Advancing Cybersecurity Use of Sensitive Data in Electronic Healthcare System: A Review of Privacy and Regulations

Ugochukwu Okwudilli Mathew[1]
Renata Lopez Rosa[2]
Oyedemi Oluyemisi Adenike[3]
Demostenes Zegarra Rodriguez[4]

Department of Computer Science Federal University of Lavras Minas Gerais, Brazil.
[1]ugochukwu.mathew@estudante.ufla.br
[2] renata.rosa@ufla.br
[3] oyedemi.adenike@ufla.br
[4] demostenes.zegarra@ufla.br

Abstract. Addressing cybersecurity challenges in electronic health system is imperative in ensuring trustworthiness of distributed healthcare information systems, thereby safeguarding sensitive patient information and optimizing healthcare service delivery. The use of data-driven technologies presents a promising opportunity for significant advances in information management required for an improved healthcare privacy protection for patients care, offering opportunities toward increased database accessibility in healthcare information system. This not only guarantees adherence to legal frameworks but also lays the groundwork for the ethical and accountable application of distributed systems in the medical field. To gain a thorough grasp of the requirements for cybersecurity in healthcare workforce groups, this paper applied a methodology that relied on a survey questionnaire. After that, it uses a risk-based methodology to estimate the risk of different cybersecurity and data privacy threats related to the stakeholder, determines the best ways to mitigate those cybersecurity risks, and suggests subsets of human-centric policies to manage each cybersecurity risk in the distributed healthcare setting. The results we obtained indicate that the effective management of individual cybersecurity risks across various healthcare organizations and diverse employee groups are facilitated by the adoption of a risk-based strategy for information privacy and cybersecurity risks protection. The research paper addressed cybersecurity and data privacy concerns in a distributed healthcare data warehouse while improving the current security challenges in electronic healthcare systems. The implementation of regulatory standards regarding GDPR and HIPAA is particularly crucial for the widest applicability in the global health system.

Keywords: Cybersecurity, Data Protection, Data Warehouse, Electronic Healthcare System, Information System, Privacy,

(Received November 19th, 2024 / Accepted December 19th, 2024)

1 Introduction

The purpose of this study is to give policymakers, healthcare professionals, and other interested parties a knowledgeable understanding of the restrictions and difficulties associated with exchanging information in the digital era [59, 13, 55, 12, 9, 48]. In addition, the paper aims to draw attention to the challenges nations, organizations and businesses will encounter when putting into practice efficient data security measures so that pursuing organization could adopt regulations that work with technological innovations in healthcare, and add to the continuing discussion on data security and privacy requirements in electronic health (e-health) system.This study aims to provide a better knowledge of the intricate issues involved and provide guidance for evidence-based policies and practices that prioritize patient privacy and security in the digital era by investigating the legal duties governing security of information in the healthcare sector. As healthcare systems information storage evolve into Internet of Things (IoT) cloud data warehouse system, a proactive and flexible strategy is needed to keep ahead of emerging privacy and cybersecurity concerns [2].

The digital health ecosystem may offer the framework for a more private and secure healthcare system by encouraging collaboration and making use of state-of-the-art cybersecurity technologies [24]. Cybersecurity is the use of tools, procedures, and policies to defend against cyberattacks on programs, devices, networks, systems, and data [44]. Given the harsh penalties imposed by the General Data Protection Regulation (GDPR) and the Network and Information Systems (NIS) regulations, an organization's response to a cyber-attacks events can frequently determine whether it succeeds or fails [27]. How quickly an organization detect and address such issues has a big impact on how well organizations manage the exposure, expenses, and risks. A thorough cybersecurity risk assessment may help identify problems early, lessen the chance that additional events will occur, and build a strong defense against attacks that might save the organization from misfortune. Computer hacking and data breaches are unavoidable, consequently responding preemptively to security breaches are crucial [49].

Multidisciplinary study on cybersecurity including the views of specialists in distributed databases for healthcare information systems will be crucial to the creation of all-encompassing solutions for electronic healthcare data warehousing systems [30], [38]. Organizations frequently utilize data warehouses as a logical system to record keeping and reuse answers to common issues through distributed online database systems. These systems are typically expected to increase throughput, lower information storage costs, and improve work quality. When distributed systems are integrated, there is great potential to improve data accessibility and interoperability in the healthcare industry [28], [39]. The healthcare industry is not the only one affected by cybersecurity, but compared to other industries, the healthcare sector has not made as much effort to protect its stakeholders' data [46]. The rapid digitization of medical histories for patients have resulted in significant financial and intangible harm to hospitals due to data breaches. Organizations have implemented electronic data governance tactics to encourage best practices for safeguarding the electronic infrastructure of hospitals and other clinical settings in order to mitigate the effects of cyberattacks [6]. Healthcare personnel may collaborate more easily when medical data is distributed and exchanged across a network of nodes, which enhances overall patient care and personalization. Nevertheless, the distributed design of these systems presents privacy and data security challenges, especially when handling private health information that is subject to United States Health Insurance Portability and Accountability Act (HIPAA) of 1996 and United Kingdom GDPR requirements.

In contrast to GDPR restrictions, HIPAA regulations do not grant patients the ability to view where or how their data is being utilized [14]. Because anonymized data can be shared according to GDPR's framework criteria, research using secondary sources is also made possible. GDPR does not apply to fully anonymized patient health information, but HIPAA is a framework that only safeguards such information [20]. Along with comparing the fundamentals of GDPR and HIPAA, this paper will show how GDPR and EU Member States have effectively addressed significant HIPAA concerns because GDPR legislation is better suited to meeting the demands of the modern healthcare technology implementation. In order to maintain HIPAA compliance with information communication and networks, the decentralized data warehouse system requires strong protections like encryption, access controls, and auditing procedures, even if it allows real-time data sharing and collaboration [36]. For distributed healthcare systems to be implemented successfully, the proper balance between data accessibility and privacy protection must be established. In addition, this paper highlights the necessity of standardized procedures and frameworks designed specifically for healthcare providers, taking into account the special qualities of medical data as well as the strict HIPAA rules and regulations. One of the main obstacles to the smooth integration of distributed systems in various healthcare settings is the absence of standardized cybersecurity requirements for improved service delivery in the ongoing development and use of IoT in the healthcare industry [32].

To protect patient data and uphold their right to privacy, compliance with regulatory requirements is essential in the healthcare industry [8]. The GDPR in the European Union and the HIPAA in the United States both place strict guidelines on how health data, including data gathered by IoT devices, must be handled. Organizations must put in place measures including access controls, encryption, and audit trails in order to comply with HIPAA's strict requirements for the security of digitally stored health information. In a similar development, GDPR mandates concepts such as accountability, purpose limitation, and data minimization, and for non-compliance, it imposes severe fines. The effectiveness of the GDPR is still being questioned, despite the fact that it appears to be the most advanced regulation regarding data protection and a global standard. Notable nations have created privacy legislation that adhere to the regulation's design and tenets since its creation in 2018 [52]. Brazil's privacy regulations are modeled after the GDPR, and the US adopted the California Consumer Protection Act in a manner similar to that of the EU [42]. As it has consistently done over the years, the Nigerian Data Protection Act is also seen as having obviously adopted the European model [37]. In order to comply with these regulations, organizational and technical precautions for health data gathered by IoT embedded devices must be put in place. This includes implementing privacy by design principles, carrying out cybersecurity risk assessments, and creating explicit policies and processes for handling data and responding to breaches [22]. Healthcare organizations may avoid legal risks, improve patient trust, and cultivate a culture of security and confidentiality of information by coordinating IoT implementation strategy with legal and regulatory requirements.

Innovative approaches are needed to handle the cybersecurity-related issues with electronic healthcare data warehouse technologies, including safeguarding private health information, maintaining compliance, assuring transparent information processing, and fostering trust [50]. The confidentiality of patients and the integrity of medical data have been compromised by the inadequate cybersecurity measures currently in place in healthcare institutions. Healthcare businesses are increasingly becoming a prime target for cybersecurity attacks due to significant volume of personal data they handle, which has a high black market value [11]. Healthcare companies have historically not seen the need to invest in cybersecurity because their primary focus has been on patient care, and they assumed that there would be little inducement for an attacker to target them [46]. Nonetheless, new research has shown that medical data is far more valuable than any other type of data. The growing adoption of IoT technology in healthcare has expanded the attack surface beyond information security to physical safety, resulting in hospital technical staff lacking adequate security controls to meet cybersecurity needs [35], [29]. As the Nigeria Data Protection Commission (NDPC) has stated that it is actively looking into significant data breach instances in a number of industries, including health, banking, technology, education, consulting, government, logistics, and lottery, the country is not exempt from these data breaches conundrum [20]. One such investigation that is presently underway involves the National Identity Management Commission (NIMC), which has made an effort to refute claims of data breaches by asserting that the NIMC data breach controversy is not about a significant data leak but rather about unauthorized access by certain entities [1], [20].

As reported by cybersecurity firm Surfshark, the number of data breach events in Nigeria rose by 64% in the first quarter of 2023, from 50,000 in the fourth quarter of 2022 to 82,000 in the first quarter of 2023 [20]. The healthcare industry's ability to successfully implement data warehouse information digital ecosystem initiatives depends on how well healthcare workers understand the risks associated with information security threats [34]. Healthcare organizations generally aim to implement data privacy and cybersecurity policies that prioritize the human element. This is due to the fact that generic principles are usually difficult to translate into specific controls such training programs and awareness campaigns that have been shown to benefit staff members while minimizing budget expenditure. The risk associated with different human-related cybersecurity and data privacy concerns is then quantified using a risk-based methodology in this paper. Appropriate techniques for tackling these risks are then identified, and combinations of human-centric controls are suggested for controlling every possible risk. The remaining part of the paper is stricture into : Objectives of the Study, Theoretical Framework, Research Methodology, Research Design, Method of Data Collection, Survey Design, Analysis of Research Findings, Recommendation and Conclusion.

1.1 Objective of the Study

It became necessary to put in place suitable protections and controls to improve the privacy and security of every piece of data that was gathered and uploaded since patient data is extremely sensitive. Clarifying the cybersecurity challenges, approaches, and possible developments in protecting health data in IoT ecosystems is the aim of this article. The introduction starts off by giving a general review of the laws pertaining to electronic health security, emphasizing their importance and wide range of uses in the healthcare industry. The emphasis then shifts to the healthcare sector, highlighting the critical function of gathering and organizing health data. The findings prepares the audience on the discussions of the significance of identity and access management frameworks in protecting private health information. In the end, this opens the door to a more thorough investigation of incorporating identity and access management for improved security into IoT embedded systems. In the subsisting sections, the fundamental principles of accessibility and identity management and IoT connected devices are examined, along with their interrelationships, in the context of healthcare data security. By conducting a comprehensive analysis, the authors intend to identify issues, provide solutions, and outline future research directions to strengthen the cybersecurity posture of IoT-enabled healthcare networks.

2 Theoretical Framework

By leveraging data warehouse technology, the digitization of data and information visualization have transformed the healthcare sector and created previously unimaginable opportunities for medical record federation, fostering efficiency and further development [57], [51]. Healthcare providers must balance the advantages and challenges of this digital transformation as they adjust to this innovation and deal with improved patientâs management. The way clinicians diagnose, treat, and monitor patients have changed dramatically as a result of the revolutionary rise of artificial intelligence (AI) and machine learning in conjunction with IoT cloud data warehouse technology in the digital health sector [31]. By enabling more individualized treatments and generating more accurate diagnoses, this technology is significantly enhancing healthcare research and results. Medical practitioners can find disease signs and patterns that would otherwise go unnoticed because of AIâs rapid analysis of enormous volumes of clinical data. AI has a wide range of possible uses in healthcare, from predicting results to electronic medical records to analyzing radiological images for early detection [33], [15]. Healthcare businesses can redefine the future of healthcare by adopting digitization and using data in order to enhance patient outcomes, expedite clinical operations, and spur innovation. Healthcare data protection policies provide people control over their personal information, allowing them to decide how it is used, shared, and disclosed [45].

The goal of data security is to protect the accessibility, privacy, and security of the stored data, which means that only authorized parties can access the data within specified timeframes to reduce the risk of data fraud.Healthcare systems can handle millions of patients queries globally more intelligently, quickly, and efficiently by utilizing AI in clinics and hospitals setting [25]. The potential applications of AI in healthcare are simply astounding and are anticipated to significantly alter how we handle medical data, identify infections, create cures, and even prevent them entirely. Medical personnel can save time, cut expenses, and enhance medical records administration by employing artificial intelligence in healthcare to make better judgments based on more accurate information [40]. AI in healthcare has the potential to revolutionize everything from finding novel cancer treatments to enhancing patient experiences, paving the path for a time when patients will receive high-quality care and treatment more quickly and precisely than in the past [18]. By improving medical diagnosis and treatment, machine learning which is a crucial aspect of AI application in healthcare, has drastically changed the industry. Algorithms can find patterns and make previously unheard-of accurate predictions about medical outcomes by analyzing enormous volumes of clinical data [16].

Healthcare practitioners can enhance treatments and cut costs by using this technology to analyze patient information, medical imaging, and find new therapies. Precise illness diagnosis, tailored therapies, and the identification of minute variations in vital signs that may point to possible health problems are all made possible by machine learning application in the clinical diagnosis [7]. The most popular use of machine learning in precision medicine, uses supervised learning to forecast successful treatment plans based on patient-specific data. In addition, deep learning being a branch of artificial intelligence is employed in the medical field for tasks like natural language processing-based speech recognition [56]. Healthcare workers will need to comprehend and apply deep learning in clinical contexts more and more as it develops, compelling AI to revolutionize the healthcare sector by enabling computers to comprehend and utilize human language through natural language processing [56]. Many health data applications, including the enhancement of patient care through increased diagnosis accuracy, expediting clinical procedures, and offering more individualized services, use natural language processing [10]. For instance, by gleaning valuable information from health data, natural language processing can be used to accurately detect ailments in medical records [58]. It can be used to determine which medications and therapies are appropriate for each patient, or even forecast possible health hazards by using historical health data.

The natural language processing gives therapists strong tools for handling vast volumes of complex data, something that would often take a lot longer time to accomplish by human indicators. Natural language processing is turning out to be a very useful technology in the medical field that enables doctors to employ artificial intelligence to detect diseases more precisely and treat patients more individually [5]. One of the most recent and significant advancements in healthcare is precision medicine, which holds promise for enhancing the conventional symptom-driven practice of medicine by enabling earlier interventions through the use of sophisticated diagnostics and creating more effective and cost-effectively individualized therapies [3]. Utilizing healthcare information in clinical decision-making has proven challenging due to the individual-level intricacies of disease; nevertheless, technological breakthroughs such as the application of artificial intelligence and machine learning have significantly reduced some of the current limitations. The power of electronic health records must be harnessed to integrate disparate data sources and identify patient-specific patterns of disease progression in order to implement effective precision medicine with improved capacity to positively impact patient outcomes and provide real-time decision support [53].

In addition to addressing ethical and social concerns about the privacy and preservation of healthcare data in an efficient manner, useful analytical tools, technologies, databases, and methodologies are needed to enhance the networking and interoperability of clinical, laboratory, and public health systems [41]. Creating multipurpose machine learning platforms for the extraction, aggregation, management, and analysis of clinical data might help physicians by effectively classifying participants to comprehend certain situations and enhance decision-making. The implementation of artificial intelligence in healthcare is an intriguing idea that could result in major advancements in reaching the objectives of more personalized, population, and real-time medicine at reduced costs [23]. The increasing digitization of medical records represents a significant advancement in healthcare, offering improved patient care in terms of quality, efficacy, and accessibility. The electronic health records, have facilitated information retrieval, accelerated decision-making, and enhanced communication between healthcare practitioners [47]. But the digital revolution brought with it a number of unprecedented challenges, particularly with regard to safeguarding the integrity and confidentiality of private health data. Because healthcare organizations are responsible for keeping vast volumes of sensitive and private patient data, they must traverse a challenging landscape of increasing cybersecurity threats [17]. In the healthcare sector, the demand for strong data security measures have increased along with the rise in data breaches, computer hacking, and the lucrative black market for medical data [54]. As organizations struggle with cybersecurity problems, blockchain technology seems to be a ray of hope; it is a disruptive force that might completely alter the way we think about patient data management [61]. Blockchain technology adds an additional degree of protection for patient information, enabling the technology to offer a transparent, decentralized, and incorruptible patient data log. The data is transparent, but it uses complicated and secure codes to hide a person's identify, protecting the privacy of healthcare data. As a result, patients, healthcare professionals, and physicians may all safely and securely access and share the decentralized data. In addition, fast data transfers shorten the period of time that the data is susceptible, enabling blockchain technology to facilitate safe management and preservation of healthcare data and transactions while properly identifying potentially harmful errors in medical history [21].Healthcare data privacy is effective data management techniques and defense against cyberattacks [24].

In the healthcare sector, data privacy is controlled by a system of laws and guidelines that guarantee that only authorized personnel have access to patient information and medical records. There are a number of shortcomings in traditional healthcare systems, including as disjointed medical records, data integrity problems, inefficient supply chains, interoperability problems, patient data security breaches, and more [62]. In addition to mistakes like fraud, data fabrication and mischievousness during trials hinder the intended outcomes of medical researches. Blockchain technology employs cryptography to establish a decentralized database of transactions in which the record of transactions cannot be changed without the agreement of all network participants. Blockchain's decentralized and irreversible nature is the basis of its revolutionary potential for healthcare data. The narrative then seamlessly transitions to a discussion of how blockchain technology may be applied to address the many issues around patient data management. As the study progresses, a thorough approach includes everything from ensuring the security of patient data because of the inherent immutability of blockchain technology to building access control mechanisms utilizing permissioned blockchains. Examining safe data transfer and interoperability among healthcare organizations demonstrates how blockchain technology may be the solution to problems pertaining to the exchange of sensitive medical information.

3 Research Methodology

The goal of this research paper is to advance cybersecurity improvements by offering frameworks for privacy and digital governance in the electronic healthcare system. Utilizing a doctrinal research methodology, this study thoroughly examines primary and secondary sources of data, such as government legislation governing electronic healthcare technologies, data protection laws, and health laws with respect HIPAA and GDPR requirements for healthcare data. The focus of doctrinal research approach is on the language of the law as opposed to how it is applied.

A researcher writes a thorough and descriptive examination of legal requirements that can be found in original sources such as statutes, regulations, or cases decided by courts. This approach is to compile, arrange, and explain the legislation; offer commentary on the sources that were used; and then pinpoint and explain the overarching theme or system and the connections between each source of law. In order to substantiate research inquiries, the researcher uses this method to critically and qualitatively analyze legal information. After identifying certain legal rules that governs the use of electronic health data, the researcher must go over the rules' legal meaning, guiding principles, and decision-making processes, including whether or not instances in interpreting the rules make sense as a whole. The individual conducting the study must also point out legal ambiguities and critiques and provide answers. The rule itself, the instances brought about by the government, legislative history when relevant, literature and commentary on the rule are all sources of data used in doctrinal research in this regard.

A comprehensive awareness of the healthcare data security landscape will be aided by published books, journals, articles, and case study. To increase the understanding of cybersecurity and data privacy among various employee groups in healthcare organizations, the primary source used a novel survey-based risk assessment approach. The suggested cybersecurity methodology takes into account the human factors in the cybersecurity mitigation approaches by concentrating on the requirements and gaps of distinct employee groups. Finding the best approach to managing data privacy and cybersecurity risks is the primary goal of this methodology. To put the strategy into practice, it suggests a human-centered controls like awareness campaigns, training courses, motivations, etc., that are adaptable to the needs of the healthcare enterprise with respect to organizational culture, employee positions and duties, and personnel backgrounds. The methodology comprised a recommended risk-based approach survey analysis after a cross-sectional exploratory survey investigation. In the beginning, the survey made it is easier to gather information and evaluate the shortcomings and requirements of four distinct employee groups among three selected healthcare institutions: i) Healthcare Managerial Staff; ii) Medical/Clinical Staff; iii) Information Technology (IT)/Technical Staff; and iv) Cybersecurity Administrative Staff. To characterize the circumstances for each of the four employee groups at each organization with regard to seven different cybersecurity and data privacy attacks scenarios, a 15-question online survey was administered. After that, authors transcribed the answers to the suggested risk-based analysis method in order to gain knowledge about the risk levels for each employee group, risk category in the healthcare organizations.Specifically, five risk management strategies were established, and cybersecurity risks were assigned a number between 1 and 5, where 1 denoted the least amount of vulnerability and 5 the most, as perceived by the researchers.

The methods for measuring the risk using the risk marking calculated from the survey answers were established. Based on data collected from the online survey, the authors were able to quantify risk and choose the best course of action, which included mitigation measures to data privacy preservations. For the healthcare sector, managing massive amounts of patient data and protecting its digital infrastructure are significant challenges. Resolving issues like data breaches, cybersecurity threats, and poor data management is crucial to ensuring patient safety and improving healthcare delivery. For fake data injection and electronic data manipulation, the paper proposed blockchain federated learning for cybersecurity and IT advancements which offered innovative solutions for data privacy preservation [26]. This paper looks at how these technologies can be utilized to protect hospital infrastructure and enhance patient data accessibility and ease of use for healthcare across electronic digital ecosystem.

4 Research Design

A proposed risk-based analysis and a cross-sectional exploratory survey study were created and made available online to describe cybersecurity incidents in the three healthcare organization that took part in the survey. In order to adopt preemptive data breaches attack in the healthcare industry, the current study was created to collect data on the cybersecurity status within the institutions. In order to look into people's expectations about the ongoing research goal, the study used a questionnaire that was split into three sections and distributed online. With regard to privacy and data security, the first section was thoughtfully designed to gather information on the intended audience regarding the advancements in cybersecurity technologies in the healthcare industry. The second section included questions about management attitudes toward implementing electronic healthcare and digital data protection, as well as the development of the organization's IT infrastructure. To protect patient data and uphold their right to privacy, compliance with regulatory requirements is essential in the healthcare industry. Strict guidelines for safeguarding health data, including data gathered by IoT devices, are enforced by laws like the GDPR and HIPAA. Access controls, encryption, and audit trails are just a few of the procedures that institutions must put in place to comply with HIPAA's strict safeguards for the protection of electronic health information. In a similar development, GDPR upholds the requirements permitting accountability and data minimization, compelling substantial punishments for inability to comply with acceptable standards. In order to comply with these regulations, organizational and technical safeguards for health data gathered by IoT embedded devices must be put in place. This includes implementing privacy by design principles, carrying out risk assessments, and creating explicit policies and processes for handling data and responding to breaches. Healthcare organizations can reduce legal risks, improve patient trust, and cultivate a data privacy and security culture by coordinating IoT deployment strategy with regulatory requirements.

5 Method of Data Collection

A systematic recruitment procedure was used to get end-users to participate in the study, and it was started with an open online survey tool. Direct emails were another method of recruiting, when participants were viewed as knowledgeable in the healthcare and cybersecurity studies by the authors. The user recruitment process took place from the middle of June 2024 to the end of November 2024. The preliminary section of the survey, which included information about its goal, was available to all participants. Before the survey questions were asked, each participant gave their digital consent. By denying access to the survey again to people with the same IP address, duplicate entries were prevented. The survey's theme and format led to the grouping of the questions into eleven risk categories. The process of creating the final survey questionnaire required mapping the cybersecurity environment by examining the body of current literature and researching the resources that were accessible. The list of the top threats in the healthcare industry, for example, prompted the inclusion of specific questions to find out how familiar the employees are with these threats, whether they are aware of relevant incidents that have occurred both inside and outside their organization, whether they can identify such incidents in their early stages, and how confident they feel handling them. Furthermore, considering the nature of these major threats, it was determined to clearly distinguish between cybersecurity and data privacy issues while defining the risk categories and related survey questions. Lastly, a number of risk categories and related poll questions represent the professional perception of cybersecurity authorities and organizations.

6 Survey Design

The purpose of the current survey was to gather information about many facets of healthcare cybersecurity development, data privacy, and data protection in the context of the extensive distributed healthcare digital ecosystem and connected system. The representation in Figure 1 shows the process involved in the creation of the survey. The project's research team first established a consensus group with experts from three healthcare organizations. This group conducted an initial review of the body of knowledge on healthcare cybersecurity, including pertinent publications from healthcare organizations in line with National Cybersecurity Coordination Centre (NCCC) that highlight the leading threats in this field. In order to create the final survey questionnaire that addressed the research questions, it was essential to map the cybersecurity environment using the review of the existing literature and the analysis of the data was available.

In addition to earlier surveys on the subject, a review of reports and recommendations from global cybersecurity organizations and centers, including the Center for Internet Security (CIS), the European Network and Information Security Agency (ENISA), and the European Cybersecurity Organization (ECSO), were adequately consulted.

Seven people made up the research team, and their backgrounds ranged from technical and medical academia to healthcare practitioners, IT and cybersecurity specialists, and data scientists. In order to fully compose the research population, the research team then determined the primary staff groups in the healthcare businesses, which include administrative, medical/clinical, IT/technical, and executive/security individuals. Given that different employee groups have different levels of cybersecurity and data privacy knowledge and do everyday duties that expose them to different risks, it stands to reason that they are not all equally vulnerable to cybersecurity vulnerabilities. With re-

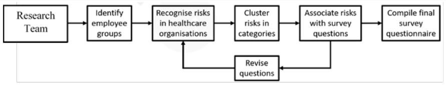
Research Team
Identify employee groups
Recognise risks in healthcare organisations
Cluster risks in categories
Associate risks with survey questions
Compile final survey questionnaire
Revise questions

Figure 1: An illustration of the survey construction process

gard to the cybersecurity risk category, the first set of questions were designed with the intention of estimating the pertinent risk based on the answers. Several rounds of the questions were examined and improved, and when new hazards were identified, they were repeated. This resulted in the creation of new risk categories or the modification of previously established categories, which was followed by the addition of new questions. The research team eventually decided on a final survey with 50 English-language cybersecurity questions after several rounds of evaluation.

6.1 Data Presentation

This section presents the result of applying the exploratory methodology to the healthcare organizations including the survey demographics, the risk-based analysis of the survey responses, and our observations. The analysis of the results is performed with regards to four different aspects of occupational specialization in line with cybersecurity outcomes. A total of 225 people accessed the survey link, and 185 completed the survey for the rightful purpose, which represent 82.22% response rate. The remaining responses that does not aligned with the occupational target were classified under others and discarded.

From Table 1, 30(13.3%) respondent were managerial staff within the selected healthcare organization. Medical/Clinical staff represent 45(20%) of the distribution. IT/Technical staff represent 60(26.7%) of the distribution, Cybersecurity staff represent 50(22.2%) while the rest respondents were classified as others amounting to 40(17.8%) respondent. Phishing attacks account for almost 90% of all attacks on the healthcare sector [4], in line with the findings of Herjavec Group, a pioneer in cutting-edge cybersecurity operations that has proven successful in cybersecurity challenges in multi-technology settings. Similar to this, 45% of healthcare cybersecurity experts reported that their organization's most serious data breach was caused by a phishing attack [60]. General email phishing accounted for 71% of instances, spear phishing for 67%, voice phishing (vishing) for 27%, whaling for 27%, business email compromise for 23%, and SMS phishing [63]. Healthcare workers clicked on almost one out of every seven phishing emails sent in a study that mimicked phishing tactics targeting US healthcare institutions [43]. Compared to most other industries, just 16% of healthcare workers say they are very well understand the hazards posed by social engineering cybersecurity threats like phishing. From Table 2, 80(25.4%) respondents reported Phishing attack as the topmost cybersecurity risk in healthcare, 12(3.8%) reported man in the middle attack, 60(19.1%) ransomware, 25(7.9%) reported DoS/DDoS attack, 26(8.2%) reported brute force attack/password attack, 9(2.9%) reported vishing attack, 32(10.2%) reported malware/virus attack, 22(6.8%) reported social engineering ,6(1.9%) reported cross site scripting, 11(3.5%) reported SQL injection attack while 32(10.2%) reported Insider threat attack.

Table 1: Survey Demographics for the Healthcare Organizations Cybersecurity Participant

Occupational Specialization	Frequency	Perc. (%)
Managerial Staff	30	13.3
Medical/Clinical Staff	45	20.0
Cybersecurity Admin Staff	50	22.2
IT/Technical Staff	60	26.7
Others	40	17.8
Total	225	100

Table 2: Cyber-Attack Classification base on IT Department

Cyber sec. Attacks Categ.	Frequency	Perc. (%)
Phishing Attack	80	25.39
Man in the Middle Attack	12	3.81
Ransomware	60	19.05
DoS/DDoS Attack	25	7.94
Brute Force Attack /Password Attack	26	8.25
Vishing Attack	9	2.86
Malware/Viruses attack	32	10.16
Social Engineering	22	6.98
Cross-Site Scripting	6	1.90
SQL Injection Attack	11	3.49
Insider Threat Attack	32	10.16
Total	315	100

From Table 2, 80(25.4%) respondents reported Phishing attack as the topmost cybersecurity risk in healthcare, 12(3.8%) reported man in the middle attack, 60(19.1%) ransomware, 25(7.9%) reported DoS/DDoS attack, 26(8.2%) reported brute force attack/password attack, 9(2.9%) reported vishing attack, 32(10.2%) reported malware/virus attack, 22(6.8%) reported social engineering, 6(1.9%) reported cross site scripting, 11(3.5%) reported SQL injection attack while 32(10.2%) reported Insider threat attack.

7 Discussion of Research Findings

Healthcare organizations need to handle cyber security risks holistically, combining business workflow, data management procedures, user access control management, and information technology and disaster recovery [19]. In order to combat the recent surge in cyberattacks such as ransomware and phishing attack, which have been used by attackers to take advantage of flaws in people and technology brought about by changes in working procedures in response to the automation of electronic healthcare, this review set out to identify the main cybersecurity challenges, solutions adopted by the health sector, and areas that require improvement. This survey include specific control measures such as cybersecurity awareness, data privacy/protection awareness, cybersecurity training, communication channel secured connection, device use, and social engineering attack detection.

The survey indicates that ransomware and phishing emails are two common types of attacks. In order to perpetrate crimes or obtain access to an organization's network for fraudulent reasons and financial gain, phishing email attacks seek to gather sensitive information, including user passwords. The study noted that there was growing worry about insider threats in relation to the lessons learned from cybersecurity disasters in the healthcare industry. Healthcare information security breach numbers, relating to this analysis, clearly demonstrate an upward trend in data breaches over the last 14 years, with 2021 reporting more data breaches than any other year since the Office of Civil Rights (OCR) began publishing records. In 2022, there was another surge in data breaches; OCR received complaints of 720 data breaches involving 500 or more records.

In 2023, cyberattacks on healthcare institutions continued to escalate, setting two new milestones: the most reported data breaches and the most compromised records. OCR received reports of 725 data breaches in 2023, resulting in the exposure or unlawful disclosure of over 133 million records. Because OCR does not release information about minor data breaches, even though HIPAA mandates that all data breaches, regardless of size, be reported, the healthcare data breach statistics below only cover data breaches involving 500 or more records that have been reported to OCR. The statistics and graphs below show both closed cases and breaches that OCR is currently looking into for possible HIPAA violations. In 2023, OCR discovered that between January 1, 2018, and September 30, 2023, ransomware attacks rose by 27.8% and hacking-related data breaches rose by 23.9%. Hacking was responsible for 49% of the breaches that were disclosed in 2019. In 2023, hacking attacks were responsible for 79.7% of data breaches. HIPAA compliance is crucial both financially and morally because of the harsh penalties for infractions, which can reach multi-million dollar fines if violations have been let to continue for years or if there is systemic non-compliance with the HIPAA Rules. One of the main causes of the significant increase in HIPAA violation penalties in 2020 was OCR's new enforcement campaign that focused on non-compliance with the HIPAA Right of Access, which is patients' right to view and acquire a copy of their medical records. In 2020, healthcare providers negotiated 11 settlements to address incidents in which patients were denied timely access to their medical data. In 2021, all but two of the 14 penalties were related to violations of the HIPAA Right of Access. To address violations of the HIPAA Right of Access, 46 penalties were levied between September 2019 and December 2023. In 2022, the United States Department of Health and Human Services (HHS) Office for Civil Rights imposed 22 penalties for violations of the HIPAA, which happened to be the highest reported number since 2008, Refer to Figure 2. In the first half of 2024, the number of OCR fines was six. The second-highest number of penalties imposed by OCR was in 2020 when due to COVID-19, the healthcare sector was highly targeted by cyber-attacks.

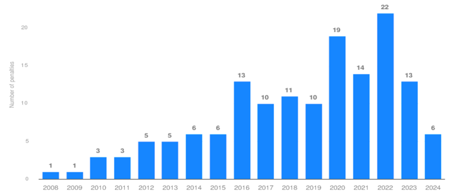

Figure 2: U.S. number of Office for Civil Rights penalties for HIPAA violations 2008-H1 2024: Published by Ani Petrosyan, Sep 12, 2024.Source: https://www.statista.com/statistics/1403620/ocr-penalties-hipaa-violations-us/

8 Recommendation

Information security and privacy can be maintained by the adaptation of blockchain technology between the client and server nodes. Blockchain provides decentralization, incentive mechanisms, and cyberattack resistance, while federated learning enables the collaborative integration of data aggregation and machine learning models in a remote environment. Federated learning provided by blockchain speeds up member verification and selection. Cognitive computing may improve accuracy, resistance to data injection cyberattacks, and incentive systems for the healthcare sector by incorporating blockchain into federated learning. Future research should incorporate blockchain technology and machine learning to improve the system's resistance to DoS and DDoS attacks and experiment any limitation of the implementation. The system's daily record will be used to train the current model, which will allow for the prompt observation of attack behavior and the efficient application of adaptive defense mechanisms based on training instances and report every shortcoming.

9 Conclusion

This work advances the field of cyber security research by presenting a cyberattack development in the electronic healthcare industry. It categorized attacks according to their target, typical vulnerabilities used to launch cyberattacks, operational impact and attack pathways in line with regulatory requirements. As healthcare data becomes more digitalized and attacks get more sophisticated, the number of HIPAA breaches continues to rise despite increased awareness of HIPAA compliance. While some contend that a greater understanding of HIPAA compliance is contributing to fewer HIPAA breaches caused by misplaced or stolen drives and devices, others counter that fewer covered organizations are transferring unencrypted patient health information on drives and devices as a result of the rise in cloud computing. While a HIPAA data breach is a breach of any Protected Health Information including financial information from any covered health plan, health care clearinghouse, healthcare provider, or business associate offering a service for or on behalf of a covered entity, a healthcare data breach is one in which healthcare data is accessed without authorization from a healthcare provider who may or may not be a HIPAA covered entity or business associate. As a result, what separates a healthcare data breach from a HIPAA data breach depends not only on the type of data, healthcare data versus healthcare, payment, and other data with protected status, but also on the organization's status at the time of the unauthorized access covered or non-covered healthcare provider versus HIPAA covered entity or business associate. The regulatory body, the breach reporting requirements, and the penalty for a data breach can all be affected by the seemingly insignificant variation.

10 Conflict of Interest

There is no conflict of interest regarding this publication.

References

[1] Adegoke, A. Digital rights and privacy in nigeria. *Paradigm Initiative*, 4, 2024.

[2] Ahmed and Khan. Securing the internet of things (iot): A comprehensive study on the intersection of cybersecurity, privacy, and connectivity in the iot ecosystem. *AI, IoT and the Fourth Industrial Revolution Review*, 13:1–17, 2023.

[3] Ahmed, M. et al. Artificial intelligence with multi-functional machine learning platform development for better healthcare and precision medicine. *Database*, 2020.

[4] Alkhalil, H. et al. Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, 3, 2022.

[5] Alowais, A. et al. Revolutionizing healthcare: the role of artificial intelligence in clinical practice. *BMC medical education*, 23, 2023.

[6] Argaw, T.-P. et al. Cybersecurity of hospitals: discussing the challenges and working towards mitigating the risks. *BMC medical informatics and decision making*, 20, 2020.

[7] Asif, W. et al. Advancements and prospects of machine learning in medical diagnostics: Unveiling the future of diagnostic precision. *Archives of Computational Methods in Engineering*, 2024.

[8] Begum, D. et al. Health care data privacy and compliance: Navigating regulatory landscape. *Central Asian Journal of Medical and Natural Science*, 4, 2023.

[9] Carvalho Barbosa, R., Shoaib Ayub, M., Lopes Rosa, R., Zegarra Rodrïgues, D., and Wuttisittikulkij, L. Lightweight pvidnet: A priority vehicles detection network model based on deep learning for intelligent traffic lights. *Sensors*, 20, 2020.

[10] Chaurasia, A. Algorithmic precision medicine: Harnessing artificial intelligence for healthcare optimization. *Asian Journal of Biotechnology and Bioresource Technology*, 2023.

[11] Chavan and Kanade. Blockchain and cybersecurity revolutionizing healthcare in the digital era. In *Ensuring Security and End-to-End Visibility Through Blockchain and Digital Twins, ed: IGI Global*, 2024.

[12] de Sousa, A. L., Okey, O. D., Rosa, R. L., Saadi, M., and Rodriguez, D. Z. A novel resource allocation in software-defined networks for iot application. In *2033 International conference on Software, Telecommunications and Computer Networks (SoftCOM)*, 2023.

[13] dos Santos, M. R., Batista, A. P., Rosa, R. L., Saadi, M., Melgararejo, D. C., and Rodrí'guez, D. Z. Aqm: Audio streaming quality metric based on network impairments and user preferences. *IEEE Transactions on Consumer Electronics*, 2023.

[14] Fede, L. M. et al. Protection of patient data in digital oral and general health care: A scoping review with respect to the current regulations. *Oral*, 3, 2023.

[15] Gou, L. et al. Research on artificial-intelligence-assisted medicine: a survey on medical artificial intelligence. *Diagnostics*, 14, 2024.

[16] Gupta, S. et al. Building predictive models with machine learning. In *Data Analytics and Machine Learning: Navigating the Big Data Landscape, ed: Springer*, 2024.

[17] Herath, H. et al. Data protection challenges in the processing of sensitive data. In *Data Protection: The Wake of AI and Machine Learning, ed: Springer*, 2024.

[18] Hesso, K. et al. Cancer care at the time of the fourth industrial revolution: an insight to healthcare professionalsâ perspectives on cancer care and artificial intelligence. *Radiation Oncology*, 18, 2023.

[19] Huda, I. et al. A cyber risk assessment approach to federated identity management framework-based digital healthcare system. *Sensors*, 24, 2024.

[20] Isibor, E. Regulation of healthcare data security: Legal obligations in a digital age," available at ssrn 4957244, 2024.

[21] Karthikeyan, K. et al. Creative strategies to protect patientsâ health records and confidentiality using blockchain technology. *BlockchainâEnabled Solutions for the Pharmaceutical Industry*, 2025.

[22] Kavak, A. Privacy of information and data: Policies, threats, and solutions. In *Creating and Sustaining an Information Governance Program, ed: IGI Global*, 2024.

[23] Khatoon, U. et al. Ethical reflections on data-centric ai: balancing benefits and risks. *International Journal of Artificial Intelligence Research and Development*, 2, 2024.

[24] Layode, N. et al. The role of cybersecurity in facilitating sustainable healthcare solutions: Overcoming challenges to protect sensitive data. *International Medical Science Research Journal*, 4:668 – 693, 2024.

[25] Lee and Yoon. Application of artificial intelligence-based technologies in the healthcare industry: Opportunities and challenges. *International journal of environmental research and public health*, 18, 2021.

[26] Mahmood and Jusas. Blockchain-enabled: Multi-layered security federated learning platform for preserving data privacy. *Electronics*, 11, 2022.

[27] Markopoulou, D. Cyber-insurance in eu policy-making: Regulatory options, the market's challenges and the us example. *Computer Law Security Review*, 43, 2021.

[28] Mathew, R. et al. Advancing healthcare 5.0 through federated learning: Opportunity for security enforcement using blockchain. In *International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pages 1–6, 2024.

[29] Matthew, K. et al. Role of internet of health things (iohts) and innovative internet of 5g medical robotic things (iio-5gmrts) in covid-19 global health risk management and logistics planning. In *COVID-19 global health risk management and logistics planning," in Intelligent Data Analysis for COVID-19 Pandemic, ed: Springer*, 2021.

[30] Matthew, O. et al. E-healthcare data warehouse design and data mining using ml approach. In *Reshaping Healthcare with Cutting-Edge Biomedical Advancements*, 2024.

[31] Monteiro, F. et al. An overview of medical internet of things, artificial intelligence, and cloud computing employed in health care from a modern panorama. *The Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care*, 2021.

[32] Mwangi, E. Exploring iot embedded systems along the line of identity access management for

enhanced health data security. *Authorea Preprints*, 2024.

[33] Nasarudin, J. et al. A review of deep learning models and online healthcare databases for electronic health records and their use for health prediction. *Artificial Intelligence Review*, 57, 2024.

[34] Nifakos, C. and Others. Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, 21, 2021.

[35] Nissar, K. and Others. Iot in healthcare: a review of services, applications, key technologies, security concerns, and emerging trends. *Multimedia Tools and Applications*, 2024.

[36] Odeh, A. et al. Privacy-preserving data sharing in telehealth services. *Applied Sciences*, 14, 2024.

[37] Olukoya, O. Assessing frameworks for eliciting privacy security requirements from laws and regulations. *Computers Security*, 117, 2022.

[38] Onyebuchi, M. et al. Business demand for a cloud enterprise data warehouse in electronic healthcare computing: Issues and developments in e-healthcare cloud computing. *International Journal of Cloud Applications and Computing (IJCAC)*, 12, 2024.

[39] Onyebuchi, M. et al. Cloud-based iot data warehousing technology for e-healthcare: A comprehensive guide to e-health grids. In *Pioneering Smart Healthcare 5.0 with IoT, Federated Learning, and Cloud Security, ed: IGI Global*, 2024.

[40] Oyekunle, O. et al. Trust beyond technology algorithms: A theoretical exploration of consumer trust and behavior in technological consumption and ai projects. *Journal of Computer and Communications*, 12, 2024.

[41] Patel, K. Ethical reflections on data-centric ai: balancing benefits and risks. *International Journal of Artificial Intelligence Research and Development*, 2, 2024.

[42] Pimenta-Rodrigues, M.-S. et al. Understanding data breach from a global perspective: Incident visualization and data protection law review. *Data*, 9, 2024.

[43] Priestman, A. et al. Phishing in healthcare organisations: Threats, mitigation and approaches. *BMJ health care informatics*, 26, 2019.

[44] Prince, A. M. et al. Ieee standards and deep learning techniques for securing internet of things (iot) devices against cyber attacks. *Journal of Computational Analysis and Applications*, 33, 2024.

[45] Prince, O. et al. Online privacy literacy and users' information privacy empowerment: the case of gdpr in europe. *Information Technology People*, 37, 2024.

[46] Rahim, R. et al. Cybersecurity threats in healthcare it: Challenges, risks, and mitigation strategies. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, 6, 2024.

[47] Rolla, K. Trends and futuristic applications of big data and electronic health record data in empowering constructive clinical decision support systems. *Bio-Science Research Bulletin (Life sciences)*, 2024.

[48] Rosa, R. L., Rodriguez, D. Z., and Bressan, G. Sentimeter-br: A social web analysis tool to discover consumers' sentiment. In *2013 IEEE 14th international conference on mobile data management*, volume 2, 2013.

[49] Shandilya, D. et al. Advancing security and resilience. In *Digital Resilience: Navigating Disruption and Safeguarding Data Privacy*, 2024.

[50] Shandilya, D. et al. Navigating the regulatory landscape. In *Digital Resilience: Navigating Disruption and Safeguarding Data Privacy, ed.* Springer, 2024.

[51] Sharma, P. et al. A review: Transformative impact of data visualization across various industries. In *8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, pages 799–804, 2024.

[52] Sirur, N. et al. Are we there yet? understanding the challenges faced in complying with the general data protection regulation (gdpr). In *Proceedings of the 2nd international workshop on multimedia privacy and security*, 2018.

[53] Sitapati, K. et al. Integrated precision medicine: the role of electronic health records in delivering personalized treatment. *Wiley Interdisciplinary Reviews: Systems Biology and Medicine*, 9, 2017.

[54] Tao, B. et al. Economic perspective analysis of protecting big data security and privacy. *Future Generation Computer Systems*, 98, 2019.

[55] Teodoro, A. A., Silva, D. H., Rosa, R. L., Saadi, M., Wuttisittikulkij, L., Mumtaz, R. A., and Rodriguez, D. Z. A skin cancer classification approach using gan and roi-based attention mechanism. *Journal of Signal Processing Systems*, 95(2-3), 2023.

[56] Tyagi and Bhushan. Natural language processing (nlp) based innovations for smart healthcare applications in healthcare 4.0. In *Enabling Technologies for Effective Planning and Management in Sustainable Smart Cities, ed: Springer*, 2023.

[57] Uddin and Hossan. A review of implementing ai-powered data warehouse solutions to optimize big data management and utilization. *Academic Journal on Business Administration, Innovation Sustainability*, 4, 2024.

[58] Verma, J. Unleashing the power of artificial intelligence: Exploring multidisciplinary frontiers for innovation and impact. In *Artificial Intelligence for Intelligent Systems, ed: CRC Press*, 2025.

[59] Vieira, S. T., Rosa, R. L., and Rodrií'guez, D. Z. A speech quality classifier based on tree-cnn algorithm that considers network degradations. *Journal of Communications Software and Systems*, 16(2), 2020.

[60] Wasserman and Wasserman. Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in Digital Health*, 4, 2022.

[61] Webster, M. Do no harm: protecting connected medical devices, healthcare, and data from hackers and adversarial nation states. *John Wiley Sons*, 2021.

[62] Wenhua, Q. et al. Blockchain technology: security issues, healthcare applications, challenges and future trends. *Electronics*, 12, 2023.

[63] Yeng, F. et al. Investigation into phishing risk behaviour among healthcare staff. *Information*, 13, 2022.