introduction

The number of cyberattacks has significantly increased during the past two years due to the COVID-19 pandemic, as organizations have shifted to the new normal of virtual interactions with employees and clients (Ramadan et al., 2021). According to INTERPOL (2020), "An INTERPOL assessment of the impact of COVID-19 on cybercrime has shown a significant target shift from individuals and small businesses to major corporations, governments, and critical infrastructure" (INTERPOL, 2020). Therefore, it has become more significant for organizations to respond apprehensively to the increase in data breaches. The need for health organizations to shift their priorities from utilizing conventional security controls to implementing effective cybersecurity strategies has come at a demanding time. These strategies and cyber defenses are based upon best practices derived from global frameworks that provide sets of standards and guidelines for managing cybersecurity risks.

There are several worldwide cybersecurity frameworks and regulations, however, for this research study, the researcher reviewed and analyzed the main frameworks and regulations in the United States healthcare sector. The paper will differentiate between regulations, standards, and cybersecurity frameworks as there are varied guidelines for each category. The cybersecurity regulations and private-sector standards discussed are shown below:

- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- Payment Card Industry Data Security Standard (PCI-DSS)

- International Organization for Standardization and International Electrotechnical Commission (ISO/IEC 27000 Series)

The cybersecurity frameworks examined in the research study are listed below:

- National Institute of Standard and Technology (NIST)
- MITRE ATT&CK
- Control Objectives for Information and Related Technology (COBIT)
- Health Information Trust Alliance (HITRUST)

There are a wide array of cybersecurity strategies and policies utilized in countries around the world. The research study will encompass a detailed discussion of the cybersecurity frameworks and regulations in the United States, specifically. The review will concentrate on the United States as a study population because there are distinct variations in the economy, infrastructure, and technological advancements within the healthcare field. The United States aims and continues to protect the American people by enforcing various security guidelines. The first enforcement is with the creation of the Fourth Amendment in the United States Constitution, in which certain aspects of security and privacy are outlined. Specifically, "privacy risks and harms are addressed in sector-and harm-specific privacy laws, which are tailored to industries and risks" (Determann, 2020, p. 241). The Fourth Amendment and subsequent privacy laws are pertinent as the analyzed cybersecurity frameworks in the following research study are based out of the United States.

This research assessed cybersecurity frameworks and regulations, based on certain limitations of data protection within the healthcare sector in the United States. These regulations reinforce patient care and comply with policy requirements through increased privacy, data protection, and precise health information management. Analysts from the U.S. Department of Health and Human Services (DHHS) Office for Civil Rights (OCR) have reported on the immense challenges of data breaches and residual cyber effects on healthcare organizations (U.S. DHHS-OCR, 2015). According to the HIPAA Journal (2022), "data breach statistics clearly show that there has been an upward trend in data breaches over the past 10 years, with 2021 seeing more data breaches reported than any other year since records first started being published by OCR" (HIPAA Journal, 2022). It is important to note the statistics of data breaches as the cybersecurity frameworks in healthcare organizations will enable greater security protection.

Purpose

The purpose of the study is to evaluate the cybersecurity frameworks and regulations in the US healthcare sector and propose the most advantageous guidelines. Healthcare organizations should implement a cybersecurity framework and Information Security (IS) strategies to safeguard healthcare data from corporate negligence and cyberattacks. The implementation of security requirements will further promote the mitigation of cyber risks in healthcare practices.

Research Questions

The research study acknowledged the following questions about cybersecurity and regulatory requirements:

RQ1: In what way can cybersecurity frameworks be transformed to drive security enhancements in the healthcare sector?

RQ2: What are the strategies delineated by health organizations to attain compliance with cybersecurity regulations and standards in the United States to ensure effective data privacy?

The first research question relates to the future of cybersecurity frameworks to transform the digital enterprise within healthcare. The second question addresses the current state of IT security governance in the healthcare sector.

The objective of the study was to identify an optimal cybersecurity framework that is opportune for healthcare organizations in the United States. The framework will outline a set of regulatory standards and protocols that will enable healthcare organizations to safeguard against new and ongoing malicious activities. Several approaches will be discussed in the study, including the analysis of effective cybersecurity strategies to prepare for the present and immediate future, implementing proactive techniques and robust controls to secure critical assets, modernizing cybersecurity infrastructure, increasing measures in systems development, promoting a corporate culture of security, and providing comprehensive security awareness training programs for all employees.

The research study entails a review of the literature, a detailed methodology, results, and a discussion. The review of the literature consists of cybersecurity frameworks in the healthcare sector. The methodology of the study includes the data procedure, eligibility criteria of the references, and thematic analysis. Following the literature review and methodology sections, the study will encompass the findings as presented in the results and a pertinent discussion of the related cybersecurity outcomes. These outcomes will further include the interpretation and implications of the findings. To complete a comprehensive research analysis, a conclusion is presented to address the limitations and recommendations of potential future studies.

Review of the Literature

The United States healthcare industry is burgeoning yearly, and its effects are increasing rapidly with the occurrence of the COVID-19 Pandemic in 2020. As security breaches continue to rise, health organizations have prompted investments in cybersecurity and modernized technologies to address challenges in data protection and privacy (He et al., 2021). In response to COVID, the spending of the U.S. healthcare system tremendously increased by 10.3% in 2020 and 2.7% in 2021, reaching $4.3 trillion which accounted for a total expenditure of 18.3% of Gross Domestic Product (GDP) as reported by the U.S. Centers for Medicare & Medicaid Services (2021).

Technological advancements, in the early 2000s, transformed the health record and care procedures in the industry by striving to protect practitioners and patients alike. These advancements were initiated through patient form digitization, cybersecurity guidelines, and data privacy protocols. Critical analysis of the United States protection laws to information technology compliance and policies must be referenced to adequately evaluate the modernization of the cybersecurity frameworks and regulations in the healthcare sector today. There is an ongoing consensus among researchers and professionals that the United States lacks a comprehensive federal data security law. However, there are industry-specific laws, policies, and state regulations to protect individuals (Mabee, 2020).

The healthcare sector quickly discerned the essentiality of protecting its data for patients and medical organizations. For the health industry, the U.S. Congress introduced the first industry-specific legislation as Health Insurance Portability and Accountability Act (HIPAA) in 1996. HIPAA consists of security rules that mandate "hospitals, clinics, and other healthcare establishments must keep all electronic protected health information (e-PHI) confidential and secure from potential cyber-attacks" (Moore, 2018, p. 30). By further establishing HIPAA, the protected health information ("PHI") was introduced in 45 CFR § 160.103 to define personal, protected information such as medical history, health diagnoses, and insurance data to identify patients' information. PHI was supplemented by the development of electronically protected health information (ePHI). According to researcher Lothar Determann, "the disclosure of such information is based on the patient's express written authorization, with some exceptions for specific circumstances, such as a legal requirement for disclosure" (Determann, 2020, p. 242).

In response to HIPAA compliances, healthcare providers implemented information security guidelines and enhanced privacy protocols to protect their patients' health information. The healthcare field had a dynamic shift when electronic health records (EHR) were introduced. The development of EHR has stimulated the evolution of HIPAA compliance (Kim, 2016). HIPAA and additional privacy laws have promoted significant IT policies and compliance transformations by enabling a new security standard for the healthcare field and pertinent industries such as the pharmaceutical and financial sectors. The second law consecutive to HIPAA was the Health Information Technology for Economic and Clinical Health (HITECH) Act (Mabee, 2020; Rowe, 2016). The HITECH act enabled a greater network integration among US health providers by inciting them to adopt privacy and security protocols to protect the patients' health data. These two laws are recognized by researchers as the fundamental security and privacy guidelines in the US healthcare industry.

Correlating to HIPAA and HITECH, the United States government implemented consumer privacy protocols to strengthen the existing cybersecurity guidelines. This was initiated by the Federal Trade Commission (FTC), an independent agency, that strives to enforce civil liberties to protect consumers. One important enforcement is the Gramm-Leach-Bliley Act which specifically includes the FTC's Standards for Safeguarding Customer Information. The standards primarily incorporate more "guidance on how to develop and implement specific aspects of an overall information security program, such as access controls, authentication, and encryption" about patient information (Federal Trade Commission, 2022). Furthermore, a Payment Card Industry (PCI) Data Security Standard was established and imposed to shield cardholder data privacy. This standard enabled a higher level of data security by protecting "all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data" (Sloan, 2014, p. 15).

In discussing federal laws, one must highlight complementary state laws. One primary regulation enforced in the state of California is the Confidentiality of Medical Information Act (CMIA), which was issued in 1981 (California Legislative Information, 2017). With the implemented Act, several states are following suit. The policy regulation addresses online services, more specifically the providers and contractors that disclose the patients' medical information (Determann, 2020).

As more healthcare organizations aim to protect their patient's information through federal and state laws, these professionals must also strive to implement secure networks by evaluating comprehensive information security and quality standards. One organization that specializes in the creation of these principles is the International Organization of Standardization (ISO). ISO was established in 1947 as a non-governmental international organization consisting of various industry experts that concentrate on areas of safety, quality, efficiency, and systems management. In association with ISO, the International Electrotechnical Commission (IEC) also contributes to international standards. The primary guidelines addressed in this literature review correspond significantly with the ISO/IEC 27000 series, these encompassing standards support information security and privacy protection.

In greater detail, ISO 27001 focuses on Information Security Management Systems (ISMS) primarily utilized to enforce information security and risk management guidelines within organizations (Taherdoost, 2022). The second standard in the series is 27002 which consists of the information security code of practice (International Organization for Standardization, 2013). The code describes the wide array of "potential controls and control mechanisms which may be implemented, in theory, subject to the guidance provided within ISO 27001" (International Organization for Standardization, 2013). The third standard in the series is 27003 which further supports the implementation of ISMS. The fourth standard in the series is 27004 which incorporates the performance evaluation, measurements, and metrics of ISMS. The fifth standard in the series is 27005 which outlines risk management approaches for an organization, "specifically supporting the requirements of an information security management system defined by ISO 27001" (International

Organization for Standardization, 2013). The last standard in the series is ISO 27006 where organizations can reference certification and registration about ISMS.

When addressing security guidelines in healthcare, one must be cognizant of the various cyber frameworks that are built upon the foundation of privacy laws and regulations. Each framework has its advantages allowing an organization to adopt a unique model that considers the essential cybersecurity needs of their business. The literature review will analyze four essential and prominent cybersecurity frameworks.

The first cybersecurity framework addressed in this literature review was developed by the National Institute of Standards and Technology (NIST, a non-regulatory agency) within the United States Department of Commerce. The National Institute of Standards and Technology released the specific guidelines of NIST SP 800-53, in 2005, where it characterized the protection of information systems and the mitigation of privacy risks, in addition to highlighting the implementation of security controls for the federal government agencies (NIST, 2005). It is significant to note that the revisions of NIST SP 800-53 were made consonant with the Federal Information Security Management Act (FISMA) and the Public Law (P.L.) 107-347 (Ibrahim et al., 2018).

The specific references will discuss the "Cybersecurity Framework (CSF)" established by President Obama's Executive Order (EO) 13636 named "Improving Critical Infrastructure Cybersecurity" and issued in February 2013. One of the key components of EO 13636 is the NIST requirement to create "a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks" (Obama, 2013, Section 7). Corresponding to President Obama's Executive Order, President Trump also enforced Executive Order 13800 entitled "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" in May 2017. This Executive Order mandated that all federal agencies must manage cyber risks through the NIST cybersecurity framework. With Trump's enforcement, the NIST Cybersecurity Framework became the law of the land for federal government agencies (U.S. Cybersecurity & Infrastructure Security Agency, 2020). NIST CSF was founded based on existing cybersecurity standards and practices that are identified as an abstraction of distinguished cybersecurity frameworks, such as NIST SP 800-53, ISO 27001, and COBIT 5. With the new Biden administration, the 14028 Executive Order published on May 12, 2021, outlined the standards and guidelines that focused on improving cybersecurity approaches across several frameworks, including NIST for federal agencies and industry-specific organizations (Biden, 2021). The executive order concentrates on numerous factors such as the modernization of cybersecurity standards, advancement of supply chain security, and refinement of remediation competencies (U.S. Cybersecurity & Infrastructure Security Agency, 2021).

NIST CSF is based on three main segments which are the core, risk tiers, and alignment profiles. The framework core is a compilation of cybersecurity activities that are "intended to result in specific cybersecurity outcomes. These activities are specified in terms of the following five basic functions: Identify, Protect, Detect, Respond, and Recover" (Gordon et al., 2020, p. 3). The risk tiers are organizational instruments to model risk management practices in cybersecurity. There are four self-ranking tiers that range from Partial (Tier 1) to Adaptive (Tier 4). "Each Tier refers to an increasing level of rigor and sophistication in an organization's cybersecurity practices" (Shen, 2014, p. 4). Tier 1 (Partial) is the lowest ranking that is categorized as "an organization not having "formalized" risk management practices and having little awareness of cybersecurity risks" (Shen, 2014, p. 4). Tier 4 (Adaptive) demonstrates that organizations can comply with cybersecurity etiquettes through a current structured knowledge base. Lastly, the alignment profiles refer to how a specific organization's cybersecurity action coordinates with the various NIST CSF requirements, potential risks, and subsequent mitigation tactics.

For an accurate assessment, cybersecurity professionals should evaluate the "as is" security profile state of the organization, this can be known as the Current Profile. With this profile, the organization should collaborate to create a Target Profile which is the “to be” security profile state. The planning and implementation of these two profiles will enable the organization to identify various opportunities and limitations for improving cybersecurity maturity. “Framework profiles can be determined based on particular implementation scenarios, and therefore, the gap between Current Profile and Target Profile would vary as per scenario” (Ibrahim et al., 2018, p. 5173). The utilization of NIST CSF can be customized to adapt across industries in the United States and abroad.

For relevant context, the frameworks presented in the literature review will be mapped in a simplified version of the table later presented in the Appendix. The frameworks and standards include ISO/IEC 27000 Series, NIST CSF, and COBIT. The purpose of the table is to highlight the correlation between the five functions, as provided by the NIST CSF, and the corresponding security controls from each framework. The five functions are Identify, Protect, Detect, Respond, and Recover. Please refer to the extensive version of the table in section A of the Appendix.

Table 1: Mappings of NIST CSF Functions and Categories to Corresponding Security Control Classifications from ISO/IEC 27000 Series, NIST CSF, and COBIT.

Function	Category	Corresponding Security Control Classification
Identify	Governance	• ISO/IEC 27001:2013 Clause 6 • NIST SP 800-53 Rev. 4 SA-2, PM-3, PM-7, PM-9, PM-10, PM-11 • COBIT 5 EDM03.02, APO12.02, APO12.05, DSS04.02
	Risk Management Strategy	• ISO/IEC 27001:2013 Clause 6.1.3, Clause 8.3, Clause 9.3 • NIST SP 800-53 Rev. 4 PM-9 • COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02
Protect	Identity Management, Authentication, and Access Control	• ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 • NIST SP 800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24 • COBIT 5 DSS05.04
	Awareness and Training	• ISO/IEC 27001:2013 A.7.2.2, A.12.2.1 • NIST SP 800-53 Rev. 4 AT-2, PM-13 • COBIT 5 APO07.03, BAI05.07
	Data Security	• ISO/IEC 27001:2013 A.6.1.2 – A.14.1.3 • NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4 • COBIT 5 APO01.06, DSS05.04, DSS05.07, DSS06.02
	Information Protection Processes and Procedures	• ISO/IEC 27001:2013 A.12.1.2 – A.14.2.4 • NIST SP 800-53 Rev. 4 CM-2 – CM-7, CM-9, SA-10 • COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05
Detect	Security Continuous Monitoring	• ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1 • NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4 • COBIT 5 DSS05.02, DSS05.05
Respond	Mitigation	• ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 • NIST SP 800-53 Rev. 4 IR-4 • COBIT 5 APO12.06
Recover	Improvements	• ISO/IEC 27001:2013 A.16.1.6, Clause 10 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8 • COBIT 5 APO12.06, BAI05.07, DSS04.08

Information was researched in part by the US Department of Health and Human Services (HHS) – Office for Civil Rights (OCR) which released a crosswalk document addressing NIST and other various cybersecurity frameworks (U.S. DHHS-OCR, 2016).

In addressing NIST CSF, researchers, and professionals assert that another commonly utilized framework is the MITRE ATT&CK. MITRE ATT&CK is an open-source cybersecurity framework that utilizes real-world experiences to develop tactics, techniques, and a substantive knowledge base to provide organizations with a foundation of security standards and guidelines (Strom et al., 2020). The MITRE ATT&CK framework is composed of three main matrices: Enterprise, Mobile, and Industrial Control Systems (ICS). The MITRE ATT&CK adopts a more holistic approach with both PRE-ATT&CK and ATT&CK models. PRE-ATT&CK is a complementary model that focuses on "the preceding preparation phases, allowing organizations to predict and prepare for attacks before they even happen" (Georgiadou et al., 2021).

Authors Alexander et al. (2020) examined the correlation between the MITRE ATT&CK framework for Enterprise and ICS by positing the following primary question asked by numerous MITRE researchers, "How well do attacks against ICS map to the existing ATT&CK for Enterprise knowledge base?" (Alexander et al., 2020, p. 1). The question was answered through the scope of the different stages of the cybersecurity attacks discussed in the reference article. In "the initial stages of these attacks involving IT infrastructure were able to be expressed using tactics, techniques, and procedures (TTPs) present in the ATT&CK for Enterprise knowledge base" (Alexander et al., 2020, p. 1).

There are four fundamental concepts of MITRE ATT&CK that have been distinguished by researchers (Alexander et al., 2020). The first concept is the maintenance of an effective adversary's perception. The second concept is incorporating and refining the organization based on "real-world event activity, derived from empirical examples and incidents" (Alexander et al., 2020, p. 14). "Content with appropriate levels of abstraction, to effectively connect offensive behavior with potential countermeasures" is the third encompassing concept of MITRE ATT&CK. The fourth and final concept is underscoring "the failures and consequences that can arise from these adversary behaviors" (Alexander et al., 2020, p. 14). The integration of these four essential concepts has demonstrated how organizations comprehensively plan for adversarial tactics, techniques, and common knowledge.

Corresponding to the earlier frameworks discussed, the Control Objectives for Information and Related Technologies (COBIT) is an additional cybersecurity scaffolding that was initially established in 1996 by ISACA, a non-profit global association centralized around technology governance. Within the realm of COBIT, there are two relevant publications: COBIT 5, which was released in 2012, and more recently COBIT 2019, which was released in 2018. The literature review and subsequent paper sections will refer to COBIT 5 as COBIT, given that the present analysis aligns with the guidelines of the COBIT 5 cybersecurity framework. Cybersecurity professionals assert that COBIT 5 can be utilized in both commercial and public enterprises of all sizes. Through the application of COBIT, information technology can be governed and managed holistically by aligning business objectives, tools, and resources to reflect adequate IT compliance responsibilities (ISACA, 2012). Furthermore, COBIT 5 "not only can be used for IT Governance but can be used as a controller for Information Security and Cybersecurity" (Wang, 2019, p. 159). The following five main COBIT principles are universal to organizations and businesses across industries (in the private and public sectors):

- Principle 1 – Meeting Stakeholder Needs: This principle strikes a balance between optimization of risk and benefits where the organization can enrich business value for their stakeholders. Generating business value is done through the use of COBIT and additional enablers where every organization can tailor its need and requirements to specific goals.
- Principle 2 – Covering the Enterprise End-to-end: This principle utilizes governance and risk management through a business-wide scope entailing all aspects of an organization instead of just the technology division. Therefore, COBIT should be applied to the enterprise as a whole to promote the organization's value.
- Principle 3 – Applying a Single, Integrated Framework: COBIT provides a comprehensive framework that combines processes and best practices correlating to information technology

governance. This is accomplished through the identification of risks and the delineation of procedures to enhance the current processes within the enterprise.

- Principle 4 – Enabling a Holistic Approach: This principle highlights the significance of utilizing the seven core COBIT enablers to implement efficient methodologies for management systems and governance in the organization's IT enterprise. The seven COBIT enablers provided by ISACA (2012) are principles (policies and frameworks), processes, organizational structures, culture (ethics and behavior), information, services (infrastructure and applications), and people (skills and competencies).
- Principle 5 – Separating Governance From Management: It is essential for the organization to make a clear distinction between management and governance. These respective specialties incorporate various organizational structures, purposes, and requirements. There are two specific definitions for governance and management as mentioned by ISACA.

    - Governance ensures that "stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives" (ISACA, 2012, p. 14).
    - Management is defined as the creation of distinct plans that execute "activities in alignment with the direction set by the governance body to achieve the enterprise objectives" (ISACA, 2012, p. 14).

Coinciding with the previous frameworks discussed, the last framework examined is the Health Information Trust Alliance Cybersecurity Framework (HITRUST CSF), which provides "a comprehensive, flexible, and efficient approach to regulatory compliance and risk management" (HITRUST Alliance, 2021, p. 5). The framework integrates both the security and privacy provisions for organizations including federal laws, such as HIPAA and HITECH, while encompassing various federal rules and guidelines for agencies such as NIST and COBIT. HITRUST CSF implements a centralized solution that is customized to the demands of the classified organization by streamlining the complex security requirements. HITRUST was established in partnership with data protection specialists that deliberated over relevant regulations and standards to create a distinct risk and compliance-based cybersecurity framework. The pertinent security and privacy controls can be tailored to fit the risk profile of a specific organization (HITRUST Alliance, 2021). Risk profiles can vary from organization to organization because each specific entity must interact with distinct consumers, stakeholders, and third-party end-users.

HITRUST CSF consists of 14 control categories that entail extensive control objectives and specifications. The primary HITRUST approach embodies four main phases: identify & define (phase 1), specify (phase 2), implement & manage (phase 3), and assess & report (phase 4). These four phases illustrate the standard mapping of the framework to enhance the risk management process and present security controls. The basis of the HITRUST CSF is contingent on ISO/IEC 207000 series as discussed previously in the literature review. With the incorporation of the security guidelines in the ISO 27000 series, organizations can acquire an accumulated knowledge of "more than 40 other security and privacy-related regulations, standards, and frameworks providing comprehensive and prescriptive coverage" (HITRUST Alliance, 2021, p. 3). This demonstrates an interdisciplinary perspective on how cybersecurity frameworks correlate and build upon the current models to advance protection initiatives.

HITRUST initiated a way to reach organizations of different sizes through a distinct technique known as CyberAid. This technique was constructed to primarily reinforce security protocols for small-size health organizations, specifically for practices with 100 employees or less (Cabrera, 2017). Small-size organizations are the target clients for CyberAid because studies show that these entities are struggling with implementing cyber defenses, regulatory compliances, and security training for their employees. With the utilization of HITRUST, organizations of varying sizes can proactively respond to the expanding potential risks and data breaches.

Methodology

Data Procedure

The various cybersecurity frameworks and regulations were meticulously assessed with a constructive narrative review (Jones, 2004). The articles utilized in the paper are based on a forward and backward citation searching technique, which facilitated extensive research on advantageous cybersecurity frameworks and regulations implemented in the United States healthcare system. Selected articles were identified through a set of inclusion and exclusion criteria connected to the AND Boolean search strategy.

Eligibility Criteria

The inclusion criteria were research articles that provided empirical comparisons between the various cybersecurity frameworks and regulations, papers published between 2002 and later, and full-text peer-reviewed articles. The exclusion criteria were research articles written in other languages than English, presentations, posters, and short articles with less than four pages.

Search Strategy

Key articles and relevant topic articles were utilized in the narrative review. The relevant articles were classified by title and abstract examination through institutionally funded subscriptions that are comprised of Google Scholar, ACM Digital Library, Computer Source, ProQuest Research Library, Academic Search Complete, PubMed, and IEEEXPLORE digital libraries. These digital libraries provide a wide array of peer-reviewed journal articles, research papers, and electronic books (e-books) corresponding to the study topic. The bibliographies for on-topic articles were then utilized to source further articles. A date range restriction was applied, and all chosen articles were dated from the last ten years. The study population was restricted to only the United States healthcare system. Peer-reviewed articles were retained to highlight cybersecurity implications on the US healthcare sector, specific framework limitations, and current mitigation methods of cyber risks in these settings. The keywords applied in the digital library searches were cybersecurity, healthcare, frameworks, United States legislation, regulations, privacy, information security, data breaches, cyberattacks, threats, risks, and critical infrastructure. The desired search string for the frame of reference of the overall paper was as followed: (cybersecurity AND healthcare) OR frameworks OR United States legislation OR regulations OR privacy OR information security OR data breaches OR cyberattacks OR threats OR risks OR critical infrastructure. Articles were retained where there was evidence of cybersecurity issues, and clear implications for healthcare settings, organizational practice, individual practice, or health technology development.

Thematic Analysis

The article methodology follows a scientific method of identification, analysis, evaluation, and proposed recommendations. The findings of the primary articles were determined and categorized into emerging themes. The specific themes are listed below:

1. Preliminary knowledge of the advantageous cybersecurity frameworks:
   A foundational understanding is needed to critically analyze the strengths and limitations of each adequate cybersecurity framework discussed throughout the research paper such as NIST, COBIT, and ISO/IEC 27000 Series.

2. The Impactions of the discussed frameworks in modern healthcare settings:
   More often than not cybersecurity frameworks are utilized in IT-specific industries. However, healthcare organizations have endured numerous breaches of data privacy that demonstrate the essentiality of utilizing cybersecurity techniques to ensure data protection.
3. Assessment of the strengths and limitations of the various frameworks:
   A more well-rounded analysis must entail the advantages and disadvantages to comprehend each cybersecurity framework thoroughly.
4. Analysis of current mitigation methods of cyber risks in US healthcare practice:
   This theme represents the significance of risk management and firmly defines mitigation controls to reduce adverse ramifications in the US healthcare industry.
5. Proposed recommendations for cybersecurity enhancements:
   Providing comprehensive propositions to healthcare organizations in the United States will effectively enable them to address the present cybersecurity implications and prevent future security infringements.

The paper will thoroughly outline these five analytical themes in the various sections of the study. The research will highlight the correlation between the themes and the respective sections.

Results

Over the last decade, the United States healthcare system has actively pursued safeguarding actions to protect patients' health information. These actions span from data privacy guidelines to principles and cybersecurity practices that correlate to data compliance with several federal, state, and industry provisions. Healthcare organizations are obligated to implement security measures to respond to the growing demands of data breaches and comply with cybersecurity regulations (nationally and internationally based). The application of information security approaches is achieved by providing organizations with appropriate methodologies for implementing cybersecurity frameworks and standards, these entail the NIST, MITRE ATT&CK, COBIT, HITRUST, and ISO 27000.

With the variety of frameworks and standards available to healthcare organizations, these entities must choose wisely in implementing a framework that is suitable to the distinct needs and risk tolerance of the organization. The following criteria were created to demonstrate the selection features that coincide with the cybersecurity elements outlined throughout the paper. The feature criteria entail compliance standard level, approach, scope complexity, mechanism, suitability, flexibility, and location prominence. For clarity, the mechanism feature presented in the tables indicates if the framework/regulation is mandatorily or voluntarily applied to the healthcare organization.

Regarding the research question (RQ1- in what way can cybersecurity frameworks be transformed to drive security enhancements in the healthcare sector), the research results indicate that the variable cybersecurity frameworks and the subsequent comparisons are based on the selected feature criteria. Each framework has been identified with its recognizable scope and limitations. These factors illustrate how the frameworks adhere to the guidelines of the healthcare sector. The research question highlights security enhancements as they correspond to the varying frameworks, further analysis of these enhancements will be evaluated in the discussion section of the paper. Based on the results compiled from this research study, HITRUST CSF is the most prevalent framework applied by healthcare organizations in the United States. The design of HITRUST CSF was created with health providers in mind to guarantee compliance with health regulations and policies, especially when organizations are maintaining sensitive patient data.

In reference to the second research question (RQ2 - what are the strategies delineated by health organizations to attain compliance with cybersecurity regulations and standards in the United States to ensure effective data privacy), the research findings denote that the distinct cybersecurity regulations/standards and the corresponding criteria are based on certain key features ranging from scope to compliance and international recognition. For effective maintenance of PHI data, health organizations ought to comply with the United States' regulations and standards to fortify data privacy. Any patient information must be secured as required by United States' law. The specific requirements and limitations illustrate the extent of varied security regulations that health organizations must utilize to comply with data privacy and standards. Based on these features, detailed strategies for health organizations will be defined in practical aspects to achieve compliance and data privacy. The comprehensive strategies will be addressed thoroughly in the discussion section of the paper.

The first table presented below illustrates a comparison of the various cybersecurity frameworks (NIST CSF, MITRE ATT&CK, COBIT, and HITRUST CSF) based on the entailed feature criteria. The second table exhibits a comparison of the cybersecurity regulations and standards (HIPAA, HITECH, PCI-DSS, and ISO/IEC 27000) based on the same feature criteria.

Table 2: Cybersecurity Frameworks Comparison

Features	NIST CSF	MITRE ATT&CK	COBIT	HITRUST CSF
Establisher	U.S. Department of Commerce	MITRE Organization	ISACA	HITRUST Alliance
Date Founded	2004	2013	1996	2007
Current Version	V1.1 in April 2018	V12.1 in October 2022	COBIT 2019 released in 2018	V11.0.0 in January 2023
Origin Background	Cybersecurity research and development was gathered from stakeholders in the public sector, industry, and academia	A common knowledge base of adversary behaviors compiled from real-world observations	Initially planned for large corporations consisting of IT governance controls that were later simplified to meet the specific needs of smaller organizations	A set of security and privacy categories that originally leveraged the ISO/IEC security standards
Approach	Control-based framework	Risk-based framework	Risk-based framework	Control-based framework
Core Foundation	Risk management based	Curated knowledge and threat-based defense	Performance and risk management based	Compliance and information risk management based
Structure	5 core functions, 4 implementation tiers (with 23 categories and 108 subcategories), and a framework profile	Adversarial tactics, techniques, and common knowledge across enterprise, mobile, and ICS matrices	5 main principles with coinciding enablers that outline management and governance	14 control categories comprised of 49 control objectives and 156 control specifications
Mechanism	Voluntary framework	Voluntary framework	Voluntary framework	Voluntary framework
Scope	A set of structural guidelines and best practices to protect organizations against cyberattacks and reduce infrastructure security risk	A professional knowledge base that consists of adversary tactics, techniques, and procedures (TTPs) demonstrating how threat actors execute cyberattacks	A set of guidelines, processes, and tools for IT management and governance including security and risk management	Regulatory requirements and industry standards, including HIPAA, HITECH, and PCI-DSS to manage information security and privacy risks
Certifiability	No	No	Individual-level certification	Yes
Compliance	Not mandatory	Not mandatory	Not mandatory	Not mandatory

Table 2: Cybersecurity Frameworks Comparison (Continued)

Features	**NIST CSF**	**MITRE ATT&CK**	**COBIT**	**HITRUST CSF**
Flexibility	Scalable and customizable to meet the specific requirements of each respective organization	Scalable and customizable to meet the specific requirements of each respective organization	Scalable and customizable to meet the specific requirements of each respective organization	Scalable and customizable to meet the specific requirements of healthcare organizations
Suitability	Pertinent for varied sizes of organizations across industries	Pertinent for varied sizes of organizations across industries	Pertinent for varied sizes of organizations across industries	Healthcare organizations including payers and providers
Location Prominence	Widely adopted, mainly in the United States	Applied internationally	Recognized and applied worldwide	Primarily applied in the United States healthcare sector

Table 3: Cybersecurity Regulations & Standards Comparison

Features	**HIPAA**	**HITECH**	**PCI-DSS**	**ISO/IEC 27000**
Establisher	U.S. Department of Health and Human Services	U.S. Department of Health and Human Services	Payment Card Industry Security Standards Council	International Organization for Standardization
Date Founded	1996	2009	2004	1995
Current Version	HIPAA Omnibus rule in March 2013	HITECH Act amendment in January 2021	V4.0 in March 2022	ISO/IEC 27001: 2022 in October 2022
Origin Background	Federal protection laws for the security and privacy of individuals' health information	Federal law issued to enhance the protection and privacy of electronic health information	Began as requirements to reduce credit card fraud that was later applied as standards for payment processing	A set of standards developed for ISMS covering cybersecurity, privacy, and confidentiality
Approach	Control-based	Control-based	Control-based	Risk-based
Core Foundation	Standard measure of security and privacy protections for PHI data	Guidelines to promote the implementation of electronic health records and the protection of ePHI data	Based standards of payment card data and security management	Based standards of information security management
Structure	Federal law and regulatory standards consisting of privacy, security, breach notification, enforcement, and omnibus rules	Federal law consisting of 4 major subtitles entailing health information technology utilization and privacy improvement	6 categories that contain 12 security requirements and more than 300 sub-requirements	6 primary standards for managing information security and implementing an ISMS

Table 3: Cybersecurity Regulations & Standards Comparison (**Continued**)

Features	**HIPAA**	**HITECH**	**PCI-DSS**	**ISO/IEC 27000**
Mechanism	Mandatory national regulations	Mandatory national regulations	Mandatory national standards	Voluntary international standards
Scope	National standards for electronic health records and privacy protections for individual's health information	National standards for fostering the use of health information technology and enhancing the protection of PHI data	A set of standards designed for securing payment card data and preventing data breaches	Standards for information security management including risk tolerance and compliance with regulatory requirements
Certifiability	No	No	Yes	Yes
Compliance	Mandatory	Mandatory	Mandatory	Not mandatory
Flexibility	Confined to abide by compliance obligations and achieve privacy protections	Confined to abide by compliance obligations and achieve privacy protections	Moderately adaptable to achieve compliance of the regulatory standards and meet the needs of organizations	Scalable and customizable to meet the specific requirements of each respective organization
Suitability	All organizations that manage PHI data	All organizations that manage ePHI data	All organizations that store and process cardholder data	Pertinent for varied sizes of organizations across industries
Location Prominence	Primarily applied in the United States healthcare sector	Primarily applied in the United States healthcare sector	Applied nationally and globally	Recognized and applied worldwide

There are two identified criterion features that were not included in the comparison tables. The two features are the cost and implementation efforts of the different cybersecurity frameworks and standards. Comparing the cost and time efficiency required to implement a cybersecurity framework is based on various aspects, such as the size and complexity of the distinct organization, the scope of the cybersecurity needs, the level of existing protection measures, the cyber-maturity level of the organization, and the required level of regulatory compliance.

Some of the voluntary cybersecurity frameworks, including NIST CSF and MITRE ATT&CK, are open sources and available for free licensing to the public. Other frameworks are proprietary licensed products, such as COBIT and HITRUST CSF. These frameworks have associated fees for tools, enterprise licenses, certifications, training, and consulting services.

Implementing these distinct cybersecurity frameworks vary based on the certification level, validation assessments, audit services, and advisory support of the respective organization. When an organization applies a cybersecurity framework, it is known that there are additional costs associated with the planning and development activities administered by security professionals. These activities are prepared to customize the framework to the organization's specific needs and best cybersecurity practices. Moreover, there are supplementary costs associated with technology resources (e.g., software applications and hardware infrastructure). Once the framework is deployed, the organization must consider ongoing costs that include monitoring and maintenance activities, cybersecurity insurance, and periodical audits to govern compliance.

Discussion

In the last two years with the circumstance of COVID, healthcare organizations have been struggling to maintain the imposed guidelines and procedures of the U.S. Department of Health and Human Services. There was and continues to be an imperative need to enhance cybersecurity practices in the sector to address these new guidelines and the phenomenon of increased cyber incidents. One example of the enhancements is the introduction of new cybersecurity recommendations provided by the U.S. DHHS-OCR to demonstrate the emphasis on telehealth services and the protection of patients' data during the pandemic (U.S. DHHS-OCR, 2022). Moreover, the Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA) have collaborated to release cybersecurity guidelines for healthcare organizations that highlight techniques for combating cybersecurity attacks (National Security Agency/Central Security Service, 2022; U.S. Cybersecurity & Infrastructure Security Agency, 2022). These protocols have contributed to the maturity of the cybersecurity frameworks and best practices which have corresponded to the digital health solutions utilized within the healthcare sector.

To adequately discuss data protection for health organizations (also referred to as research question RQ1 in the present paper), professionals must understand how the various cybersecurity frameworks can be transformed to drive security enhancements in the healthcare sector. All the analyzed frameworks in the research study yield suggestive specifications for advancing cybersecurity practices in the healthcare field. Each specification varies in its scope, depth, focus, and level of relevance. Health organizations can decide on frameworks and standards that are most applicable to their business needs and risk tolerance. This can be the first step in developing the company's cybersecurity strategic plan and implementing robust cyber defenses.

The compliance and privacy requirements of healthcare organizations determine the optimal cybersecurity framework utilized within the medical field. Correlating to the posited research question (RQ1), each framework has an assortment of valuable aspects that range from core foundation to certifiability and suitability. According to the narrative research study, HITRUST CSF has been identified as a widely recognized leading framework in the healthcare industry. Numerous sources have reported the adoption of the HITRUST framework by many health providers, payers, and technology companies in the United States. HITRUST CSF is specifically designed for the healthcare sector which is rooted in industry collaboration. This collaboration demonstrates that medical security professionals have provided their security expertise in the field to assist in constructing a framework, which reflects best practices in health information security and data privacy.

HITRUST CSF is a comprehensive framework that comprises a wide range of security controls and risk management principles that are essential for safeguarding patients' data. One of the greatest advantages of the HITRUST framework is that it complies with healthcare regulations and standards such as HIPAA, HITECH, and PCI-DSS. This ensures that organizations utilizing the framework adhere to the United States' security rules and privacy laws. Furthermore, healthcare organizations can demonstrate their dedication to data privacy and information security by obtaining a HITRUST CSF certification which attests to regulatory compliance and medical data protection (HITRUST Alliance, 2023). The HITRUST Alliance organization continuously improves the framework by conducting frequent reviews, regular audits, potential threat identifications, and guideline updates.

The HITRUST framework has numerous advantages, but like any framework, there are some potential limitations. One broad limitation is the complexity which requires considerable effort and time to implement and maintain within organizations. Small size businesses can find it challenging to utilize the framework effectively. Moreover, the cost of the HITRUST certification process (e.g., audits and assessments) can be excessive for small to mid-sized health organizations as they may have a limited number of resources. In addition, the framework requires persistent maintenance and protocol updates to effectively address evolving threats and the data compliance landscape. Health organizations need to regularly evaluate their risks and revise their security controls to remain compliant with healthcare regulations and privacy standards.

HITRUST CSF provides a concentrated emphasis on healthcare regulatory and standard compliance instead of prominence on proactive cybersecurity measures and risk management. Since the framework does not proactively address risks, there is an increased demand for a more thorough security approach that protects patients' data. One theorized enhancement that can transform the present cybersecurity framework is the integration of multiple frameworks into one comprehensive security structure. This encompassing structure will enhance security coverage, increase efficiency, and streamline the processes of regulatory compliance. Combining multiple frameworks will allow health organizations to abide by their cybersecurity initiatives and accommodate their needs more effectively.

Customizing an enhanced framework will allow organizations to implement a more modernized approach and construct robust security controls that are in line with industry best practices. Subject to the present research analysis, it was determined that a combination of HITRUST and NIST can provide the most effective cybersecurity framework for healthcare organizations. For instance, integrating the HITRUST CSF with the NIST cybersecurity framework can present a stronger emphasis on proactive risk management and cybersecurity measures. The new consolidated framework will bridge any disparities in data protection and provide effective security controls that can mitigate a wider array of potential risks.

A compelling approach to revolutionizing the present cybersecurity frameworks can be the incorporation of emerging technologies, in particular, Artificial Intelligence (AI), Machine Learning (ML), and Data Science (DS). There have been immense technological and operational changes in recent years, predominately in the cybersecurity landscape (Sarker et al., 2020). Corresponding to these changes, industry-specific organizations have initiated intelligent technologies to derive business insights from established security analytics. AI technology has the potential to enhance cybersecurity frameworks by enabling predictive analytics, astute threat detection, and automated response capabilities. These characteristics can be leveraged to analyze large data sets, identify new patterns, and anticipate security threats in the future. Traditional cybersecurity frameworks frequently react to threats after they have already occurred, which generates a reactive functionality. Health organizations will be able to adopt a proactive security approach, through the application of AI and data analytics. The approach will entail a cybersecurity framework that identifies threats in real-time and allow the organization to address any damages effectively.

An additional enhancement to improve a cybersecurity framework's efficacy is applying automated monitoring and testing of security controls. With the proper configuration of automated monitoring, healthcare organizations will be to oversee evolving threats and security risks comprehensively. Presently, one large adverse factor that has impacted health organizations is human error. Increasing automated processes will curtail the number of manual errors caused by end users. Therefore, guarantees that security incidents are detected on a 24/7 basis and governed in a way that provides the organizations with present insights into imminent threats.

By addressing the cybersecurity frameworks and their enhancements, health organizations must consider strategies to attain compliance with cybersecurity regulations and standards in the United States (about research question RQ2). A strategy that can be considered by health organizations is the implementation of a broad spectrum of cybersecurity controls (i.e., management, operational, and physical security controls). These controls will safeguard patients' data from unauthorized access, corruption, and unintentional loss. When health organizations manage sensitive data, there must be effective cybersecurity controls that increase privacy assurance, such as access management, firewalls, encryption, security incident response, and data loss prevention. Supplementary to the security controls, health organizations should apply and maintain their internal policies for adequate cybersecurity practices. For example, organizations can develop incident response and business continuity plans to respond to security incidents effectively, minimize the impact of data breaches, and restore business operations. These policy initiatives should be regularly updated to ensure that the organization complies with the regulations and standards.

Another strategy is to enforce a critical risk assessment where health organizations should periodically evaluate their risks, especially when there is a main business or technology change within the organization. Introducing new technology or operational functions to an organization such as enabling new telemedicine channels, will increase the amount of risk and liability. Therefore, an extensive risk assessment must be undertaken to identify evolving vulnerabilities and implement corresponding preventive measures and safeguards for the organization. Risk assessments are an important component of any effective security operation.

An additional strategy to risk assessment is undergoing security audits within organizations. Regular security audits are necessary for health organizations to assess their security posture, identify areas that require improvement, and continue to maintain compliance with regulations and standards. Security audits recognize any instances in which health organizations are not adhering to the regulatory requirements. The audits will allow organizations to identify and resolve any compliance issues before they turn into more significant ramifications (e.g., data breaches, legal penalties, regulatory fines). These security audits must be conducted consistently to have a more proactive security approach. Various types of audits that aid an organization with compliance and cybersecurity standards. An internal audit is one type of audit where organizations utilize their internal professionals or independent auditors to evaluate security policies and regulations. External audits, which are assessed by outside regulatory agencies or authorized certifying bodies, are conducted to examine compliance with cybersecurity regulations and standards such as HIPAA and ISO/IEC 27000. Vendor audits are administered by healthcare organizations to guarantee that the third-party vendor's security practices are compliant with cybersecurity regulations. Therefore, third-party access to the organization's data is protected and the systems are secured.

It is important to indicate the criticality of conducting cybersecurity awareness training for all employees in healthcare organizations. Employees trained in cybersecurity are more aware of their obligations and responsibilities under the organization's security policies. Thus, the employees are more inclined to adhere to the proper security etiquette. Cybersecurity awareness training for healthcare staff is essential to comply with regulations, reduce security risk, prevent data breaches, and maintain a sustainable reputation.

Correlating to cybersecurity training for employees, health organizations should provide patients with detailed guidelines to safeguard their personal information and maintain private security when using healthcare services. Organizations should indicate to their patients some of the best security practices such as recognizing potential phishing attacks (emails, text messages, and phone calls), maintaining security patches on their technological devices, utilizing the most recent antivirus software, and creating strong passwords (including special characters, numbers, and uppercase letters). Health organizations should ensure that secured communication channels are utilized by their patients and providers through encrypted emails and patient portals. Applying these strategies will allow healthcare organizations to adequately maintain compliance protocols and regulations to ensure effective data privacy. United States' healthcare organizations must hold firm in achieving compliance with cybersecurity standards and regulations by addressing the various aspects of cybersecurity and data privacy.

Conclusion

The United States healthcare sector is inherently intricate as it includes an assortment of medical protocols and administrative capabilities. The healthcare industry strives to offer patient care, clinical services, and curative commodities. Nonetheless, in the realm of cybersecurity, the healthcare sector continues to mature as the rise in cyberattacks and data breaches have demonstrated an upward trend since the beginning of the COVID-19 Pandemic. According to The HIPAA Journal, the average rate of healthcare data breaches (of 500 or more records) doubled from the year 2018 (HIPAA Journal, 2022). The growing cybersecurity concerns for health organizations as it relates to patient data are concentrated on complying with US regulations and information security.

A compilation of cybersecurity frameworks and regulations was analyzed to identify distinct security enhancements and strategies that assist healthcare organizations in abiding by data privacy protocols. The literature review was carried out to discern two US regulations (HIPAA and HITECH), two international standards (ISO/IEC 27000 and PCI-DSS), and four cybersecurity frameworks (NIST CSF, MITRE ATT&CK, COBIT, and HITRUST CSF) in the healthcare sector. Concerning the paper methodology, the narrative review analyzed five significant themes: advantageous cybersecurity frameworks, corresponding implications in healthcare settings, a thorough comparison of frameworks and regulations, proposed mitigation strategies, and decisive cybersecurity enhancements.

In the results and discussion sections of the paper, the examination of RQ1 determined the specifications of the various frameworks in their scope, depth, focus, and level of relevance; concluding that HITRUST CSF is the leading framework in the healthcare industry. One proposed security enhancement (about RQ1) is the integration of HITRUST and NIST which can provide an effective cybersecurity framework for healthcare organizations. The analysis of RQ2 further identified critical strategies for organizations to attain compliance with cybersecurity regulations and standards in the United States healthcare system. The study will conclude with a brief discussion of the limitations and future work corresponding to cybersecurity frameworks and regulations in healthcare.

The scope of the study analyzed particular cybersecurity frameworks, regulations, and standards that are most applicable to the healthcare industry. Thus, one primary limitation is the narrow purview of the study. For future work, researchers can broaden the scope to analyze additional cybersecurity controls and standards as they relate to data privacy in healthcare. Another limitation classified is the minimal accessibility to relevant real-world cybersecurity context as this information is a secure proprietary to health organizations. There is a level of security that is only privy to the specific healthcare professionals in an organization. Moreover, this research study entails organizations only within the United States. Therefore, a proposed recommendation for future research can consider international cybersecurity practices and examine compliance with data privacy regulations worldwide. In conclusion, there are numerous future research channels correlated to cybersecurity frameworks and standards that can be applied to current emerging technologies in cybersecurity such as the Internet of Things (IoT), blockchain, cloud computing, and intelligent automation. As the United States healthcare system continues to evolve, health organizations must carry on implementing cybersecurity frameworks and regulations that enforce effective data privacy.

References

Alexander, O., Belisle, M., & Steele, J. (2020). *MITRE ATT&CK® for industrial control systems: Design and philosophy*. The MITRE Corporation. Retrieved October 24, 2022, from https://attack.mitre.org/docs/ATTACK_for_ICS_Philosophy_March_2020.pdf

Biden, J. (2021). *Executive Order 14028 on Improving the Nation's Cybersecurity. 12 May 2021*. The White House. Retrieved October 28, 2022 from https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Cabrera, E. (2017). HITRUST Addresses Cybersecurity Concerns for Smaller Health Care Providers with CyberAid. *Journal of Health Care Compliance*, *19*(1), 37–54.

California Legislative Information. (2017). *California Civil Code 56.10*. Retrieved October 22, 2022 from https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=56.10.&lawCode=CIV

Determann, L. (2020). Healthy Data Protection. *Michigan Telecommunications & Technology Law Review*, *26*(2), 229–278.

Federal Trade Commission (2022). *Standards for Safeguarding Customer Information*. Federal Register. Retrieved October 22, 2022 from https://www.federalregister.gov/documents/2021/12/09/2021-25736/standards-for-safeguarding-customer-information

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. *Sensors*, *21*(9), 3267. https://doi.org/10.3390/s21093267

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), 1–8. https://doi.org/10.1093/cybsec/tyaa005

He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. *Journal of Medical Internet Research*, *23*(4), e21747. https://doi.org/10.2196/21747

HIPAA Journal. (2021). *Healthcare Data Breach Statistics*. Retrieved November 8, 2022 from https://www.hipaajournal.com/healthcare-data-breach-statistics/

HITRUST Alliance. (2021). *Introduction to the HITRUST CSF, Version 9.6.0*. Retrieved December 18, 2022 from https://hitrustalliance.net/product-tool/hitrust-csf/

HITRUST Alliance. (2023). *Why HITRUST Certifications are Broadly Accepted and Considered the Gold Standard.* Retrieved February 25, 2023 from https://hitrustalliance.net/content/uploads/Why-the-HITRUST-Certification-is-So-Broadly-Accepted.pdf

Ibrahim, A., Valli, C., McAteer, I., & Chaudhry, J. (2018). A security review of local government using NIST CSF: a case study. *Journal of Supercomputing*, *74*(10), 5171–5186. https://doi.org/10.1007/s11227-018-2479-2

INTERPOL. (2020). *INTERPOL report shows alarming rate of cyberattacks during COVID-19. INTERPOL*. Retrieved October 20, 2022, from https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

International Organization for Standardization. (2013). *An Introduction to ISO 27001, ISO 27002....ISO 27008*. Retrieved October 30, 2022, from https://www.27000.org/iso-27002.htm

Iqbal H. Sarker, A. S. M. Kayes, Shahriar Badsha, Hamed Alqahtani, Paul Watters, & Alex Ng. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data, 7(1), 1–29. https://doi.org/10.1186/s40537-020-00318-5

ISACA. (2012). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Retrieved November 30, 2022 from https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoCDEA0

Jones, K. (2004). Mission Drift in Qualitative Research, or Moving Toward a Systematic Review of Qualitative Studies, Moving Back to a More Systematic Narrative Review. *Qualitative Report*, *9*(1), 95–112.

Kim, S. (2016). *A mobile device security implementation model for a national medical center complying with the HIPPA security rule*. Doctoral dissertation, Robert Morris University. ProQuest LLC. Retrieved October 28, 2022 from https://www.proquest.com/dissertations-theses/mobile-device-security-implementation-model/docview/1973156179/se-2?accountid=12418

Mabee, M. J. (2020). Healthcare Data Breaches in South Dakota: Postbreach Legislation Is Not Enough. *South Dakota Law Review*, *65*(3), 511–539.

Moore, P. Y. (2018). *Factors influencing the adoption of bring your own device policies in the united states healthcare industry*. Doctoral dissertation, Capella University. ProQuest LLC. Retrieved November 2, 2022 from https://www.proquest.com/dissertations-theses/factors-influencing-adoption-bring-your-own/docview/2170026324/se-2

National Security Agency/Central Security Service. (2022). *End User Telework and Network Security Guides*. Retrieved December 18, 2022, 2022 from https://www.nsa.gov/Press-Room/Telework-and-Mobile-Security-Guidance/#Telework%20and%20Network%20Security%20Guides

NIST. (2005). *Recommended Security Controls for Federal Information Systems*. Retrieved October 9, 2022 from https://www.nist.gov/publications/recommended-security-controls-federal-information-systems

Obama, B. (2013) *The White House, Presidential Executive Order 13636, Improving Critical Infrastructure Cybersecurity*. *12 February 2013*. The White House. Retrieved October 28, 2022 from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

Ramadan, R. A., Aboshosha, B. W., Alshudukhi, J. S., Alzahrani, A. J., El-Sayed, A., & Dessouky, M. M. (2021). Cybersecurity and Countermeasures at the Time of Pandemic. *Journal of Advanced Transportation*, 1–19. https://doi.org/10.1155/2021/6627264

Rowe K. (2016). Healthcare IT transformation: how has ransomware shifted the landscape of healthcare data security? *HealthcInform*, *33*(3): 44-45.

Shen, L. (2014). The NIST Cybersecurity Framework: Overview and Potential Impacts. *Journal of Internet Law*, *18*(6), 3–6.

Sloan, P. (2014). The Compliance Case for Information Governance. *Richmond Journal of Law & Technology*, *20*(2), 1–46.

Strom, B., Applebaum, A., Miller, D., Nickels, K., Pennington, A., & Thomas, C. (2020). *MITRE ATT&CK: Design and Philosophy*. The MITRE Corporation. Retrieved October 22, 2022 from https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics*, *11*(2181), 2181. https://doi.org/10.3390/electronics11142181

U.S. Centers for Medicare & Medicaid Services. (2021). *National Health Expenditure Data*. Retrieved October 5, 2022 from https://www.cms.gov/research-statistics-data-and-systems/statistics-trends-and-reports/nationalhealthexpenddata

U.S. Cybersecurity & Infrastructure Security Agency. (2020). *Executive Order 13800. Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. 11 May 2017*. Retrieved October 28, 2022 from https://www.cisa.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure

U.S. Cybersecurity & Infrastructure Security Agency. (2021). *Executive Order 14028. Improving the Nation's Cybersecurity. 12 May 2021*. Retrieved October 28, 2022 from https://www.cisa.gov/executive-order-improving-nations-cybersecurity

U.S. Cybersecurity & Infrastructure Security Agency. (2022). *Coronavirus: CISA information and updates on COVID-19*. Retrieved December 18, 2022, 2022 from https://www.cisa.gov/topics/risk-management/coronavirus

U.S. DHHS-OCR. (2015). *List of Breaches of Unsecured Protected Health Information Affecting 500 or More Individuals*. U.S. Department of Health and Human Services Office of Civil Rights. Retrieved October 27, 2022 from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

U.S. DHHS-OCR. (2016). *Addressing Gaps in Cybersecurity: OCR Releases Crosswalk Between HIPAA Security Rule and NIST Cybersecurity Framework*. Retrieved November 11, 2022 from https://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/index.html

U.S. DHHS-OCR. (2022). *Guidance on How the HIPAA Rules Permit Covered Health Care Providers and Health Plans to Use Remote Communication Technologies for Audio-Only Telehealth*. Retrieved February 20, 2023 from https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-audio-telehealth/index.html

Wang, G. (2019). Measuring Information Security and Cybersecurity on Private Cloud Computing. *Journal of Theoretical and Applied Information Technology*, *96*(1), 156–168