# A Systematic Review of Cybersecurity Issues in Healthcare IT: Threats and Solutions

AFEES OLANREWAJU AKINADE[1], PETER ADEYEMO ADEPOJU[2], ADEBIMPE BOLATITO IGE[3], ADEOYE IDOWU AFOLABI[4]
[1]*Independent Researcher, USA*
[2]*Independent Researcher, United Kingdom*
[3]*Independent Researcher, Canada*
[4]*CISCO, Nigeria*

***Abstract-*** ***This systematic review explores the intricate landscape of cybersecurity threats and solutions within healthcare IT, emphasizing the escalating cyber threats such as malware, ransomware, phishing, and insider attacks that jeopardize patient safety, data privacy, and healthcare operations. Through a comprehensive analysis, the review identifies key technological solutions—including encryption, firewalls, and anomaly detection systems—and highlights the critical role of cybersecurity awareness and training for healthcare professionals. It advocates for a proactive and comprehensive cybersecurity risk management strategy, underscoring the necessity of adapting cybersecurity measures in response to rapid technological advancements in healthcare. The review calls for increased investment in cybersecurity, fostering a culture of security awareness, and collaboration across the sector to enhance resilience against evolving cyber threats, ultimately ensuring the protection of healthcare systems and patient data in the digital era.***

***Indexed Terms-*** ***Cybersecurity in healthcare, Cyber threats, Technological solutions, Data privacy, Risk management, Healthcare IT systems***

## I. INTRODUCTION

Integrating Information Technology (IT) into healthcare has revolutionized how healthcare services are delivered, offering significant benefits such as improved patient care, enhanced data management, and increased efficiency in healthcare operations. However, this digital transformation has also introduced many cybersecurity challenges that pose significant risks to the confidentiality, integrity, and availability of sensitive health information. The importance of cybersecurity in healthcare IT cannot be overstated, as it directly impacts patient safety, privacy, and overall trust in the healthcare system (Argaw et al., 2020; Keshta & Odeh, 2021; Zarour et al., 2021).

Cyber threats in the healthcare sector have escalated in both sophistication and frequency, driven by the high value of medical data on the black market. Healthcare systems are now facing an unprecedented level of cyber threats, including ransomware attacks, data breaches, phishing schemes, and insider threats, among others (Minnaar & Herbig, 2021; Newaz, Sikder, Rahman, & Uluagac, 2021; Ryan, 2021). These incidents result in the loss of sensitive patient data and disrupt healthcare operations, leading to delays in patient care and, in extreme cases, endangering lives. The COVID-19 pandemic has further exacerbated these challenges, as the rapid shift towards telehealth and remote work has expanded the attack surface for cybercriminals (Stewart, 2023).

The problem lies in the increasing cyber threats healthcare systems face, which necessitate an urgent and robust response to protect patient information and ensure the continuity of healthcare services. Despite the growing awareness of the importance of cybersecurity in healthcare, there remains a gap in understanding the full scope of the threats and the effectiveness of various solutions in mitigating these risks.

The objectives of this systematic review encompass three key aspects. Firstly, the review aims to identify

and categorize cyber threats targeting healthcare IT systems, providing a comprehensive overview of the current cybersecurity landscape in the healthcare sector, including understanding the nature of the threats, their sources, and the vulnerabilities they exploit. Secondly, it seeks to evaluate the impact of these cyber threats on healthcare organizations and patients, focusing on the consequences of data breaches, system disruptions, and the compromise of patient confidentiality and safety. Lastly, the review intends to assess existing solutions and best practices for mitigating cybersecurity risks in healthcare IT, spanning technological, organizational, and regulatory measures. This involves analyzing the effectiveness of various cybersecurity strategies, identifying gaps in current practices, and proposing recommendations to enhance the cybersecurity posture of healthcare organizations.

By achieving these objectives, this systematic review aims to provide a comprehensive understanding of the cybersecurity issues facing healthcare IT, offering insights into effective strategies for enhancing the security and resilience of healthcare systems in the face of evolving cyber threats.

## II. BACKGROUND

### 2.1 Brief History of Cybersecurity in Healthcare

The history of cybersecurity in healthcare is intrinsically linked to the digitization of health information and the advent of electronic health records (EHRs) in the late 20th century. Initially, cybersecurity concerns were limited, as healthcare IT systems were relatively isolated, and the internet was not as integral to healthcare operations as it is today. However, as healthcare providers began to leverage digital technologies for storing patient records, sharing information across networks, and improving healthcare delivery, the need for robust cybersecurity measures became increasingly apparent (Dwivedi, Mehrotra, & Chandra, 2022; Qadri, Nauman, Zikria, Vasilakos, & Kim, 2020).

The early 2000s marked a significant turning point with the widespread adoption of EHRs, spurred by governmental initiatives and the promise of improved clinical outcomes, reduced errors, and enhanced efficiency. This digital shift, while beneficial, also exposed healthcare data to a broader range of cyber threats. Initial cybersecurity efforts focused on compliance with privacy regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, which set the first standards for protecting patient information. As cyber threats evolved, so did the cybersecurity measures, shifting from basic compliance to a more comprehensive risk management approach (Halsey, 2022; Rose, Kumar, & Kass, 2023; Thompson & Thompson, 2020; Wager, Lee, & Glaser, 2021).

### 2.2 Overview of Healthcare IT Systems and Their Critical Role in Patient Care

Healthcare IT systems encompass technologies designed to manage patient information, support clinical decision-making, and improve healthcare services. Central to these systems are EHRs, which provide a digital version of a patient's medical history and are accessible across different healthcare settings. Other components include practice management systems that automate administrative tasks, patient portals facilitating communication between patients and healthcare providers, and telehealth services enabling remote patient care.

The critical role of healthcare IT systems in patient care cannot be overstated. They enhance the accuracy and accessibility of patient data, support evidence-based treatment decisions, improve care coordination among different healthcare providers, and enable the monitoring of patient health outcomes over time. Moreover, these systems support public health initiatives by providing valuable data for research and enabling rapid response to health crises, such as pandemics.

Cyber threats in the healthcare sector have evolved significantly over the past few decades, growing in complexity and impact. Initially, threats focused primarily on unauthorized access to patient data for financial gain. However, today's cyber threats are diverse and include ransomware attacks that encrypt critical data and disrupt healthcare operations, phishing scams targeting healthcare employees to steal credentials, and advanced persistent threats (APTs) aimed at exfiltrating sensitive research data or intellectual property (Argaw et al., 2020; Tully, Selzer, Phillips, O'Connor, & Dameff, 2020).

Several factors, including the increasing value of healthcare data, the widespread adoption of digital healthcare technologies, and the interconnectedness of healthcare IT systems, have influenced the evolution of these threats. Healthcare data, which includes personal, financial, and medical information, is highly valuable on the black market, making it a prime target for cybercriminals. Additionally, the healthcare sector's complexity, often outdated IT infrastructure and a lack of cybersecurity expertise have made it more vulnerable to attacks (Rawat et al., 2022; Swasey, 2020). Moreover, the COVID-19 pandemic has accelerated the digitization of healthcare services and increased the sector's exposure to cyber threats. The rapid expansion of telehealth services and remote work has introduced new vulnerabilities and expanded the attack surface for cybercriminals, highlighting the need for enhanced cybersecurity measures in the healthcare sector (Amankwah-Amoah, Khan, Wood, & Knight, 2021; Kaiser, Wiens, & Schultmann, 2021).

## III. CYBERSECURITY THREATS IN HEALTHCARE IT

### 3.1 Classification of Cybersecurity Threats

The cybersecurity threats facing healthcare IT systems can be broadly classified into several categories, each with its characteristics and implications for healthcare data security.

i. Malware and Ransomware: Malicious software, including viruses, worms, and Trojans, is designed to infiltrate and damage computers or networks. Ransomware, a specific type of malware, encrypts data on the victim's system and demands payment for its release. These attacks can cripple healthcare IT systems, blocking access to critical patient data and disrupting healthcare services (Alenezi, Alabdulrazzaq, Alshaher, & Alkharang, 2020; Prasad, Rohokale, Prasad, & Rohokale, 2020; Vasani et al., 2023).

ii. Phishing: This cyber attack involves sending fraudulent emails that mimic legitimate sources to steal sensitive information, such as login credentials and financial data. Phishing campaigns often target healthcare personnel due to their access to valuable patient information (Alkhalil, Hewage, Nawaf, & Khan, 2021).

iii. Insider Threats: These threats come from individuals within the organization, such as employees, contractors, or business associates, who misuse their access to healthcare IT systems to steal or sabotage information. Insider threats can be malicious or the result of negligence.

iv. Advanced Persistent Threats (APTs): These are sophisticated, prolonged cyberattacks where attackers gain unauthorized access to a network and remain undetected for extended periods. APTs aim to steal data rather than cause immediate damage, posing significant risks to patient privacy and intellectual property (Hejase, Fayyad-Kazan, & Moukadem, 2020).

v. Distributed Denial of Service (DDoS) Attacks: These attacks aim to overwhelm healthcare IT systems with traffic, rendering them inaccessible to users and potentially disrupting critical healthcare operations (Gupta & Dahiya, 2021; Wani et al., 2021).

### 3.2 Impact of Cybersecurity Threats on Patient Safety, Data Privacy, and Healthcare Operations

The impact of cybersecurity threats on healthcare is profound and multifaceted, affecting patient safety, data privacy, and the continuity of healthcare operations.

Cyber attacks can directly threaten patient safety by disrupting healthcare IT systems, leading to delayed treatments, incorrect medication administration, or the inability to access critical patient data in emergencies. Patient data breaches compromise the confidentiality of sensitive health information, leading to privacy violations, identity theft, and financial fraud. Losing trust in healthcare providers can have long-lasting repercussions on the patient-provider relationship. Cyber attacks can cause significant operational disruptions, from shutting down critical care equipment to paralyzing entire hospital networks. The recovery process can be costly and time-consuming, diverting resources from patient care.

Recent years have seen a surge in cybersecurity breaches within the healthcare sector, with notable incidents underscoring the severity of the threat landscape.

- In 2020, a major U.S. healthcare provider suffered a ransomware attack that affected over 250 hospitals and clinics, disrupting services and forcing the cancellation of surgeries and medical

appointments (Klindienst, Ayanian, Schlegelmilch, & Akselrod, 2022; MacColl et al., 2024; Yan, Aziz, & Sharon, 2024).

- Another significant breach in 2019 involved the theft of personal information from over 20 million patients of a medical testing company, including Social Security numbers, health information, and financial data (Bommareddy, Khan, & Anand, 2022; Seh et al., 2020; Shachmurove & McCulloch, 2021).
- According to the Department of Health and Human Services, there were over 600 reported breaches of unsecured protected health information in 2021, affecting millions of individuals and highlighting the growing trend of cyber attacks in the healthcare sector (Alghamdi, 2022; Lehto, 2022).

These incidents illustrate the critical need for robust cybersecurity measures in healthcare IT to protect against the evolving threat landscape. The consequences of cyber attacks extend beyond financial loss, posing direct risks to patient safety and the integrity of healthcare systems. As cyber threats continue to advance in sophistication, the healthcare sector must prioritize implementing comprehensive cybersecurity strategies to safeguard patient information and ensure the continuity of care.

## IV. VULNERABILITIES IN HEALTHCARE IT SYSTEMS

The cybersecurity posture of healthcare IT systems is often compromised by various vulnerabilities, ranging from technological shortcomings to human factors. Understanding these vulnerabilities is crucial for developing effective defences against cyber threats.

### 4.1 Analysis of Common Vulnerabilities in Healthcare IT Infrastructure

- Outdated Systems: Many healthcare organizations rely on outdated software, and hardware vendors no longer support them. These legacy systems frequently contain unpatched vulnerabilities that cybercriminals can easily exploit. The complexity and cost of upgrading healthcare IT infrastructure often deter timely updates and replacements (Irani, Abril, Weerakkody, Omar, & Sivarajah, 2023).
- Lack of Encryption: Encryption is fundamental to protecting data in transit and at rest, yet many healthcare organizations fail to implement it consistently across all IT systems. The absence of encryption exposes patient data to interception and unauthorized access during transmission between devices and networks (Nidhya, Kumar, Maheswar, & Pavithra, 2022).
- Inadequate Access Controls: Weak access control policies can allow unauthorized access to sensitive health information. This includes insufficient authentication mechanisms, overly broad access permissions for users, and the lack of robust controls over third-party vendor access.
- Poor Network Security: Healthcare networks often encompass many devices and systems, making them challenging to secure. Inadequate firewall protections, unsegmented networks, and the lack of network monitoring tools can leave healthcare IT systems vulnerable to intrusions and lateral movements by attackers.
- Medical Devices: The proliferation of connected medical devices, such as pacemakers, insulin pumps, and hospital monitoring equipment, introduces significant security challenges. These devices often lack basic cybersecurity protections, making them easy targets for cyber attacks. Compromised medical devices can lead to patient safety risks and serve as entry points into broader healthcare networks (Hassija, Chamola, Bajpai, & Zeadally, 2021).
- Electronic Health Records (EHRs): EHRs contain comprehensive patient information, making them highly valuable targets for cybercriminals. Securing EHRs is challenging due to the need for widespread access by healthcare providers, the complexity of integrating EHR systems with other healthcare IT infrastructure, and regulatory compliance requirements. Ensuring the confidentiality, integrity, and availability of EHRs requires continuous vigilance and sophisticated security measures (Shah & Khan, 2020).

### 4.2 The Role of Human Error and Insider Threats

In healthcare cybersecurity, the role of human error and insider threats cannot be underestimated. Despite the implementation of robust cybersecurity measures, human error remains a significant vulnerability. This encompasses a range of mistakes, from misconfiguring systems and using weak passwords to

falling victim to phishing attacks. To mitigate these risks, training and awareness programs are crucial. However, it is acknowledged that human error can never be entirely eliminated from the equation.

Simultaneously, insider threats, whether arising from malicious intent or negligence, present a substantial challenge to the security of healthcare IT systems. Malicious insiders may aim to steal sensitive information or sabotage systems. In contrast, negligent insiders may inadvertently expose these systems to cyber threats through careless actions. The complexity lies in detecting and mitigating insider threats without unduly hindering the access and functionality required for healthcare operations to function efficiently and effectively.

Addressing the vulnerabilities in healthcare IT systems requires a multifaceted approach that includes upgrading and securing technology, implementing comprehensive security policies, and fostering a culture of cybersecurity awareness among all stakeholders. As healthcare continues to embrace digital innovation, the importance of robust cybersecurity measures to protect against evolving threats cannot be overstated.

## V. LEGISLATIVE AND REGULATORY FRAMEWORK

The legislative and regulatory framework governing cybersecurity in healthcare is designed to protect patient information and ensure the integrity and security of healthcare IT systems. Key regulations and standards have been established globally to set minimum requirements for cybersecurity practices within the healthcare sector.

### 5.1 Overview of Key Regulations and Standards Governing Cybersecurity in Healthcare

- Health Insurance Portability and Accountability Act (HIPAA): In the United States, HIPAA sets the standard for protecting sensitive patient data. Any organization that deals with protected health information (PHI) must ensure that all the required physical, network, and process security measures are in place and followed. HIPAA's Security Rule specifically focuses on electronic protected health information (e-PHI) and outlines administrative, physical, and technical safeguards to ensure its confidentiality, integrity, and availability (McNett, 2020).
- General Data Protection Regulation (GDPR): The GDPR is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas. While not healthcare-specific, GDPR has significant implications for healthcare organizations that process the personal data of individuals in the EU, including patient health information, by setting strict data protection standards and imposing heavy penalties for non-compliance (Laurer & Seidl, 2021).
- Other Relevant Regulations and Standards: Various countries and regions have healthcare data protection regulations, such as the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada and the Data Protection Act in the UK. Additionally, cybersecurity frameworks like the NIST Cybersecurity Framework provide guidelines healthcare organizations can follow to manage and reduce cybersecurity risk.

While the existing legislative and regulatory frameworks provide a foundation for cybersecurity in healthcare, there are several challenges and gaps in adequately addressing current and emerging cyber threats. Cyber threats are evolving at a pace that often outstrips the ability of regulatory frameworks to adapt. The time required to amend laws and regulations means that they may not always address the latest threats or technological advancements in healthcare IT. Geographic boundaries do not confine cyber threats, yet regulations are. This disparity can complicate compliance efforts for multinational healthcare organizations and hinder international cooperation in cybersecurity efforts.

Compliance with regulations such as HIPAA or GDPR is often seen as the end goal, but compliance alone does not guarantee security. The check-box approach to compliance can lead organizations to overlook vulnerabilities not explicitly covered by regulatory standards. Small and medium-sized healthcare organizations may struggle with the resources required to comply with complex regulations. This includes not only financial resources but also access to

cybersecurity expertise. Some regulations provide broad directives without detailed guidance on implementation, leaving organizations uncertain about achieving compliance effectively. This is particularly challenging when securing new technologies such as cloud services and mobile health applications.

To address these challenges, regulatory frameworks need to be more dynamic and adaptable to the changing cybersecurity landscape. This could include more frequent regulation updates, greater emphasis on risk management rather than prescriptive measures, and more effective international cooperation to address cyber threats. Additionally, guidance and support for smaller healthcare organizations in achieving compliance and securing their systems against cyber threats are crucial for enhancing the overall cybersecurity posture of the healthcare sector.

## VI. CYBERSECURITY SOLUTIONS AND BEST PRACTICES

In response to the growing cyber threats in healthcare, a robust combination of technological solutions, awareness and training programs, and best practices for cybersecurity risk management is essential for protecting healthcare IT systems and patient data. This multifaceted approach ensures a comprehensive defence against external and internal cyber threats.

### 4.1 Review of Technological Solutions

- Encryption: Encryption is crucial for protecting data at rest and in transit, making it unreadable to unauthorized users. Healthcare organizations should employ strong encryption standards for patient data and communication channels to ensure confidentiality and integrity (Sunday & Olufunminiyi, 2023).
- Firewalls: Firewalls are a barrier between secure internal networks and untrusted external networks like the internet. They help prevent unauthorized access to healthcare IT systems and can be configured to block data from suspicious sources (Kizza, 2024).
- Anomaly Detection Systems: These systems monitor network traffic and user behaviour to identify unusual patterns that may indicate a cyber attack. By leveraging machine learning and artificial intelligence, anomaly detection systems can quickly identify and mitigate potential threats before they cause significant damage.
- Multi-Factor Authentication (MFA): MFA adds a layer of security by requiring users to provide two or more verification factors to gain access to IT systems. This significantly reduces the risk of unauthorized access from stolen or compromised credentials (Mostafa et al., 2023).
- Access Controls and User Privilege Management: Implementing strict access controls and regularly reviewing user privileges ensures that individuals can only access the information necessary for their job functions. This principle of least privilege minimizes the risk of data breaches from external attacks and insider threats (Marbouh et al., 2020).

Cybersecurity awareness and training are critical components of a comprehensive cybersecurity strategy. Healthcare professionals are often the first line of defence against cyber threats, such as phishing attacks. Regular training sessions can help staff recognize and respond to cyber threats effectively, reducing the risk of successful attacks. These programs should cover topics like safe email practices, password management, identifying phishing attempts, and reporting suspected security incidents. Engaging and ongoing training programs can significantly enhance the overall security posture by fostering a culture of cybersecurity awareness within the organization.

### 4.2 Best Practices for Cybersecurity Risk Management in Healthcare Organizations

In the realm of healthcare cybersecurity, implementing effective risk management practices is paramount. First and foremost, healthcare organizations should regularly conduct comprehensive risk assessments to pinpoint vulnerabilities within their IT systems and processes. This entails evaluating the potential impact of various cyber threats and prioritizing remediation efforts based on risk levels.

Healthcare institutions must also develop and implement a well-defined cybersecurity policy to fortify their defences. This policy is the bedrock for securing healthcare IT systems by delineating staff responsibilities, establishing acceptable use policies, outlining data protection guidelines, and formulating

response plans for potential cyber incidents. Moreover, an incident response and recovery plan is crucial for minimizing the fallout of a cyber attack. Such a plan should encompass procedures for containing breaches, eradicating threats, recovering data, and facilitating communication with stakeholders, including patients, regulators, and law enforcement, when necessary (Wilkinson, 2020).

In an ever-evolving cybersecurity landscape, staying updated on the latest trends and threats is essential. Healthcare organizations must remain vigilant and well-informed to adapt their security measures effectively. Lastly, fostering collaboration and sharing information with other healthcare organizations and cybersecurity groups can provide valuable insights into emerging threats and defence strategies. Participation in healthcare cybersecurity consortia can elevate collective security knowledge and bolster resilience against cyber attacks (Bhuyan et al., 2020). Implementing these technological solutions, fostering a culture of cybersecurity awareness, and adhering to best practices for risk management can significantly reduce the vulnerability of healthcare organizations to cyber threats. As cybercriminals continue to target the healthcare sector, proactive and comprehensive cybersecurity strategies are essential for protecting patient data and ensuring the continuity of healthcare services.

## V. CHALLENGES AND FUTURE DIRECTIONS

Firstly, there must be increased investment in cybersecurity. Recognizing cybersecurity as a critical component of patient safety, allocating resources for advanced security technologies, staff training, and hiring skilled cybersecurity professionals can help alleviate financial constraints. Secondly, fostering a cybersecurity awareness and hygiene culture across all healthcare organizations is crucial. Regular training programs and awareness campaigns can mitigate the risk of human error and insider threats.

Furthermore, collaboration and information sharing with other healthcare organizations, cybersecurity agencies, and technology providers can enhance collective defence mechanisms. Sharing information about threats, vulnerabilities, and best practices can help organizations stay ahead of cybercriminals. Adopting a zero-trust architecture, where no entity inside or outside the network is trusted by default, can significantly enhance security. This approach requires strict identity verification, access controls, and continuous monitoring of network activities. Lastly, regulatory bodies must be more adaptable, updating guidelines and requirements in tandem with technological advancements to ensure that cybersecurity measures are effective and compliant.

## CONCLUSION

The systematic review of cybersecurity issues in healthcare IT has underscored the critical nature of the threats facing healthcare organizations today, ranging from malware and ransomware to phishing, insider threats, and advanced persistent threats. These cyber-threats pose significant risks to patient safety, data privacy, and the continuity of healthcare operations, highlighting the urgent need for robust cybersecurity measures.

Technological solutions such as encryption, firewalls, anomaly detection systems, and multi-factor authentication play a crucial role in securing healthcare IT systems. However, technology alone is not sufficient. The role of human factors—particularly through cybersecurity awareness and training for healthcare professionals—emerges as equally vital in mitigating risks. Best practices for cybersecurity risk management, including regular risk assessments, development and implementation of cybersecurity policies, incident response planning, and staying informed on cybersecurity trends, are fundamental components of a resilient cybersecurity posture.

The importance of adopting a proactive and comprehensive healthcare cybersecurity approach cannot be overstated. This entails deploying advanced technological defences, fostering a culture of security awareness throughout the organization, and ensuring that cybersecurity measures evolve with emerging healthcare IT trends. As healthcare continues to advance technologically, with innovations such as telehealth, IoT devices in patient care, and AI-driven diagnostics becoming more prevalent, the strategies for cybersecurity must also evolve. This evolution requires continuous adaptation, collaboration across

the healthcare sector, and engagement with regulatory bodies to effectively address the dynamic nature of cyber threats.

In conclusion, healthcare cybersecurity's future lies in healthcare organizations' ability to anticipate, respond to, and mitigate cyber threats through a holistic and adaptive approach. Embracing the evolving landscape of healthcare IT with a forward-looking cybersecurity strategy is essential for protecting the integrity of healthcare systems and the privacy and safety of patient data in the digital age.

REFERENCES


[1] Alenezi, M. N., Alabdulrazzaq, H., Alshaher, A. A., & Alkharang, M. M. (2020). Evolution of malware threats and techniques: A review. *International journal of communication networks and information security, 12*(3), 326-337.

[2] Alghamdi, A. (2022). *Cybersecurity threats to Healthcare Sectors during COVID-19.* Paper presented at the 2022 2nd International Conference on Computing and Information Technology (ICCIT).

[3] Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3*, 563060.

[4] Amankwah-Amoah, J., Khan, Z., Wood, G., & Knight, G. (2021). COVID-19 and digitalization: The great acceleration. *Journal of business research, 136*, 602-611.

[5] Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., . . . Eshaya-Chauvin, B. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC medical informatics and decision making, 20*, 1-10.

[6] Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., . . . Dasgupta, D. (2020). Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. *Journal of medical systems, 44*, 1-9.

[7] Bommareddy, S., Khan, J. A., & Anand, R. (2022). A review on healthcare data privacy and security. *Networking Technologies in Smart Healthcare*, 165-187.

[8] Dwivedi, R., Mehrotra, D., & Chandra, S. (2022). Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review. *Journal of oral biology and craniofacial research, 12*(2), 302-318.

[9] Gupta, B. B., & Dahiya, A. (2021). *Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges and Countermeasures*: CRC press.

[10] Halsey, M. N. (2022). A Cybersecurity Assessment of Health Data Ecosystems.

[11] Hassija, V., Chamola, V., Bajpai, B. C., & Zeadally, S. (2021). Security issues in implantable medical devices: Fact or fiction? *Sustainable Cities and Society, 66*, 102552.

[12] Hejase, H. J., Fayyad-Kazan, H. F., & Moukadem, I. (2020). Advanced persistent threats (apt): an awareness review. *Journal of Economics and Economic Education Research, 21*(6), 1-8.

[13] Irani, Z., Abril, R. M., Weerakkody, V., Omar, A., & Sivarajah, U. (2023). The impact of legacy systems on digital transformation in European public administration: Lesson learned from a multi case analysis. *Government Information Quarterly, 40*(1), 101784.

[14] Kaiser, F. K., Wiens, M., & Schultmann, F. (2021). Use of digital healthcare solutions for care delivery during a pandemic-chances and (cyber) risks referring to the example of the COVID-19 pandemic. *Health and Technology, 11*, 1125-1137.

[15] Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal, 22*(2), 177-183.

[16] Kizza, J. M. (2024). Firewalls. In *Guide to Computer Network Security* (pp. 265-294): Springer.

[17] Klindienst, J., Ayanian, S., Schlegelmilch, J., & Akselrod, H. (2022). Preparing for compounding

crises: Staff shortages and cyber-attack vulnerability in the era of COVID-19. *Journal of Business Continuity & Emergency Planning*, *16*(2), 103-120.

[18] Laurer, M., & Seidl, T. (2021). Regulating the European data-driven economy: A case study on the general data protection regulation. *Policy & Internet*, *13*(2), 257-277.

[19] Lehto, M. (2022). Cyber-attacks against critical infrastructure. In *Cyber Security: Critical Infrastructure Protection* (pp. 3-42): Springer.

[20] MacColl, J., Hüsch, P., Mott, G., Sullivan, J., Nurse, J. R., Turner, S., & Pattnaik, N. (2024). Ransomware: Victim Insights on Harms to Individuals, Organisations and Society.

[21] Marbouh, D., Abbasi, T., Maasmi, F., Omar, I. A., Debe, M. S., Salah, K., . . . Ellahham, S. (2020). Blockchain for COVID-19: review, opportunities, and a trusted tracking system. *Arabian journal for science and engineering*, *45*, 9895-9911.

[22] McNett, M. (2020). Protecting the data: Security and privacy. In *Data for Nurses* (pp. 87-99): Elsevier.

[23] Minnaar, A., & Herbig, F. J. (2021). 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.

[24] Mostafa, A. M., Ezz, M., Elbashir, M. K., Alruily, M., Hamouda, E., Alsarhani, M., & Said, W. (2023). Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication. *Applied Sciences*, *13*(19), 10871.

[25] Newaz, A. I., Sikder, A. K., Rahman, M. A., & Uluagac, A. S. (2021). A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. *ACM Transactions on Computing for Healthcare*, *2*(3), 1-44.

[26] Nidhya, R., Kumar, M., Maheswar, R., & Pavithra, D. (2022). Security and privacy issues in smart healthcare system using internet of things. *IoT-Enabled Smart Healthcare Systems, Services and Applications*, 63-85.

[27] Prasad, R., Rohokale, V., Prasad, R., & Rohokale, V. (2020). Malware. *Cyber Security: The Lifeline of Information and Communication Technology*, 67-81.

[28] Qadri, Y. A., Nauman, A., Zikria, Y. B., Vasilakos, A. V., & Kim, S. W. (2020). The future of healthcare internet of things: a survey of emerging technologies. *IEEE Communications Surveys & Tutorials*, *22*(2), 1121-1167.

[29] Rawat, R., Garg, B., Mahor, V., Telang, S., Pachlasiya, K., & Chouhan, M. (2022). Organ trafficking on the dark web—the data security and privacy concern in healthcare systems. *Internet of Healthcare Things: Machine Learning for Security and Privacy*, 189-216.

[30] Rose, R. V., Kumar, A., & Kass, J. S. (2023). Protecting privacy: Health Insurance Portability and Accountability Act of 1996, Twenty-First Century Cures Act, and social media. *Neurologic Clinics*, *41*(3), 513-522.

[31] Ryan, M. (2021). *Ransomware Revolution: The Rise of a Prodigious Cyber Threat*: Springer.

[32] Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020). *Healthcare data breaches: insights and implications.* Paper presented at the Healthcare.

[33] Shachmurove, N. C., & McCulloch, W. (2021). Health care companies face financial strain from data breaches. *American Bankruptcy Institute Journal*, *40*(8), 20-52.

[34] Shah, S. M., & Khan, R. A. (2020). Secondary use of electronic health record: Opportunities and challenges. *IEEE access*, *8*, 136947-136965.

[35] Stewart, H. (2023). Digital transformation security challenges. *Journal of Computer Information Systems*, *63*(4), 919-936.

[36] Sunday, A. E., & Olufunminiyi, O. E. (2023). An Efficient Data Protection for Cloud Storage Through Encryption. *International Journal of Advanced Networking and Applications*, *14*(5), 5609-5618.

[37] Swasey, K. (2020). Insufficient healthcare cybersecurity invites ransomware attacks and sale of phi on the dark web. *Center for*

*Anticipatory Intelligence Student Research Reports*.

[38] Thompson, E. C., & Thompson, E. C. (2020). Hipaa security rule and cybersecurity operations. *Designing a HIPAA-Compliant Security Operations Center: A Guide to Detecting and Responding to Healthcare Breaches and Events*, 23-36.

[39] Tully, J., Selzer, J., Phillips, J. P., O'Connor, P., & Dameff, C. (2020). Healthcare challenges in the era of cybersecurity. *Health security, 18*(3), 228-231.

[40] Vasani, V., Bairwa, A. K., Joshi, S., Pljonkin, A., Kaur, M., & Amoon, M. (2023). Comprehensive Analysis of Advanced Techniques and Vital Tools for Detecting Malware Intrusion. *Electronics, 12*(20), 4299.

[41] Wager, K. A., Lee, F. W., & Glaser, J. P. (2021). *Health care information systems: a practical approach for health care management*: John Wiley & Sons.

[42] Wani, S., Imthiyas, M., Almohamedh, H., Alhamed, K. M., Almotairi, S., & Gulzar, Y. (2021). Distributed denial of service (DDoS) mitigation using blockchain—A comprehensive insight. *Symmetry, 13*(2), 227.

[43] Wilkinson, I. C. (2020). *Cybersecurity using risk management strategies of US Government health organizations.* Walden University,

[44] Yan, A. M. M. F. Y., Aziz, Y. N. A., & Sharon, S. N. G. (2024). *Check for updates Modus Operandi, Factors, Implications and Governance of Ransomware Attacks on Transportation Systems.* Paper presented at the Proceedings of the 12th UUM International Legal Conference 2023 (UUMILC 2023).

[45] Zarour, M., Alenezi, M., Ansari, M. T. J., Pandey, A. K., Ahmad, M., Agrawal, A., . . . Khan, R. A. (2021). Ensuring data integrity of healthcare information in the era of digital health. *Healthcare Technology Letters, 8*(3), 66-77.