World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Review Article)

Check for updates

Navigating Cyber Threats in Health Information Systems: Safeguarding Patient and Clinical Data

Omowunmi Folashayo Makinde *

Department of Information Systems Security, University of the Cumberlands, Williamsburg, KY, United States of America.

World Journal of Advanced Research and Reviews, 2025, 28(01), 1290-1300

Publication history: Received on 10 September 2025; revised on 15 October 2025; accepted on 18 October 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.28.1.3566

Abstract

Healthcare organizations today face unprecedented challenges in protecting sensitive patient information from increasingly sophisticated cyber threats. The digital transformation of healthcare has brought remarkable benefits in terms of efficiency and patient care, but it has also created new vulnerabilities that malicious actors are eager to exploit. This study examines the current landscape of cybersecurity threats facing health information systems and explores comprehensive strategies for safeguarding patient and clinical data. Through analysis of recent security incidents and evaluation of protective measures, this research identifies critical vulnerabilities in healthcare IT infrastructure and proposes practical solutions for strengthening data security. The findings reveal that successful protection of health information requires a multi-layered approach combining technical controls, staff training, policy development, and continuous monitoring. Healthcare organizations must recognize that cybersecurity is not merely an IT issue but a fundamental component of patient safety and quality care. The study emphasizes that protecting patient data requires ongoing commitment from leadership, adequate resource allocation, and a culture of security awareness throughout the organization. As cyber threats continue to evolve, healthcare providers must remain vigilant and adaptive in their security strategies to maintain patient trust and comply with regulatory requirements.

Keywords: Cybersecurity; Health Information Systems; Patient Data Protection; Clinical Data Security; Healthcare IT; Data Breach Prevention; Electronic Health Records

1. Introduction

The healthcare industry has undergone a dramatic transformation over the past two decades. What was once a paper-based system of medical records and manual processes has evolved into a complex digital ecosystem. Electronic health records, telemedicine platforms, medical devices connected to networks, and cloud-based data storage have become standard components of modern healthcare delivery. This digital revolution has brought tremendous benefits. Doctors can access patient histories instantly, specialists can collaborate across continents, and data analytics can identify treatment patterns that save lives (Stoumpos et al., 2023).

However, this same digital transformation has created a massive target for cybercriminals. Healthcare organizations now store vast amounts of sensitive information in electronic formats. Patient records contain not just medical histories but also social security numbers, insurance details, financial information, and other personal data that criminals find valuable. A single patient record can sell for hundreds of dollars on the dark web, far more than a credit card number. This economic reality has made healthcare one of the most targeted industries for cyberattacks (Seh et al., 2020).

The consequences of a healthcare data breach extend far beyond financial losses. When patient information is compromised, it can lead to identity theft, insurance fraud, and even physical harm if medical records are altered.

* Corresponding author: Omowunmi Folashayo Makinde

Healthcare organizations face regulatory penalties, lawsuits, and damage to their reputation. Most importantly, patients lose trust in the institutions responsible for their care. In some cases, cyberattacks have forced hospitals to divert ambulances, cancel surgeries, and revert to paper records, directly impacting patient safety (Dolezel et al., 2023).

The challenge facing healthcare organizations is significant. They must protect their systems against a wide range of threats, from sophisticated nation-state actors to opportunistic criminals using readily available hacking tools. At the same time, they must ensure that security measures do not impede the delivery of care. A doctor treating a patient in an emergency cannot wait for multiple authentication steps or navigate complex security protocols. The balance between security and accessibility is delicate and requires careful planning (Wasserman & Wasserman, 2022).

This study examines the current state of cybersecurity in healthcare, identifies the most pressing threats, and explores strategies for protecting patient and clinical data. The goal is to provide healthcare organizations with practical insights they can use to strengthen their security posture while maintaining the efficiency and accessibility that modern healthcare demands.

1.1. The Growing Threat Landscape

Cyberattacks on healthcare organizations have increased dramatically in recent years. Hospitals, clinics, insurance companies, and pharmaceutical firms all report rising numbers of security incidents. The attacks come in many forms. Ransomware attacks encrypt critical data and demand payment for its release. Phishing schemes trick employees into revealing passwords or downloading malware. Insider threats involve employees or contractors who misuse their access to steal or compromise data. Advanced persistent threats involve sophisticated attackers who infiltrate networks and remain undetected for months, slowly gathering information (Neprash et al., 2022).

The healthcare sector faces unique vulnerabilities that make it particularly attractive to attackers. Many healthcare organizations operate with limited IT budgets and struggle to keep pace with security updates. Medical devices often run on outdated operating systems that cannot be easily patched without affecting their functionality. Healthcare workers need quick access to information in emergency situations, which can lead to shortcuts in security protocols. The interconnected nature of healthcare systems means that a breach at one organization can potentially affect many others (Ewoh & Vartiainen, 2024).

Recent years have seen several high-profile attacks that demonstrate the severity of the threat. Major hospital systems have been forced offline for days or weeks. Health insurance companies have reported breaches affecting millions of patients. Medical device manufacturers have discovered vulnerabilities that could allow attackers to manipulate devices remotely. These incidents have raised awareness of the problem, but many organizations still lack the resources or expertise to implement comprehensive security measures (Aldosari, 2025).

1.2. Regulatory and Compliance Requirements

Healthcare organizations operate in a heavily regulated environment. Laws and regulations governing patient data protection have been established to ensure that sensitive information is handled appropriately. These regulations impose specific requirements on how data must be stored, transmitted, and accessed. Organizations that fail to comply face significant penalties, including fines that can reach millions of dollars (Subramanian et al., 2024).

The regulatory landscape creates both challenges and opportunities for healthcare cybersecurity. On one hand, compliance requirements can be complex and resource-intensive. Organizations must implement specific technical controls, conduct regular audits, train staff, and maintain detailed documentation. On the other hand, these requirements provide a framework for building a robust security program. By following regulatory guidelines, organizations can establish baseline protections that address many common vulnerabilities (Osifowokan et al., 2025).

However, compliance alone is not sufficient. Regulations typically establish minimum standards, and determined attackers can often find ways around these basic protections. Healthcare organizations must go beyond mere compliance and adopt a proactive approach to security. This means staying informed about emerging threats, implementing advanced security technologies, and fostering a culture where everyone understands their role in protecting patient data (Wasserman & Wasserman, 2022).

1.3. The Human Factor in Healthcare Security

Technology plays a crucial role in cybersecurity, but human behavior often determines whether security measures succeed or fail. Healthcare workers are busy professionals focused on patient care. They may view security protocols as obstacles that slow them down. This attitude can lead to risky behaviors such as sharing passwords, clicking on suspicious links, or accessing patient records without proper authorization (Alhuwail et al., 2021).

Social engineering attacks exploit human psychology rather than technical vulnerabilities. An attacker might call a hospital claiming to be from the IT department and ask an employee to reveal their password. They might send an email that appears to come from a supervisor, requesting access to sensitive files. These attacks succeed because they manipulate trust and authority rather than breaking through firewalls or encryption (Hijji & Alam, 2021).

Training and awareness programs are essential for addressing the human factor in security. Healthcare workers need to understand the threats they face and how their actions can either protect or compromise patient data. However, training alone is not enough. Organizations must create a culture where security is valued and where employees feel comfortable reporting suspicious activity without fear of punishment. Security policies must be practical and aligned with the realities of healthcare work. When security measures are too burdensome, people find ways around them, creating new vulnerabilities (Ewoh & Vartiainen, 2024).

1.4. Purpose and Scope of This Study

This research aims to provide a comprehensive examination of cybersecurity challenges in healthcare and identify effective strategies for protecting patient and clinical data. The study explores the types of threats facing healthcare organizations, analyzes vulnerabilities in health information systems, and evaluates various protective measures. It considers both technical and organizational aspects of security, recognizing that effective protection requires a holistic approach. The findings are intended to help healthcare leaders, IT professionals, and policymakers understand the current threat landscape and make informed decisions about security investments. While the study acknowledges that no system can be completely secure, it demonstrates that thoughtful planning and consistent implementation of security best practices can significantly reduce risk and protect patient data from most threats.

2. Understanding Cyber Threats in Healthcare

2.1. Types of Cyber Threats

Healthcare organizations face a diverse array of cyber threats, each with different motivations, methods, and potential impacts. Understanding these threats is the first step in developing effective defenses.

- Ransomware has emerged as one of the most disruptive threats to healthcare. These attacks involve malicious software that encrypts files and systems, making them inaccessible until a ransom is paid. Healthcare organizations are particularly vulnerable to ransomware because they cannot afford extended downtime. When patient care is at stake, the pressure to pay the ransom and restore systems quickly is immense. Attackers know this and specifically target hospitals and clinics. Some ransomware groups have even threatened to publish stolen patient data if their demands are not met, adding an additional layer of extortion (Jiang et al., 2025).
- Phishing attacks remain one of the most common and effective methods for compromising healthcare systems. These attacks typically involve emails that appear legitimate but contain malicious links or attachments. An employee might receive what looks like a message from their supervisor asking them to review an attached document. When they open the attachment, malware is installed on their computer, giving attackers access to the network. Phishing attacks succeed because they exploit human trust and the fast-paced nature of healthcare work where people may not carefully scrutinize every email (Ewoh & Vartiainen, 2024).
- Insider threats pose a unique challenge because they involve individuals who already have legitimate access to systems and data. A disgruntled employee might steal patient records to sell on the black market. A curious staff member might access the medical records of a celebrity patient without authorization. A contractor with system access might inadvertently introduce malware. These threats are difficult to detect because the activity comes from authorized users and may not trigger typical security alerts (Ewoh & Vartiainen, 2024).
- Advanced persistent threats involve sophisticated attackers, often backed by nation-states or organized crime groups, who infiltrate networks and remain hidden for extended periods. These attackers move slowly and carefully, avoiding detection while they map the network, identify valuable data, and establish multiple access points. Their goal is often espionage or theft of intellectual property such as research data or pharmaceutical formulas. By the time these intrusions are discovered, attackers may have been present for months or years (Ewoh & Vartiainen, 2024).
- Distributed denial of service attacks flood systems with traffic, making them unavailable to legitimate users. While these attacks do not typically result in data theft, they can disrupt healthcare operations and prevent

access to critical systems. In some cases, denial of service attacks are used as a distraction while other attacks are carried out (Ewoh & Vartiainen, 2024).

- Medical device vulnerabilities represent an emerging threat as more devices become connected to networks. Insulin pumps, pacemakers, imaging equipment, and monitoring systems all contain software that may have security flaws. Attackers who exploit these vulnerabilities could potentially harm patients directly by manipulating device functions. Even if direct harm is not the goal, compromised medical devices can serve as entry points into hospital networks (Ewoh & Vartiainen, 2024).

2.2. Vulnerabilities in Health Information Systems

Healthcare IT environments are complex and often contain numerous vulnerabilities that attackers can exploit. Understanding these weaknesses is essential for developing effective security strategies. Legacy systems are a significant problem in healthcare. Many organizations continue to use older software and hardware because replacing them is expensive and disruptive. These legacy systems often run outdated operating systems that no longer receive security updates. They may not support modern encryption or authentication methods. Yet they remain in use because they perform critical functions and are deeply integrated into workflows. These systems create security gaps that are difficult to address without major investments in modernization (Wasserman & Wasserman, 2022).

The interconnected nature of healthcare systems creates additional vulnerabilities. A typical hospital network includes electronic health record systems, billing systems, laboratory information systems, radiology systems, pharmacy systems, and numerous other applications. These systems need to share data to support coordinated patient care. However, each connection represents a potential pathway for attackers. If one system is compromised, attackers may be able to move laterally through the network, accessing other systems and data (Ewoh & Vartiainen, 2024).

Medical devices present unique security challenges. Many devices were designed with functionality and safety as the primary concerns, with security as an afterthought. They may have hardcoded passwords that cannot be changed, lack encryption for data transmission, or run on operating systems that cannot be patched without voiding warranties or regulatory approvals. As these devices become networked, their vulnerabilities become network vulnerabilities (Bracciale et al., 2023).

Third-party vendors and business associates create additional risk. Healthcare organizations work with numerous external partners who may have access to their systems or data. A billing company might have access to patient information. A cloud service provider might host electronic health records. An IT contractor might have administrative access to networks. Each of these relationships creates potential vulnerabilities. If a vendor has weak security practices, attackers might compromise the vendor and use that access to reach healthcare organizations (He et al., 2021).

Inadequate access controls allow users to access more data than necessary for their jobs. A receptionist might have access to complete medical records when they only need demographic information. A billing clerk might be able to view clinical notes. These excessive permissions increase the risk of both accidental and intentional data exposure. Implementing proper access controls requires careful analysis of job functions and ongoing monitoring to ensure permissions remain appropriate as roles change (Aldosari, 2025).

Poor network segmentation means that once attackers gain access to any part of a network, they can potentially reach all parts. Critical systems should be isolated from general networks, with strict controls on what traffic can pass between segments. However, many healthcare networks lack this segmentation, allowing attackers who compromise a single workstation to potentially access servers containing sensitive data (He et al., 2021).

Insufficient monitoring and logging make it difficult to detect attacks in progress or investigate incidents after they occur. Many healthcare organizations lack the tools or expertise to analyze network traffic, system logs, and user activity for signs of compromise. Attackers can operate undetected for extended periods because no one is watching for suspicious behavior (Pool et al., 2024).

2.3. The Impact of Data Breaches

When healthcare data is compromised, the consequences extend far beyond the immediate incident. Understanding these impacts helps justify the investments needed for robust security programs. Patient harm is the most serious potential consequence. If medical records are altered, patients might receive incorrect treatments. If systems are unavailable due to an attack, care may be delayed. Patients whose information is stolen face risks of identity theft and fraud that can persist for years. The psychological impact of knowing that intimate health information has been exposed can be significant (Aldosari, 2025).

Financial costs from data breaches are substantial. Organizations face expenses for incident response, forensic investigation, legal fees, regulatory fines, and settlements of lawsuits. They must provide credit monitoring services to affected patients. They may need to invest in new security infrastructure to prevent future incidents. Lost revenue from disrupted operations adds to the financial burden. For smaller healthcare organizations, a major breach can be financially devastating (Seh et al., 2020).

Reputational damage affects patient trust and can have long-term business implications. Patients may choose to seek care elsewhere if they do not trust an organization to protect their information. Referring physicians may send patients to other facilities. Recruiting and retaining staff becomes more difficult when an organization is known for security problems. Rebuilding trust after a breach takes years of consistent effort (Arafat et al., 2025).

Regulatory penalties can be severe. Organizations that fail to adequately protect patient data face fines and corrective action plans imposed by regulators. In serious cases, executives may face personal liability. The regulatory process itself is time-consuming and expensive, requiring extensive documentation and often resulting in mandated changes to policies and systems. Operational disruption from cyberattacks can affect patient care directly. Hospitals have been forced to divert ambulances, cancel elective procedures, and operate without access to electronic records. Staff must work longer hours using manual processes. The stress on healthcare workers during these incidents is significant and can lead to burnout and errors (Triplett, 2024).

3. Strategies for Safeguarding Patient and Clinical Data

3.1. Technical Security Controls

Effective cybersecurity requires multiple layers of technical controls that work together to prevent, detect, and respond to threats. Network security forms the foundation of technical protection. Firewalls control traffic between networks and the internet, blocking unauthorized access attempts. Intrusion detection and prevention systems monitor network traffic for suspicious patterns and can automatically block attacks. Virtual private networks encrypt communications between remote users and healthcare networks. Network segmentation divides networks into zones with different security levels, limiting how far attackers can move if they breach one area (Anwar et al., 2021).

Endpoint protection secures individual devices such as computers, tablets, and smartphones. Antivirus and anti-malware software detect and remove malicious programs. Endpoint detection and response tools provide more advanced capabilities, monitoring device behavior for signs of compromise and allowing security teams to investigate and remediate threats. Device encryption ensures that if a laptop or mobile device is lost or stolen, the data on it remains protected (Suleski et al., 2023).

Access controls ensure that users can only access the data and systems necessary for their jobs. Strong authentication methods, including multi-factor authentication, verify user identities before granting access. Role-based access control assigns permissions based on job functions rather than individual users, making it easier to manage access consistently. Regular reviews of access rights help identify and remove unnecessary permissions (Shojaei et al., 2024).

Data encryption protects information both when it is stored and when it is transmitted. Encrypted data is unreadable without the proper decryption keys, so even if attackers steal data, they cannot use it. Healthcare organizations should encrypt data on servers, backup systems, portable devices, and during transmission over networks. Encryption key management is critical, as keys must be protected as carefully as the data they secure (Sharma et al., 2024).

Patch management keeps software and systems up to date with the latest security fixes. Software vendors regularly release patches to address newly discovered vulnerabilities. Organizations must have processes to test and deploy these patches promptly. However, healthcare environments present challenges because patching may require system downtime or could affect the functionality of medical devices. A risk-based approach helps prioritize which systems to patch first (Naghib et al., 2025).

Backup and recovery systems ensure that data can be restored if it is lost or encrypted by ransomware. Regular backups should be stored securely, with at least some copies kept offline or in immutable storage that cannot be altered or deleted by attackers. Organizations must regularly test their backup and recovery procedures to ensure they work when needed (Sharma et al., 2024).

Security monitoring and incident response capabilities allow organizations to detect and respond to threats quickly. Security information and event management systems collect and analyze logs from across the IT environment, identifying patterns that might indicate an attack. Security operations centers provide dedicated teams to monitor for threats and coordinate responses. Incident response plans define roles, responsibilities, and procedures for handling security events (Naghib et al., 2025).

3.2. Administrative and Policy Controls

Technical controls must be supported by policies, procedures, and governance structures that establish expectations and guide behavior. Security policies define how the organization approaches information security. They establish requirements for password strength, acceptable use of systems, data handling, and other security-related activities. Policies should be clear, practical, and aligned with regulatory requirements. They must be communicated to all staff and regularly updated to address new threats and technologies (Umejiaku et al., 2023).

Risk assessment processes help organizations identify and prioritize security risks. Regular assessments examine systems, processes, and threats to determine where vulnerabilities exist and what the potential impacts might be. This information guides decisions about where to invest security resources for maximum benefit. Risk assessments should consider both technical and operational factors (Cremer et al., 2022).

Vendor management programs ensure that third parties who have access to systems or data maintain appropriate security standards. Organizations should assess vendor security practices before establishing relationships, include security requirements in contracts, and monitor vendor compliance over time. When vendors experience security incidents, healthcare organizations must understand how they might be affected (Ilori et al., 2024).

Incident response planning prepares organizations to handle security events effectively. Plans should define how incidents are detected, reported, assessed, contained, and resolved. They should identify who has authority to make decisions during an incident and how communication will be managed. Regular exercises and simulations help ensure that plans work and that staff know their roles (Cremer et al., 2022).

Business continuity and disaster recovery planning addresses how the organization will maintain operations during and after a significant disruption. These plans consider various scenarios, including cyberattacks, and define how critical functions will continue. They identify backup systems, alternative processes, and recovery priorities. Compliance management ensures that the organization meets regulatory requirements for data protection. This involves understanding applicable regulations, implementing required controls, maintaining documentation, and conducting audits. Compliance should be viewed as a baseline rather than a goal, with organizations striving to exceed minimum requirements (Chandra et al., 2022).

3.3. Training and Awareness Programs

Human behavior plays a critical role in security, making training and awareness essential components of any security program. Security awareness training should be provided to all staff, not just IT personnel. Training should cover common threats such as phishing, the importance of strong passwords, how to recognize suspicious activity, and what to do if a security incident is suspected. Training should be engaging and relevant to healthcare work, using examples and scenarios that resonate with healthcare professionals (Cremer et al., 2022).

Role-specific training provides more detailed instruction for staff with particular security responsibilities. IT administrators need training on secure system configuration and management. Staff who handle sensitive data need training on proper data handling procedures. Managers need training on their responsibilities for overseeing security in their departments (Clarke & Martin, 2023).

Simulated phishing exercises test whether staff can recognize and avoid phishing attempts. These exercises send fake phishing emails to employees and track who clicks on links or provides credentials. The goal is not to punish those who fall for the simulations but to identify areas where additional training is needed and to reinforce lessons about vigilance (Rizzoni et al., 2022).

Security champions programs identify enthusiastic staff members who can promote security awareness in their departments. These champions receive additional training and serve as resources for their colleagues. They help bridge the gap between security teams and clinical staff, translating security concepts into practical guidance. Ongoing communication keeps security top of mind. Regular newsletters, posters, screen savers, and other communications remind staff about security practices and inform them about current threats. Communication should be frequent enough to maintain awareness but not so constant that it becomes background noise that people ignore (Clarke & Martin, 2023).

3.4. Organizational Culture and Leadership

Creating a secure environment requires more than policies and technology. It requires a culture where security is valued and supported at all levels of the organization. Leadership commitment is essential. When executives and board members prioritize security, allocate resources, and hold people accountable, the rest of the organization takes notice. Leaders should regularly discuss security in meetings, ask questions about security posture, and ensure that security considerations are part of strategic planning (Ewoh & Vartiainen, 2024).

Security should be integrated into organizational processes rather than treated as a separate function. When new systems are implemented, security should be considered from the beginning. When workflows are designed, security implications should be evaluated. When performance is measured, security metrics should be included (Coutinho et al., 2023).

A just culture approach to security incidents encourages reporting and learning rather than blame. Staff should feel comfortable reporting mistakes or suspicious activity without fear of punishment. When incidents occur, the focus should be on understanding what happened and how to prevent similar incidents rather than on finding someone to blame. This approach leads to better reporting and more opportunities to improve security (Murray et al., 2023).

Collaboration between security teams and clinical staff is crucial. Security professionals need to understand healthcare workflows and the pressures that clinical staff face. Clinical staff need to understand security risks and the reasoning behind security measures. Regular dialogue helps both groups find solutions that protect data without unduly burdening caregivers (Clarke & Martin, 2023).

Resource allocation for security must be adequate and sustained. Cybersecurity is not a one-time project but an ongoing effort that requires continued investment. Organizations should budget for security tools, staff, training, and improvements. Security spending should be viewed as an investment in patient safety and organizational resilience rather than as an expense (Ewoh & Vartiainen, 2024).

4. Emerging Technologies and Future Considerations

4.1. Artificial Intelligence and Machine Learning

Artificial intelligence and machine learning technologies offer both opportunities and challenges for healthcare cybersecurity. On the defensive side, these technologies can analyze vast amounts of data to identify patterns that might indicate an attack. They can detect anomalies in user behavior, network traffic, or system activity that human analysts might miss. Machine learning models can adapt to new threats more quickly than traditional signature-based detection methods (Khan & Alkhathami, 2024).

However, attackers are also using artificial intelligence to make their attacks more sophisticated. AI-powered phishing campaigns can create highly personalized messages that are more likely to deceive recipients. Machine learning can help attackers identify vulnerabilities in systems or optimize their attack strategies. As both defenders and attackers adopt these technologies, the cybersecurity landscape becomes more complex (Guembe et al., 2022).

Healthcare organizations should explore how AI and machine learning can enhance their security programs while remaining aware of how these technologies might be used against them. They should also consider the security implications of AI systems used for clinical purposes, as these systems may become targets for attackers seeking to manipulate healthcare decisions (Mensah, 2022).

4.2. Cloud Computing and Data Storage

Cloud computing offers healthcare organizations scalability, flexibility, and potentially enhanced security compared to on-premises systems. Major cloud providers invest heavily in security and employ large teams of security experts. They can often provide better protection than individual healthcare organizations could achieve on their own (Mehrtak et al., 2021).

However, cloud adoption also introduces new considerations. Organizations must understand their responsibilities versus those of the cloud provider. They must ensure that data is encrypted and that access controls are properly configured. They must consider where data is stored and whether that raises regulatory or privacy concerns. They must have plans for what happens if the cloud provider experiences an outage or security incident (Cresswell et al., 2022).

Hybrid environments that combine on-premises and cloud systems create additional complexity. Data may move between environments, and security controls must be consistent across both. Organizations need clear visibility into where data resides and how it is protected regardless of location (Zandesh, 2024).

4.3. Internet of Medical Things

The proliferation of connected medical devices, often called the Internet of Medical Things, creates new security challenges. These devices collect and transmit sensitive patient data. They may be controlled remotely by healthcare providers. They often have limited security capabilities due to constraints on processing power, memory, and battery life (Svandova & Smutny, 2024).

Securing these devices requires collaboration between healthcare organizations, device manufacturers, and regulators. Manufacturers must design security into devices from the beginning rather than adding it as an afterthought. Healthcare organizations must maintain inventories of connected devices, monitor them for vulnerabilities, and segment them on networks to limit potential damage if they are compromised. Regulators must establish and enforce security standards for medical devices (Youssef, 2022).

As medical devices become more sophisticated and more connected, the potential impact of security vulnerabilities increases. Organizations must stay informed about vulnerabilities in the devices they use and have processes to address them promptly (Bracciale et al., 2023).

4.4. Telemedicine and Remote Care

The expansion of telemedicine and remote care, accelerated by recent global health events, has created new security considerations. Video consultations, remote monitoring, and digital health apps all involve transmission of sensitive health information. Patients may be using personal devices and home networks that are less secure than hospital systems (Ansarian & Baharlouei, 2023).

Healthcare organizations must ensure that telemedicine platforms use strong encryption and authentication. They must provide guidance to patients about securing their devices and networks. They must consider how to verify patient identity remotely and how to ensure that consultations are private. They must also address the security of data collected by remote monitoring devices and health apps. The convenience and accessibility of telemedicine make it an important tool for healthcare delivery. Security measures must protect patient data without making these services so difficult to use that patients avoid them (Dalloul et al., 2023).

5. Conclusion

The protection of patient and clinical data from cyber threats is one of the most pressing challenges facing healthcare organizations today. The digital transformation that has brought so many benefits to healthcare has also created vulnerabilities that malicious actors are eager to exploit. The consequences of failing to adequately protect health information extend beyond financial losses to potentially affect patient safety and erode the trust that is fundamental to the healthcare relationship.

This study has examined the complex landscape of cybersecurity threats in healthcare, from ransomware and phishing to insider threats and medical device vulnerabilities. It has explored the various weaknesses in health information systems that attackers exploit, including legacy systems, inadequate access controls, and insufficient monitoring. Most importantly, it has outlined comprehensive strategies for protecting patient and clinical data through technical controls, administrative policies, training programs, and organizational culture.

Several key themes emerge from this analysis. First, effective cybersecurity requires a multi-layered approach. No single technology or policy can provide complete protection. Organizations need multiple defensive measures that work together, so that if one layer fails, others remain in place. Second, security must be balanced with usability. Measures that are too burdensome will be circumvented, creating new vulnerabilities. Security solutions must be designed with an understanding of healthcare workflows and the pressures that healthcare workers face.

Third, the human element is critical. Technology alone cannot secure health information if people do not understand threats or follow security practices. Training, awareness, and a culture that values security are essential. Fourth, leadership commitment makes the difference between security programs that succeed and those that fail. When leaders prioritize security, allocate resources, and hold people accountable, organizations can build robust defenses.

Fifth, cybersecurity is not a destination but a journey. Threats evolve constantly, and defenses must evolve with them. Organizations cannot implement security measures once and consider the job done. They must continuously monitor for new threats, assess their security posture, and adapt their strategies. This requires sustained investment and ongoing attention from leadership.

Looking forward, healthcare organizations face both challenges and opportunities. Emerging technologies such as artificial intelligence, cloud computing, and connected medical devices offer new capabilities but also create new security considerations. The expansion of telemedicine and remote care extends the boundaries of healthcare networks and introduces new vulnerabilities. Organizations must stay informed about these developments and adapt their security strategies accordingly.

The regulatory environment will likely continue to evolve, with increasing expectations for data protection and potentially more severe penalties for failures. Organizations that view compliance as merely checking boxes will find themselves at risk. Those that embrace security as a core value and strive to exceed minimum requirements will be better positioned to protect patient data and maintain trust.

Collaboration and information sharing within the healthcare industry can help all organizations improve their security. When one organization experiences an attack, others can learn from that experience. Industry groups, government agencies, and security researchers all play roles in identifying threats and developing defenses. Healthcare organizations should participate in these collaborative efforts and share their own experiences to benefit the broader community.

Ultimately, protecting patient and clinical data is not just a technical challenge or a compliance requirement. It is a fundamental responsibility that healthcare organizations owe to the patients who trust them with their most sensitive information. In an era where data breaches are common and cyber threats are sophisticated, organizations must recognize that cybersecurity is integral to their mission of providing safe, high-quality care.

The path forward requires commitment, resources, and sustained effort. It requires technical expertise, thoughtful policies, engaged leadership, and a workforce that understands its role in protecting patient data. It requires balancing security with the need for healthcare workers to access information quickly in critical situations. It requires staying informed about evolving threats and continuously improving defenses.

Healthcare organizations that rise to this challenge will not only protect their patients from the harms of data breaches but will also strengthen trust, improve their operational resilience, and position themselves for success in an increasingly digital healthcare landscape. Those that fail to adequately address cybersecurity risks face not only financial and regulatory consequences but also the potential for patient harm and loss of the trust that is essential to healthcare.

The stakes are high, but the path forward is clear. By implementing comprehensive security strategies, fostering a culture of security awareness, and maintaining vigilant attention to emerging threats, healthcare organizations can navigate the complex landscape of cyber threats and fulfill their responsibility to safeguard the patient and clinical data entrusted to their care.

Compliance with ethical standards

Disclosure of conflict of interest

There is no conflict of interest to be disclosed.

Statement of Ethical Approval

This article does not contain any studies with human participants or animals performed by the author.

References

[1] Aldosari, B. (2025). Cybersecurity in healthcare: New threat to patient safety. *Cureus*. https://doi.org/10.7759/cureus.83614

[2] Alhuwail, D., Al-Jafar, E., Abdulsalam, Y., & AlDuaij, S. (2021). Information security awareness and behaviors of health care professionals at Public Health Care Facilities. *Applied Clinical Informatics*, *12*(04), 924–932. https://doi.org/10.1055/s-0041-1735527

[3] Ansarian, M., & Baharlouei, Z. (2023). Applications and challenges of telemedicine: Privacy-preservation as a case study. *Archives of Iranian Medicine*, *26*(11), 654–661. https://doi.org/10.34172/aim.2023.96

[4] Anwar, R. W., Abdullah, T., & Pastore, F. (2021). Firewall best practices for Securing Smart Healthcare Environment: A Review. *Applied Sciences*, *11*(19), 9183. https://doi.org/10.3390/app11199183

[5] Arafat, M. S., Desai, K., Hossain, M. A., Asha, A. I., & Akter, S. (2025). Cybersecurity challenges in healthcare IT: Business strategies for mitigating data breaches and Enhancing Patient Trust. *The American Journal of Engineering and Technology*, *07*(05), 15–38. https://doi.org/10.37547/tajet/volume07issue05-03

[6] Bracciale, L., Loreti, P., & Bianchi, G. (2023). Cybersecurity vulnerability analysis of medical devices purchased by National Health Services. *Scientific Reports*, *13*(1). https://doi.org/10.1038/s41598-023-45927-1

[7] Chandra, N. A., Ramli, K., Ratna, A. A., & Gunawan, T. S. (2022). Information security risk assessment using situational awareness frameworks and Application Tools. *Risks*, *10*(8), 165. https://doi.org/10.3390/risks10080165

[8] Clarke, M., & Martin, K. (2023). Managing cybersecurity risk in healthcare settings. *Healthcare Management Forum*, *37*(1), 17–20. https://doi.org/10.1177/08404704231195804

[9] Coutinho, B., Ferreira, J., Yevseyeva, I., & Basto-Fernandes, V. (2023). Integrated cybersecurity methodology and supporting tools for Healthcare Operational Information Systems. *Computers &amp; Security*, *129*, 103189. https://doi.org/10.1016/j.cose.2023.103189

[10] Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

[11] Cresswell, K., Domínguez Hernández, A., Williams, R., & Sheikh, A. (2022). Key challenges and opportunities for Cloud Technology in health care: Semistructured interview study. *JMIR Human Factors*, *9*(1). https://doi.org/10.2196/31246

[12] Dalloul, A. H., Miramirkhani, F., & Kouhalvandi, L. (2023). A review of recent innovations in Remote Health Monitoring. *Micromachines*, *14*(12), 2157. https://doi.org/10.3390/mi14122157

[13] Dolezel, D., Beauvais, B., Stigler Granados, P., Fulton, L., & Kruse, C. S. (2023). Effects of internal and external factors on hospital data breaches: Quantitative study. *Journal of Medical Internet Research*, *25*. https://doi.org/10.2196/51471

[14] Ewoh, P., & Vartiainen, T. (2024). Vulnerability to cyberattacks and sociotechnical solutions for Health Care Systems: Systematic review. *Journal of Medical Internet Research*, *26*. https://doi.org/10.2196/46904

[15] Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of AI-Driven Cyberattacks: A Review. *Applied Artificial Intelligence*, *36*(1). https://doi.org/10.1080/08839514.2022.2037254

[16] He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health Care Cybersecurity challenges and solutions under the climate of covid-19: Scoping review. *Journal of Medical Internet Research*, *23*(4). https://doi.org/10.2196/21747

[17] Hijji, M., & Alam, G. (2021). A multivocal literature review on growing social engineering based Cyber-attacks/threats during the COVID-19 pandemic: Challenges and prospective solutions. *IEEE Access*, *9*, 7152–7169. https://doi.org/10.1109/access.2020.3048839

[18] Ilori, O., Nwosu, N. T., & Naiho, H. N. N. (2024). Third-party vendor risks in IT security: A comprehensive audit review and mitigation strategies. *World Journal of Advanced Research and Reviews*, *22*(3), 213–224. https://doi.org/10.30574/wjarr.2024.22.3.1727

[19] Jiang, J. X., Ross, J. S., & Bai, G. (2025). Ransomware attacks and data breaches in US Health Care Systems. *JAMA Network Open*, *8*(5). https://doi.org/10.1001/jamanetworkopen.2025.10180

[20] Khan, M. M., & Alkhathami, M. (2024). Anomaly detection in IOT-based healthcare: Machine Learning for Enhanced Security. *Scientific Reports*, *14*(1). https://doi.org/10.1038/s41598-024-56126-x

[21] Mehrtak, M., SeyedAlinaghi, S., MohsseniPour, M., Noori, T., Karimi, A., Shamsabadi, A., Heydari, M., Barzegary, A., Mirzapour, P., Soleymanzadeh, M., Vahedi, F., Mehraeen, E., & Dadras, O. (2021). Security challenges and solutions using healthcare cloud computing. *Journal of Medicine and Life*, *14*(4), 448–461. https://doi.org/10.25122/jml-2021-0100

[22] Mensah, F. (2022). Ai in Healthcare Cybersecurity: Balancing the risks and benefits of Intelligent Defense Mechanisms. *International Journal of Novel Research and Development*, *7*(6). https://doi.org/10.56975/ijnrd.v7i6.305874

[23] Murray, J. S., Lee, J., Larson, S., Range, A., Scott, D., & Clifford, J. (2023). Requirements for implementing a ‘just culture’ within Healthcare Organisations: An integrative review. *BMJ Open Quality*, *12*(2). https://doi.org/10.1136/bmjoq-2022-002237

[24] Naghib, A., Gharehchopogh, F. S., & Zamanifar, A. (2025). A comprehensive and systematic literature review on intrusion detection systems in the Internet of Medical Things: Current status, Challenges, and opportunities. *Artificial Intelligence Review*, *58*(4). https://doi.org/10.1007/s10462-024-11101-w

[25] Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z., & Nikpay, S. S. (2022). Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021. *JAMA Health Forum*, *3*(12). https://doi.org/10.1001/jamahealthforum.2022.4873

[26] Osifowokan, A. S., Ahmed, Z., Adukpo, T. K., & Mensah, N. (2025). Enhancing data compliance in the United States healthcare system: Addressing challenges in HIPAA and Hitech Act Implementation. *EPRA International Journal of Multidisciplinary Research (IJMR)*, 830–837. https://doi.org/10.36713/epra21263

[27] Pool, J., Akhlaghpour, S., Fatehi, F., & Burton-Jones, A. (2024). A systematic analysis of failures in protecting personal health data: A scoping review. *International Journal of Information Management*, *74*, 102719. https://doi.org/10.1016/j.ijinfomgt.2023.102719

[28] Rizzoni, F., Magalini, S., Casaroli, A., Mari, P., Dixon, M., & Coventry, L. (2022). Phishing simulation exercise in a large hospital: A case study. *DIGITAL HEALTH*, *8*, 205520762210817. https://doi.org/10.1177/20552076221081716

[29] Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020). Healthcare data breaches: Insights and implications. *Healthcare*, *8*(2), 133. https://doi.org/10.3390/healthcare8020133

[30] Sharma, D. P., Habibi Lashkari, A., & Parizadeh, M. (2024). Healthcare System and Infra-Security. *Progress in IS*, 97–120. https://doi.org/10.1007/978-3-031-68034-2_6

[31] Shojaei, P., Vlahu-Gjorgievska, E., & Chow, Y.-W. (2024). Security and privacy of technologies in Health Information Systems: A systematic literature review. *Computers*, *13*(2), 41. https://doi.org/10.3390/computers13020041

[32] Stoumpos, A. I., Kitsios, F., & Talias, M. A. (2023). Digital Transformation in Healthcare: Technology Acceptance and its applications. *International Journal of Environmental Research and Public Health*, *20*(4), 3407. https://doi.org/10.3390/ijerph20043407

[33] Subramanian, H., Sengupta, A., & Xu, Y. (2024). Patient health record protection beyond the Health Insurance Portability and Accountability Act: Mixed Methods Study. *Journal of Medical Internet Research*, *26*. https://doi.org/10.2196/59674

[34] Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the internet of healthcare things. *DIGITAL HEALTH*, *9*. https://doi.org/10.1177/20552076231177144

[35] Svandova, K., & Smutny, Z. (2024). Internet of medical things security frameworks for risk assessment and management: A scoping review. *Journal of Multidisciplinary Healthcare*, *Volume 17*, 2281–2301. https://doi.org/10.2147/jmdh.s459987

[36] Triplett, W. J. (2024). Cybersecurity vulnerabilities in Healthcare: A threat to patient security. *Cybersecurity and Innovative Technology Journal*, *2*(1), 15–25. https://doi.org/10.53889/citj.v2i1.333

[37] Umejiaku, A. P., Dhakal, P., & Sheng, V. S. (2023). Balancing password security and user convenience: Exploring the potential of prompt models for password generation. *Electronics*, *12*(10), 2159. https://doi.org/10.3390/electronics12102159

[38] Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in Digital Health*, *4*. https://doi.org/10.3389/fdgth.2022.862221

[39] Youssef, A. (2022). A framework for a medical device security program at a healthcare delivery organization. *Biomedical Instrumentation &amp; Technology*, *56*(3), 92–97. https://doi.org/10.2345/0899-8205-56.3.92

[40] Zandesh, Z. (2024). Privacy, security, and legal issues in the Health Cloud: Structured Review for Taxonomy Development. *JMIR Formative Research*, *8*. https://doi.org/10.2196/38372.