International Journal of Leading Research Publication (IJLRP)

E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

Cybersecurity Risk Assessment Framework for EHR Systems in Clinical Settings

Kranthi Kumar Asike Parameshwa

Indian Wesleyan University

Abstract:
The healthcare revolution has led to the tremendous usage of Electronic Health Record (EHR) systems that are required to guarantee an effective clinical practice, patient care coordination, and evidence-based decision-making. The greater adoption of EHR systems, nevertheless, has exposed healthcare organizations to many forms of cybersecurity attacks, including ransomware, phishing attacks, malware, insider attacks, and network attacks. This can compromise patient privacy, disrupt the operations of a hospital, and lead to a risk to patient safety, hence the need to have a well-organized strategy on how to counter the impact of cybersecurity threats in clinical facilities. The authors in this work provide a generalized system of cybersecurity risk assessment, which specifically targets EHR systems related to healthcare. The framework includes the identification of the threat, the analysis of the vulnerability, ranking risk associated with probability and impact, and recommendations of security control, where regular monitoring and incident response should be used. Scenario-based evaluation, systematic literature assessment, and expert validation enabled the framework to reveal its potential for realizing serious threats, prioritizing risks in a productive way, and providing actionable advice on mitigating such risks without disrupting the clinical processes. The specified framework addresses the principal drawbacks of the existing standards, such as NIST, ISO/IEC 27001, and OCTAVE, by offering a healthcare-centred strategy of aligning technical, organizational, and operational perspectives. The framework will enhance the security of sensitive patient data and be more resistant to evolving cyber threats since it will enable healthcare organizations to proactively assess and control cybersecurity risks.

Keywords: Cybersecurity, Electronic Health Records, Risk Assessment, Healthcare IT, Clinical Workflows, Threat Mitigation.

1. Introduction

1.1 Background

The Electronic Health Records (HER) systems enable better clinical decision-making, better coordination of care, and improvement in the overall quality and efficiency of healthcare services through the digitization of patient records. Clinical workflow, patient history management, and interoperability among healthcare providers are among the clinical areas that are increasingly relying on EHR platforms to support healthcare organizations (Reegu et al., 2023).

Regardless of the high advantages of EHR implementation, the accelerated process of cyber-informing healthcare has posed considerable cybersecurity threats. The sensitive medical data that is sometimes loaded with personal identification information, insurance data, and clinical history has made healthcare organizations an appealing target to cybercriminals because of the high price of this kind of data (Minnaar & Herbig, 2021a). Ransomware, phishing attacks, malware attacks, and hacking into systems have become very common in the healthcare setting (Neprash et al., 2022).

Breaches of cybersecurity in EHR systems can bring far-reaching outcomes besides monetary damage (Neprash et al., 2022). Access to patient information by unauthorized individuals may jeopardize the privacy and confidentiality of patients, which may be against regulations and ethical standards. In addition, operational disturbances due to cyberattacks may adversely affect clinical processes, slow down medical

treatment, and put patient lives at risk (Odedina, 2021a). As an illustration, a ransomware of a hospital system could deny access to important patient files, thus limiting the ability to make prompt clinical decisions. As a result, securing EHR systems against cybersecurity threats has turned out to be one of the most important concerns of healthcare facilities across the globe.

1.2 Problem Statement

Despite the fact that healthcare institutions have adopted numerous cybersecurity measures, most of the current EHR systems are yet to have comprehensive and systematic cybersecurity risk assessment mechanisms. Conventional information security strategies tend to be generalized on IT infrastructures, without sufficient consideration of the specific operational and regulatory aspects of a healthcare setting.
Clinical environments are characterized by intricate interactions between health care providers, physical and information technology. Such environments often demand quick access to patient data, potentially compromising security to become more susceptible to cyber-attacks. Moreover, medical institutions frequently use outdated systems, interlinked health equipment, and third-party software, which increases the attack area as well.
Lack of an organized and healthcare-focused system of cybersecurity risk assessment of the EHR systems complicates identification, assessment, and mitigation of the emerging threats by organizations. Consequently, health facilities can be exposed to cyber-attacks, which can interfere with medical services and patient information.

1.3 Research Gap

A number of cybersecurity frameworks and risk management models have been invented to assist in information security practices in different industries. The National Institute of Standards and Technology Cybersecurity Framework, ISO/IEC 27001, and the Health Insurance Portability and Accountability Act Security Rule are frameworks that can guide in the protection of digital assets and in dealing with information security risks. Although these frameworks provide useful principles of security, they are typically in the general context of the organization, but not the operational mechanisms of the clinical healthcare system. Current research in the field of cybersecurity in healthcare usually considers a particular threat or security technology instead of offering a risk assessment model specific to EHRs. In addition to that, most conventional models focus on technical security controls and give little attention to incorporating cybersecurity practices into clinical practices and healthcare operations procedures.
The inadequate attention to human and organizational aspects of cybersecurity risks is also another constraint. Healthcare environments are associated with different stakeholders, such as physicians, nurses, administrators, and IT personnel, and all of whom respond to EHR systems in various ways. The inability to account for such factors in the risk assessment models may result in incomplete security strategies. Hence, the necessity to develop a detailed framework of cybersecurity risk assessment related to EHR systems that work in clinical environments is evident.

1.4 Research Objectives

This research study is aimed at creating a structured framework of cybersecurity risk assessment to be used on Electronic Health Record systems within the clinical setting. To attain this, the following specific objectives are followed in the study:

- To detect and discuss key cybersecurity risks to EHR systems in healthcare organizations.
- To analyze gaps that exist in clinical settings and that can put EHR systems at risk of cyber-attacks.
- To create an extensive cybersecurity risk assessment framework specifically in relation to EHR systems applied in clinical settings.
- To assess and confirm the usefulness of the suggested framework in facilitating healthcare cybersecurity risk management.

1.5 Research Questions

The proposed research will be used to develop a risk assessment model of cybersecurity that will be deployed to evaluate the risks in Electronic Health Records in a clinical environment. The goals that the study will follow to achieve this goal will include:

RQ1: What are the major cybersecurity threats and risks of Electronic Health Record systems in clinical settings?

RQ2: What can be done to enhance the detection and mitigation of cybersecurity threats within EHR systems through the adoption of a formal risk assessment model?

RQ3: What mitigation strategies and security controls are most effective in protecting EHR systems within healthcare organizations?

1.6 Contributions of the Study

This study has a number of significant implications for the area of healthcare cybersecurity and health information systems.

First, the research will present an extended model of cybersecurity risk evaluation that would apply specifically to Electronic Health Records systems in clinical settings. The proposed model takes into consideration some healthcare-specific operational and security needs, unlike the general IT security frameworks.

Second, the study presents a combined framework that includes a technical, human, and organizational perspective of cybersecurity risk management. The framework offers a comprehensive solution to the security of EHR systems by focusing on several areas of vulnerability in the healthcare system.

Lastly, the research will provide viable recommendations to healthcare facilities, hospital managers, and cyber experts aiming to enhance the security of the information and communication of patients and enhance the resilience of the healthcare system against cyber-attacks. The offered framework can help healthcare organizations to identify the weaknesses in a systematic way, prioritize threats to cybersecurity, and take the necessary steps to protect the sensitive medical information.

2. Literature Review

2.1 Electronic Health Record Systems.

Electronic Health Records (EHR) systems are now a staple of the current healthcare information management system because they allow healthcare providers to store, retrieve, and even share patient information in electronic format. These systems combine clinical, administrative, and financial data to aid in efficient healthcare provisions and advanced patient outcomes (Alshararl et al., 2025). EHRs enable providers to retrieve the history of patients, diagnostic reports, medications, and treatment plans instantly, which enables the coordination of care among various healthcare providers (Adeniyi et al., 2024).

2.1.1 Architecture of EHR Systems

EHR systems' architecture is usually characterized by several interrelated units meant to handle and trade patient information effectively (Soman et al., 2020). Some of the key architecture components are clinical data storage, interoperability engines, user interfaces, and analytics modules. The clinical data repository is used as the central repository of patient data such as lab results, medical history, prescriptions, and imaging data. Interoperability mechanisms enable the EHR systems to share information with the rest of the healthcare systems through standardized protocols like HL7 and FHIR.

The modern EHR architectures also facilitate distributed and service-based designs that facilitate scalability, integration of data, and interoperability of healthcare organizations (Casanova et al., 2025). Besides this, standardized models like openEHR also offer information models and service interfaces to ensure the consistent representation and management of health data across systems (Gamal et al., 2021). These architectural structures help in the development of interoperable health information structures and provide data sharing between healthcare institutions (Adel et al., 2022).

2.1.2 Participation in Clinical Decision Making.

EHR systems are vital in assisting in clinical decision-making (Linhares et al., 2022). EHR solutions allow clinicians to receive evidence-based recommendations, alerts, and diagnostic suggestions by combining data about patients with clinical decision support systems (CDSS) when working with patients. CDSSs are generally composed of a knowledge base, inference engine, and user interface that takes patient-specific data to produce clinical knowledge and advice (Gupta et al., 2020).

By combining the EHR data with the decision support tools, clinicians can discover possible medication interactions, track the patient's conditions, and enhance the accuracy of treatment (Sutton et al., 2020). Therefore, EHR systems help to increase patient safety, decrease medical errors, and improve clinical outcomes. The growing use of digital healthcare systems has consequently rendered EHR security and reliability essential in ensuring successful healthcare delivery.

2.2 Cybersecurity in Healthcare

The digitalization of healthcare systems has greatly exposed healthcare organizations to cybersecurity threats (Lehto et al., 2022). Hospitals, clinics, and healthcare providers deal with vast amounts of sensitive patient data, and thus, they are a good target for cybercriminals. Health information usually includes personal identification data, medical records, and insurance information, which may be used to commit identity theft, fraud, or to sell or trade it illegally.

2.2.1 Rising Attacks on Hospitals

In the last ten years, the number of cyberattacks on healthcare institutions aimed at health information systems has been growing at an alarming pace (Odedina, 2021b). Authorized access to information on patients is another aspect that is mostly used by attackers to enter patient information with the help of network infrastructures, medical devices, and health information systems vulnerabilities (Abdullahi Yari et al., 2021). The increased interconnectedness between EHR systems and medical devices, as well as third-party healthcare platforms, has further increased the areas of attack.

Health care organizations face the risk of critical operational disruptions caused by cybersecurity attacks in their systems (Okafor et al., 2023). When hospitals suffer cyber-attacks, in most instances, they are forced to close down their information systems, put off medical procedures, or revert to manual systems of documentation. These interruptions may have adverse impacts on clinical processes and undermine the continuity of care.

2.2.2 Ransomware Incidents

One of the most important cybersecurity threats to healthcare organizations is ransomware attacks (Triplett, 2022). In such attacks, the malicious software encrypts vital data or systems, and the staff members in the healthcare facility are not able to access the records of patients until they pay a ransom. Since medical professionals depend greatly on access to patient data in real-time, ransomware attacks may have a devastating effect on the functioning of a hospital and patient safety (van Boven et al., 2024).

The recent ransomware attacks on hospitals across the world have shown how healthcare systems are susceptible to cyberattacks (Minnaar & Herbig, 2021b). Such attacks frequently have vulnerabilities in poor authentication systems, old software, and low network security policies (Aslan et al., 2023). As a result, healthcare organizations are becoming more aware of the necessity to have a more robust cybersecurity structure and risk management approach.

2.3 EHR Security Vulnerabilities

However, in spite of their advantages, EHR systems have a number of security threats because of the complexity of healthcare infrastructures (Ganiga et al., 2020). The combination of various systems, devices, and users provides a great number of possible points of cyber threat.

2.3.1 Unauthorized Access

Breach of EHR systems is among the most widespread cybersecurity risks in a healthcare setting. Hackers can use the compromised credentials or vulnerabilities of the system to gain access to sensitive patient

data (Chacko & Hayajneh, 2022). Hacking can also be done through the misuse of system privileges by healthcare employees or through their negligence to observe appropriate security measures.

2.3.2 Weak Authentication

Poor authentication protocols, including basic passwords or a lack of adequate access control protocols, may increase the probability of cybersecurity attacks considerably. Most of the healthcare systems are based on outdated authentication systems that do not support multi-factor authentication or any other strong identity management system, and, as such, they are prone to credential-based attacks.

2.3.3 Insider Threats

Another significant weakness in the healthcare information systems is insider threats. Patient data may be disclosed by healthcare staff who can gain legitimate access to the EHR systems either intentionally or unintentionally. The threats of insiders can be associated with the intent to harm the system, human factors, or a lack of awareness about security among healthcare workers.

2.3.4 Network Vulnerabilities

Interconnected systems that may be part of healthcare networks include EHR platforms, medical devices, laboratory information systems, and external healthcare databases (Singh, 2024). Poor network security infrastructures, software that is not up to date with the latest versions, or systems that are not patched may offer avenues to the attackers to crack into the healthcare networks and steal confidential information.

2.3.5 Data Leakage

Data leakage may be experienced when patient data are not stored, transmitted, and accessed in a proper way (Wang et al., 2024). Poorly set up cloud service, insecure communication systems, or inappropriate data sharing regulations can make sensitive health records vulnerable to unauthorized users. These cases can attract regulatory violations and the invasion of the privacy of patients.

2.4 Existing Cybersecurity Risk Frameworks.

A number of cybersecurity frameworks have been created to assist organizations in detecting and dealing with security risks. These models introduce the guidelines for the implementation of security controls, vulnerability evaluation, and the protection of digital properties.

The National Institute of Standards and Technology Cybersecurity Framework is one of the frameworks widely used and offers a systematic framework in addressing the risk of cybersecurity using 5 core functions to identify, protect, detect, respond, and recover (Syafrizal et al., 2020). The next important standard on the international level is the ISO/IEC 27001, which provides the terms of the establishment, implementation, maintenance, and constant improvement of the information security management system (Mirtsch et al., 2020). These standards focus on risk management, security policies and continuous assessment of information security controls.

Regulatory bodies, including the Health Insurance Portability and Accountability Act Security Rule, in the healthcare industry provide guidelines on how sensitive patient information can be safeguarded (Subramanian et al., 2024). The HIPAA security rule mandates healthcare facilities to adopt administrative, physical, and technical security measures that will guarantee the privacy, integrity, and accessibility of electronic health records (Szalados, 2021). Also, very useful is the framework of Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), which is a well-organized risk evaluation system that assists companies in defining critical assets, assessing vulnerabilities, and creating mitigation of the risks.

2.5 Limitations of Existing Frameworks

Even though these frameworks offer important cybersecurity advice, they contain a number of limitations when implemented in EHR systems in clinical settings.

To begin with, most of the current frameworks of cybersecurity are developed to accommodate generic IT systems and not systems with specifics to healthcare. Consequently, they might fail to appropriately

respond to the operational issues of healthcare settings where healthcare providers need to have access to patient information quickly. Second, existing frameworks are, in many cases, not detailed threat models specific to EHR systems. The information systems in healthcare are associated with particular vulnerabilities of medical equipment, management of patient data, and clinical processes that are not covered by the overall cybersecurity models.

Third, numerous frameworks are related more to organizational security policies and technical controls and offer little information on how cybersecurity practices can be embedded in real-time clinical workflows. Security in a healthcare setting involves striking a balance between high protection and the imperative to access patient information as per the requirements. As indicated in Table X, the differences between the current cybersecurity structures and the proposed structure formulated in this research are as follows. Although popular general security governance and risk management standards, including the NIST Cybersecurity Framework and ISO/IEC 27001, do offer good overall standards, they have not been particularly adapted to the nature of the operations in clinical settings. Likewise, the OCTAVE model mainly emphasizes the analysis of risk with the help of assets, yet it offers minimal assistance in terms of constant monitoring of the healthcare system. Conversely, the stipulated framework combines healthcare-specific risk considerations connected to Electronic Health Records systems, integrating the threat detection, vulnerability assessment, risk rating, and continuous monitoring to assist cybersecurity management in clinical facilities.

Table 1: Comparison of Existing Cybersecurity Risk Frameworks and the Proposed Framework for EHR Systems

Framework	Strength	Limitation
NIST	Strong risk management	Not healthcare specific
ISO/IEC 27001	Security governance	Limited clinical focus
OCTAVE	Asset-based risk assessment	Limited continuous monitoring
Proposed Framework	Healthcare-specific risk analysis	Requires real-world validation

3. Methodology

3.1 Research Design

The proposed research design used in this study is a qualitative research design with a systematic literature review and conceptual framework development to design a framework of cybersecurity risk assessment in Electronic Health Records (EHR) in the clinical setting. This methodological approach aims at identifying key cybersecurity threats, vulnerabilities existing within the healthcare information systems, and generating a systematic framework that helps healthcare organizations to measure and reduce the risk of cybersecurity threats.

The qualitative approach is suitable since cybersecurity in healthcare consists of multifaceted relationships between technical infrastructure, human behaviour, and organizational policies. The interrelated aspects cannot be entirely encompassed in terms of mere quantitative techniques. Qualitative analysis, therefore, will provide the possibility to understand the issues of cybersecurity in clinical settings better.

There are four key steps to the research process, including literature review, risk identification, framework development, and validation. The first step of the research involved a methodological review of the extant literature on the topic of healthcare cybersecurity, EHR security threats, and risk management frameworks to determine common threats and mitigation measures. According to the results, a systematic identification of risks was carried out to assess the cybersecurity risks in EHR systems. Lastly, the development and refinement of a conceptual framework of cybersecurity risk assessment was done through expert validation and scenario-based evaluation.

Figure 1: The Workflow of the Cybersecurity Risk Assessment Framework of EHR Systems Methodology.

3.2 Data Sources

To cover extensively on the academic literature that was of interest, various high-quality scholarly databases were identified through which academic literature could be obtained in cybersecurity and healthcare informatics research. The main databases that will be used in this study are:

- IEEE Xplore Digital Library
- Scopus (Elsevier)
- PubMed (National Library of Medicine)
- Web of Science (Clarivate Analytics).
- Google Scholar

These databases have been chosen as they allow access to peer-reviewed journal articles, conference papers, and technical reports on the field of cybersecurity, healthcare information systems, and Electronic Health Record security.

Multiple databases would decrease the publication bias and maximize the coverage of relevant studies. Keywords that were used in the search included:

- "EHR cybersecurity"
- "healthcare cyber threats"
- "security of electronic health record"
- “risk assessment in healthcare IT”.
- "Clinical Information System Security"

Table 2: The Academic Databases to be used in the collection of the literature.

Database	Purpose
IEEE Xplore Digital Library	Access to high-quality publications on engineering, IT, and cybersecurity in healthcare.
Elsevier Scopus	Comprehensive coverage of peer-reviewed journal articles and conference papers in healthcare informatics and cybersecurity.
PubMed (National Library of Medicine)	Focused on biomedical and health-related literature, including EHR security research.
Clarivate Web of Science	Multidisciplinary database to ensure high-quality, peer-reviewed literature and reduce publication bias.
Google Scholar	Broad search of scholarly articles, including technical reports, theses, and conference papers relevant to healthcare cybersecurity.

3.3 Study Selection Criteria

Including and excluding criteria were used to select the study, as the relevant and quality literature is needed to guarantee the excellence and quality of the reviewed literature.

3.3.1 Inclusion Criteria

The studies that were incorporated in the analysis satisfied the following criteria:

- Cybersecurity research in healthcare information systems.
- Research regarding Electronic Health Record (EHR) security, in particular.
- Studies suggesting or testing cybersecurity risk evaluation models or frameworks.
- The peer-reviewed journal articles or conference papers.
- Articles in the English language.

3.3.2 Exclusion Criteria

The studies were not included in case they satisfied any of the following conditions:

- Articles that are not related to healthcare cybersecurity.
- The studies that only discuss general IT security in the absence of healthcare.
- The same publications in more than one database.
- Non-peer-reviewed articles or posts (editorials, opinion articles, blogs, etc.).

To select the study, a systematic screening process was used in order to make the selection of relevant publications. Identification, screening, and selection involve the following process, as shown in Figure 2.

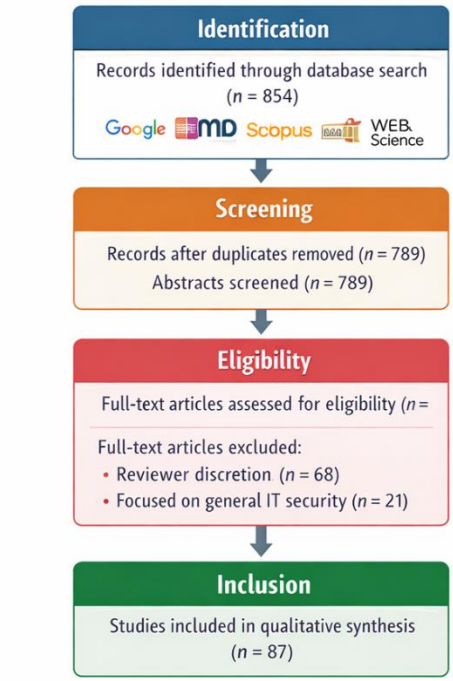

Figure 2: Process of the Study selection based on literature screening.

3.4 Process of Risk Identification of Cybersecurity.

A very imperative part of cybersecurity risk management is risk identification. In this paper, the comprehensive risk identification protocol was applied to reveal the significant threats and vulnerabilities of EHR systems in clinical settings.

The risk identification process involves four major steps, and these include threat identification, vulnerability analysis, likelihood assessment, and impact assessment.

3.4.1 Threat Identification

The initial phase is the recognition of possible cybersecurity risks to EHR systems. The literature analysis

and cybersecurity incidents were used to identify these threats. Common threats include:

- ransomware attacks
- malware infections
- phishing attacks
- insider threats
- unauthorized system access
- network intrusions

The knowledge of these threats will assist healthcare organizations in preparing in advance against potential attack vectors and reinforce its cybersecurity barriers.

3.4.2 Vulnerability Analysis

After identifying threats, it is followed by the analysis of the vulnerabilities that can enable the attackers to exploit EHR systems. Vulnerabilities can be caused by:

- Poor authentication schemes.
- obsolete software or software that has not been updated.
- badly set up access control systems.
- vulgar network setups.
- weak third-party integrations.

By spotting such vulnerabilities, healthcare organizations can have a clue on which areas their systems are at the highest risk of cyber-attacks.

3.4.3 Likelihood Assessment

Likelihood assessment is used to estimate the likelihood of the occurrence of a cybersecurity incident. The probability of the occurrence of each threat was considered using many factors, among them:

- frequency of such cyberattacks in the past in the healthcare industry.
- degree of task vulnerability to external networks.
- The difficulty of medical information technology infrastructure.
- presence or absence of security controls in place.

3.4.4 Impact Assessment

Impact assessment determines the possible effects of cybersecurity attacks on healthcare activities. Possible impacts include:

- disclosure of delicate patient data.
- impediment of clinical workflows.
- health care organizational losses.
- legal and regulatory fines.
- risks to patient safety

The evaluation of likelihood and impact will enable healthcare organizations to identify the general magnitude of cybersecurity risks.

3.5 Framework Development

According to the results of the literature survey and the risk identification process, a risk assessment framework specifically designed to identify EHR systems risks in clinical settings was elaborated.

The suggested framework combines the accepted cybersecurity risk management principles and the operational needs of the healthcare systems. The model is composed of the five stages that are interlocked:

1 **Threat Identification -** determining possible cyber threats to EHR systems.

2 **Vulnerability Analysis -** determining the weaknesses of a system that are likely to expose the EHR infrastructures to attacks.

3 **Risk Scoring Model -** the probability and impact of risk should be calculated to determine the severity of the risk.

4 **Risk Minimization Plans -** proposing technical and organizational measures of security to

minimize cybersecurity threats.

5 **Continuous Monitoring and Incident Response** - providing extended protection through constant surveillance and fast reaction systems.

These phases offer a systematic way through which healthcare organizations can identify, assess, and minimize cybersecurity threats to EHR infrastructures in a systematic manner.

Figure 3: EHR System in Clinical Settings proposes a Cybersecurity Risk Assessment Framework.

4 Cybersecurity Risk Assessment Framework Proposal

This paper presents a framework of cybersecurity risk assessment of Electronic Health Record (EHR) systems in clinical practice, unique to Electronic Health Records (EHR). This framework allows combining threat identification with vulnerability assessment, risk scoring, mitigation strategies, and continuous monitoring, which is a well-organized way of managing the risks in healthcare information systems related to cybersecurity. As much as it is based on the recognized standards like the NIST Cybersecurity Framework, the ISO/IEC 27001, and healthcare regulations like the HIPAA Security Rule, it is customized to the operational and security needs of a clinical setting.

4.1 Framework Architecture

The framework comprises five components that are interrelated and represented in Figure 4. It starts by identifying a threat section, whereby the intelligence on threats, historical attacks, and security reports is collected to detect possible cyber threats both outside and inside the healthcare entity. The vulnerability assessment is then conducted in order to identify the vulnerabilities of the software, network settings, authentication, and system integrations that may be used by the attackers. The identified risks are then quantified in a likelihood and impact scoring model by the risk analysis engine, and the most important cybersecurity issues can thus be prioritized. On the basis of the analysis, the security control recommendations are offered, including technical, administrative, and awareness-based solutions to diminish the identified risks. Lastly, incident response and monitoring are essential in the long-term protection by providing continuous monitoring, intrusion detection, and fast response to security incidents in cyberspace.

Figure 4: EHR Systems Proposed Cybersecurity Risk Assessment Framework.

4.2 Threats and Vulnerabilities.

The health IT infrastructures are very susceptible because of the sensitivity of the medical-related information and the dependence on EHR systems (Ddamba et al., 2025). The main threats are malware, which undermines the integrity of the system or network access, ransomware, which encrypts an important part of patient data and disrupts the work of a health organization, insider threats, which occur due to the misuse of authorized access, phishing, and unauthorized network intrusions. Simultaneously, EHR systems can contain internal vulnerabilities, including weak/easy passwords, unpatched/outdated software, misconfigured access control systems, insecure APIs, and third-party integration risks. The framework also tackles these risks and vulnerabilities holistically, connecting a weakness that has been identified with the possible ways of mitigating it.

4.3 Risk Assessment and Prioritization.

In order to aid decision-making, the framework includes a risk matrix that categorizes cybersecurity threats based on their probability of happening and the possible effects. The risks are of low level, where the incidents are infrequent with insignificant effects, and critical, where incidents are nearly inevitable and have disastrous outcomes in terms of patient safety, data integrity, and healthcare operations.

4.4 Controls and Mitigations of Security.

The framework suggests the actions of improving the EHR security depending on the findings of the risk assessment. Multi-factor authentication limits access policies, and the encryption of data protects sensitive patient information during transmission and at rest. The networks can be segmented to reduce the potential localization of intrusion; intrusion detection systems provide timely hateful action. Furthermore, the security training will equip the medical personnel with the tools to recognize phishing as well as seek safe data management practices. A combination of all these controls will produce a strong cybersecurity position that involves both technical and operational elements and human factors within the clinical environment.

5 Results

The presented section presents the outcomes of the process of assessing the risk of cybersecurity and the discussion of the developed structure of the Electronic Health Record (EHR) systems in the field of clinical facilities. The results are the identified cybersecurity threats, risk prioritization, and framework review performed with the help of scenario analysis and expert authentication.

5.1 Cybersecurity Threats Identified.

The review of the literature and cybersecurity incidents showed systematically that there are several critical threats to EHR systems. These risks are external and internal attacks on the system. Table 3 gives a summary of the most prevalent cybersecurity threats that were identified in the process of conducting the study.

Table 3: Major Cybersecurity Threats Affecting EHR Systems in Clinical Settings

Threat Category	Description	Potential Impact
Malware Attacks	Malicious software designed to infiltrate systems and steal or damage data	Data corruption and unauthorized system access
Ransomware	Encryption of hospital systems and patient records is demanding ransom	Disruption of clinical operations
Phishing Attacks	Fraudulent communications targeting healthcare staff	Credential theft and system compromise
Insider Threats	Misuse of system access by authorized personnel	Data leakage and privacy violations
Network Intrusion	Unauthorized access through network vulnerabilities	Compromise of EHR databases
Data Breaches	Unauthorized exposure of patient health records	Violation of privacy regulations

Analysis shows that ransomware and phishing cases are some of the most reported threats in the list of cybersecurity threats in healthcare.

5.2 Risk Prioritization

The proposed risk assessment model was applied to prioritize the risk after the identification of cybersecurity threats, where the risk scores were calculated depending on the likelihood and impact scores.

Table 4: Risk Prioritization of Identified Cybersecurity Threats

Threat	Likelihood	Impact	Risk Score	Risk Level
Ransomware Attack	High	Severe	9	Critical
Phishing Attack	High	Moderate	8	High
Insider Threat	Medium	Severe	7	High
Malware Infection	Medium	Moderate	6	Medium
Network Intrusion	Medium	Severe	7	High
Data Leakage	Low	Severe	5	Medium

The findings of the risk prioritization indicate that ransomware attacks are the most critical problem to healthcare systems because of their high probability and dire effects on operations. Such risks as phishing attacks and insider threats are also critical since they may cause unauthorized access to the system and sensitive patient data.

5.2.1 Framework Evaluation

The proposed cybersecurity risk assessment framework was tested on a case-by-case basis based on the scenario and expert validation. These were the assessment methods that were used to gauge the efficiency of the framework to identify cybersecurity threats and contribute to the risk mitigation measures.

Case Study Analysis: A simulated case within the clinical setting was developed to examine the ways the framework will help overcome cybersecurity threats to EHR systems. Such threats as phishing attacks on

hospital employees and ransomware attacks on EHR servers were widespread in the scenario.
It was discovered that the framework was effective in determining the key weaknesses that pertain to these threats and the development of relevant risk scores that would allow healthcare administrators to focus on mitigation efforts.

5.2.2 Expert Validation

The cybersecurity staff and healthcare IT specialists were engaged to test the viability and applicability of the proposed framework. The experts reconsidered the framework architecture, security control recommendations, and risk assessment model.
The answers provided by the professionals demonstrated that the framework is supportive in providing a systematic and holistic approach to address the issue of cybersecurity risks in clinical practice. The professionals also emphasized the necessity of including continuous detection and response to incidents in healthcare cybersecurity plans.

5.2.3 Scenario Analysis

The framework performance under different scenarios of cyberattacks was also undertaken through further scenario analysis. The framework may be able to detect threats of high risk and propose an appropriate security solution, particularly in the scenario of ransomware attacks and network intrusion incidents.

5.3 Framework Performance.

The results are that the proposed cybersecurity risk assessment model improves the overall cybersecurity of EHR systems in a number of ways.
First of all, the framework enhances the identification of threats by classifying cybersecurity threats and vulnerabilities to healthcare systems systematically. This standard approach helps health systems to be more informed of the extent of the threat to their EHR infrastructure.
Second, the framework improves prioritization of risks as it is based on a quantitative risk scoring model considering the probability and potential impact of risk. This will help healthcare administrators allocate the cybersecurity resources more efficiently and initially reduce the threat of severe ones.
Third, the framework improves the security of the clinical data by proposing security practices that comprise multi-factor authentication, network segmentation, and intrusion detection systems. These alternatives reduce to the barest minimum the risks of intrusion of privacy and breach of personal data.

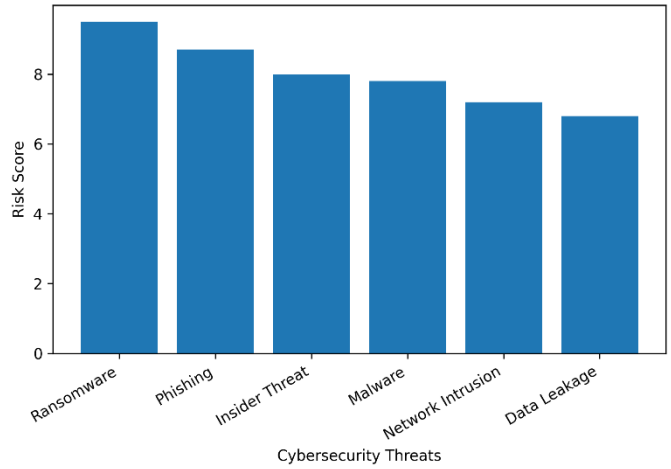

Figure 5: Risk Prioritization of EHR System Cybersecurity Threats.

This figure gives a graphical illustration of the threats that pose the highest risks in the healthcare environment as far as cybersecurity risks are concerned.

6 Discussion

This section changes the findings of the research, puts them into the framework of the existing literature, and discusses the implications for the practice, limitations, and future research perspectives.

6.1 Key Findings

The researchers discovered that Electronic Health Records (EHR) systems were susceptible to several severe attacks, which include ineffective authentication procedures, unprotected software, poor access control settings, insecure API, and third-party integration threats. Ransomware, phishing, insider assaults, malware infections, and network intrusions were discovered to pose a high risk to clinical operations and the privacy of patient information. The proposed cybersecurity risk assessment model worked well in addressing these weaknesses since it provided a well-rounded approach in the identification of threats, vulnerability assessment, risk rating, and formulating a mitigation strategy. The scenario analyses and confirmation by experts revealed that the framework is capable of effectively and systematically identifying and categorizing threats, measuring them against their likelihood and severity, prioritizing the major threats to be managed initially, and suggesting security measures that will not affect clinical operations. Overall, the framework has helped identify and successfully address cybersecurity threats in the clinical facilities, which has led to resilience against cyberattacks and enhanced the safety of the sensitive patient information.

6.2 Comparison to Existing Frameworks.

The proposed framework proves to have unique benefits to healthcare settings when compared with the popular models and standards of cybersecurity, including the NIST Cybersecurity Framework, ISO/IEC 27001, and the OCTAVE Risk Assessment model. Although the NIST framework offers a very broad framework on how to manage cybersecurity in general IT settings, it does not address the special needs of clinical workflows, nor is it relevant to the unique threats that EHR systems face. Likewise, the ISO/IEC 27001 focuses on managing information security of the organization, yet it does not specify threat models and does not offer guidance on the ability to enter the sphere of security management in clinical operations. OCTAVE methodology provides a framework for conducting risk assessment based on assets but fails to operationalize risk mitigation strategies with reference to EHR systems, as well as lacks continuous monitoring systems within clinical settings. Conversely, the given framework is directly adapted to EHR systems and includes a quantitative risk scoring scheme according to which the threats are ranked according to their probability and impact. It also incorporates practical security measures, operationalizes constant monitoring, and considers human, technical, and organizational aspects, hence sealing the loopholes that the available frameworks leave behind.

6.3 Practical Implications

The proposed framework can have a considerable influence on healthcare institutions. In hospitals, it provides a structured and limited method of identifying cybersecurity threats, determining priorities in mitigation strategies, and creatively allocating funds to the protection of important EHR systems. The framework can also be used by healthcare IT departments to establish both administrative and technical security controls that diminish vulnerability and mitigate breaches. The framework can also provide useful advice to policymakers and regulators since it provides evidence-based means of improving healthcare cybersecurity and adhering to data protection rules. The framework being developed by incorporating clinical workflow factors will ensure that the cybersecurity provisions do not interfere with the provision of patient care in a timely manner without jeopardizing the security of sensitive health information. Its wholesome nature enables healthcare institutions to strike a balance between operational effectiveness and security, which is indispensable in the contemporary, digital-intensive clinical settings.

6.4 Limitations

Although the study has its contributions, it has a number of limitations. The framework was mainly tested on simulated cases and on the basis of experts, as opposed to real-life multi-institutional datasets, which can limit the applicability of the results. The heterogeneity of the healthcare structures and regulation systems present in the hospitals may affect the applicability of the framework in practice, and its functioning within various organizational settings is yet to be experimented upon. Moreover, cybersecurity threats are dynamic, and this factor could mean that the framework is going to require a periodic update to accommodate new attack vectors, including new ransomware, malware, and insider threats. These shortcomings highlight the need to offer additional empirical support and revision so that it can be scaled and useful in other types of clinical scenarios.

6.5 Future Work

To enhance the proposed framework in the future, it is possible to consider more advanced technologies, such as artificial intelligence, that will help to monitor threats in real-time and forecast cybersecurity analytics. It is also possible to improve the security of EHR with solutions based on blockchain to ensure data integrity, uncompromised sharing, and audit trail traceability. One can utilize a response to the risks that could occur in real-time by developing automated real-time monitoring systems and incident response to enhance proactive risk management so that healthcare organizations can respond promptly to threats when they occur. Besides, the framework will be tested on different hospitals and clinical settings, which will bring light to its scalability, adaptability, and effectiveness. These innovations of the future will see healthcare organizations resistant to the ever-changing environment of cybersecurity threats, as well as protecting patient data and the continuity of clinical business.

7 Conclusion

The use of Electronic Health Record (EHR) systems is a matter of critical concern in terms of cybersecurity in the modern healthcare organization, as the systems store sensitive information about patients and help to conduct essential clinical activities. The growing number and complexity of cyberattacks, i.e., ransomware, phishing, insider threats, and network intrusions, have demonstrated the critical weaknesses in the EHR systems, i.e., weak authentication systems, unpatched software, incorrectly set access controls, unsecure APIs, and the third-party integration inherent dangers. These threats not only affect patient privacy and the integrity of data but also cause disruptions to the operations of a hospital and may compromise the safety of a patient.

This paper has solved these problems by conducting a thorough analysis of a cybersecurity risk assessment model specific to EHRs in the clinical setting. The framework is a systematic approach to identifying possible threats, vulnerability analysis, quantifying risks via a likelihood-impact model, and recommending security controls that can be implemented. The framework proved to be effective as it prioritizes the most critical risks, improves threat identification, and helps to implement preventative measures without disrupting the work of clinics.

The suggested framework can be used by hospitals, healthcare IT teams, and policymakers to reinforce cybersecurity in healthcare facilities. Incorporating the technical, human, and organizational factors, it allows healthcare organizations to become proactive in detecting, evaluating, and preventing cybersecurity threats. The suggested framework offers a systematic methodology of detecting, evaluating, and managing cybersecurity threats in EHR systems in a clinical setting, thereby enabling health services provision in safer and more resilient ways.

REFERENCES:

1. Abdullahi Yari, I., Dehling, T., Kluge, F., Geck, J., Sunyaev, A., & Eskofier, B. (2021). Security engineering of patient-centred health care information systems in peer-to-peer environments: Systematic review. *Journal of Medical Internet Research*, *23*(11), e24460.

2. Adel, E., El-Sappagh, S., Barakat, S., Kwak, K. S., & Elmogy, M. (2022). Semantic architecture for interoperability in distributed healthcare systems. *IEEE Access*, *10*, 126161–126179.
3. Adeniyi, A. O., Arowoogun, J. O., Chidi, R., Okolo, C. A., & Babawarun, O. (2024). The impact of electronic health records on patient care and outcomes: A comprehensive review. *World Journal of Advanced Research and Reviews*, *21*(2), 1446–1455.
4. Alsharari, F. A., Alsharari, L. H., Alsharari, A. S., Alsharari, M. F. H., Alsharari, M. S. M., Alsudays, A. S., Almughamis, F. K. S., & Alsharari, S. F. (2025). Integrating Health Information Systems and Administrative Processes to Improve Patient Care Efficiency: A Comprehensive Review. *Vascular and Endovascular Review*, *8*(5s), 112–120.
5. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cybersecurity vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.
6. Casanova, R., Villa-Garzon, F. A., & Branch-Bedoya, J. W. (2025). Architectural patterns for health information systems: A systematic review. *Frontiers in Digital Health*, *7*, 1694839.
7. Chacko, A., & Hayajneh, T. (2022). Security and privacy issues with IoT in healthcare. *EAI Endorsed Transactions on Pervasive Health and Technology*, *4*(14), e2.
8. Ddamba, A., Nsubuga, B., Kamabare, M., Abaho, E., Alinda, K., Arinaitwe, D., Ampaire, P., & Akello, H. (2025). Factors influencing the availability and use of electronic medical records systems in public health facilities in Uganda: A cross-sectional assessment. *BMC Medical Informatics and Decision Making*, *25*(1), 372.
9. Gamal, A., Barakat, S., & Rezk, A. (2021). Standardized electronic health record data modeling and persistence: A comparative review. *Journal of Biomedical Informatics*, *114*, 103670.
10. Ganiga, R., Pai, R. M., & Sinha, R. K. (2020). Security framework for a cloud-based electronic health record (EHR) system. *International Journal of Electrical and Computer Engineering*, *10*(1), 455.
11. Gupta, P. K., Ramachandran, A. T., Keerthi, A. M., Dave, P. S., Giridhar, S., Kallapur, S. S., & Saikia, A. (2020). An overview of the clinical decision support system (CDSS) as a computational tool and its applications in public health. *Applications in Ubiquitous Computing*, 81–117.
12. Lehto, M., Neittaanmäki, P., Pöyhönen, J., & Hummelholm, A. (2022). Cybersecurity in healthcare systems. In *Cyber Security: Critical Infrastructure Protection* (pp. 183–215). Springer.
13. Linhares, C. D., Lima, D. M., Ponciano, J. R., Olivatto, M. M., Gutierrez, M. A., Poco, J., Traina, C., & Traina, A. J. (2022). Clinicalpath: A visualization tool to improve the evaluation of electronic health records in clinical decision-making. *IEEE Transactions on Visualization and Computer Graphics*, *29*(10), 4031–4046.
14. Minnaar, A., & Herbig, F. J. (2021a). Cyberattacks and the cybercrime threat of ransomware to hospitals and healthcare services during the COVID-19 pandemic. *Acta Criminologica: African Journal of Criminology & Victimology*, *34*(3), 155–185.
15. Minnaar, A., & Herbig, F. J. (2021b). Cyberattacks and the cybercrime threat of ransomware to hospitals and healthcare services during the COVID-19 pandemic. *Acta Criminologica: African Journal of Criminology & Victimology*, *34*(3), 155–185.
16. Mirtsch, M., Kinne, J., & Blind, K. (2020). Exploring the adoption of the international information security management system standard ISO/IEC 27001: A web mining-based analysis. *IEEE Transactions on Engineering Management*, *68*(1), 87–100.
17. Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z., & Nikpay, S. S. (2022). *Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021*. *3*(12), e224873.
18. Odedina, E. A. (2021a). The impact of cyberattacks on patient safety and healthcare infrastructure: A risk management perspective. *Int. J. Eng. Technol. Res. Manag*, *5*(9), 385–398.

19. Odedina, E. A. (2021b). The impact of cyberattacks on patient safety and healthcare infrastructure: A risk management perspective. *Int. J. Eng. Technol. Res. Manag*, *5*(9), 385–398.
20. Okafor, C. M., Kolade, A., Onunka, T., Daraojimba, C., Eyo-Udo, N. L., Onunka, O., & Omotosho, A. (2023). Mitigating cybersecurity risks in the US healthcare sector. *International Journal of Research and Scientific Innovation (IJRSI)*, *10*(9), 177–193.
21. Reegu, F. A., Abas, H., Gulzar, Y., Xin, Q., Alwan, A. A., Jabbari, A., Sonkamble, R. G., & Dziyauddin, R. A. (2023). A blockchain-based framework for interoperable electronic health records for an improved healthcare system. *Sustainability*, *15*(8), 6337.
22. Singh, J. (2024). Challenges with medical devices connected to the hospital network. *International Journal for Research in Applied Science & Engineering Technology*, *12*(VI).
23. Soman, S., Ranjan, P., & Srivastava, P. (2020). A distributed architecture for hospital management systems with synchronized EHR. *CSI Transactions on ICT*, *8*(3), 355–365.
24. Subramanian, H., Sengupta, A., & Xu, Y. (2024). Patient health record protection beyond the Health Insurance Portability and Accountability Act: Mixed methods study. *Journal of Medical Internet Research*, *26*, e59674.
25. Sutton, R. T., Pincock, D., Baumgart, D. C., Sadowski, D. C., Fedorak, R. N., & Kroeker, K. I. (2020). An overview of clinical decision support systems: Benefits, risks, and strategies for success. *NPJ Digital Medicine*, *3*(1), 17.
26. Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security*, *12*(3), 417–432.
27. Szalados, J. E. (2021). Medical records and confidentiality: Evolving liability issues inherent in the electronic health record, HIPAA, and cybersecurity. In *The medical-legal aspects of acute care medicine: A resource for clinicians, administrators, and risk managers* (pp. 315–342). Springer.
28. Triplett, W. (2022). Ransomware attacks on the healthcare industry. *Journal of Business, Technology and Leadership*, *4*(1), 1–13.
29. van Boven, L. S., Kusters, R. W., Tin, D., van Osch, F. H., De Cauwer, H., Ketelings, L., Rao, M., Dameff, C., & Barten, D. G. (2024). Hacking acute care: A qualitative study on the health care impacts of ransomware attacks against hospitals. *Annals of Emergency Medicine*, *83*(1), 46–56.
30. Wang, Z., Hu, F., Su, J., & Lin, Y. (2024). Information Source Characteristics of Personal Data Leakage During the COVID-19 Pandemic in China: Observational Study. *JMIR Medical Informatics*, *12*(1), e51219.