International Journal of Technology and Applied Science (IJTAS)

E-ISSN: 2230-9004 ● Website: www.ijtas.com ● Email: editor@ijtas.com

Cybersecurity Threat Landscape in the US Healthcare Sector: Trends, Risks, and National Implications

Abimbola Filani[1], Nicholas Addotey[2], Jochebed Akoto Opoku[3]

[1]Department of Doctor in Information Technology (DIT), Trine University, IN, USA
[2]Montana State University, USA
[3]Department of Telecommunication Engineering, Kwame Nkrumah University of Science and Technology, Ghana
Corresponding author: Jochebed Akoto Opoku
opokujochebedakoto@gmail.com

Abstract:
The U.S. healthcare sector faces escalating cybersecurity threats that jeopardize patient safety, data privacy, and operational continuity. Rapid digital transformation, driven by electronic health records (EHRs), telehealth, and Internet of Medical Things (IoMT) devices, has expanded the attack surface, while outdated infrastructure and fragmented governance leave organizations vulnerable. This review paper investigates the evolving cybersecurity threat landscape in the United States healthcare industry, concentrating on trends, risks, threat actors, and policy implications. Healthcare companies are becoming more vulnerable to cyber threats as they undergo rapid digital transformations driven by electronic health records (EHRs), telehealth expansion, and the proliferation of Internet of Medical Things (IoMT) devices. The review takes a methodical approach, combining peer-reviewed literature, industry reports, and regulatory analyses to evaluate the nature and effect of important threats such as ransomware, phishing, insider risks, device vulnerabilities, and supply-chain attacks. The key findings show that healthcare institutions are particularly vulnerable due to antiquated infrastructure, fragmented governance, limited cybersecurity expenditures, and life-critical operational demands. Ransomware instances highlight the systemic threats created by vendor interdependence and poor cyber hygiene. The study discusses new vulnerabilities such as AI-driven attacks and quantum concerns, as well as current mitigating mechanisms like HIPAA, HITECH, NIST CSF, and FDA device advice. Implications for research, policy, and practice include the critical need for integrated cybersecurity governance, workforce development, vendor responsibility, and zero-trust architecture implementation. The assessment recommends targeted assistance for rural and marginalized providers, improved threat intelligence sharing, and additional research into predictive analytics and cross-sector resilience. Finally, safeguarding healthcare systems is more than a technical challenge; it is a national responsibility linked to patient safety and public trust.

Keywords: Healthcare Cybersecurity, Regulatory Frameworks, Ransom Attacks, Internet of Medical Things (IoMT), Zero-Trust Architecture.

1.0 INTRODUCTION

Every ransomware attack or data breach in healthcare has a human influence preceding delayed remediation, compromised patient privacy, and even life-threatening disruptions. As hospitals quickly digitize, the risk of cybersecurity failure has never been higher.

This transition is evident in the widespread adoption of electronic health records (EHRs), the expansion of telehealth services, and the growing use of network-connected medical devices (Mohammad et al., 2025). As healthcare technology evolves, systems like EHRs, remote monitoring tools, and telemedicine platforms become more interconnected. This integration increases the complexity of the IT and OT (information and operational technology) infrastructures. Each component now relies on the others to function effectively, resulting in a highly interdependent ecosystem. Recent evaluations reveal that medical gadget connectivity has increased significantly. In high-income environments, there may be 10 to 15 connected devices per patient bed (Khallaf et al., 2025). This level of connection significantly expands the attack surface of healthcare organizations. Cybersecurity is no longer solely an IT concern. It is now critical for medical safety, data privacy, operational resilience, and the stability of national infrastructure. Without adequate cybersecurity safeguards, healthcare delivery can be disrupted, patient information might be compromised, and lives may be jeopardized (Koul et al., 2025; Ahmed et al, 2025a).

In recent years, healthcare organizations have experienced a rise in data breaches, ransomware attacks, and phishing attempts. Many of these problems also affect legacy systems and associated medical devices. These attacks aren't only technological difficulties. They immediately jeopardize patient care continuity, the confidentiality of protected health information (PHI), and the overall security of the national healthcare system (Avanzi et al., 2025, Ahmed et al, 2025b). Several factors contribute to the rising vulnerability. Many organizations are at risk due to outdated legacy infrastructure and low cybersecurity expenditures. Furthermore, the sector operates within a fragmented regulatory and governance structure. The rapid pace of digital innovation frequently outpaces the adoption of adequate security safeguards. As a result, the healthcare industry's cyber-risk posture is out of sync with the sophistication and magnitude of today's threats (Carello et al., 2023). This issue presents a crucial question: how can the US healthcare sector be safeguarded in the face of increasing cyber threats, limited resources, and increasingly complex IT and OT architectures?

This research paper seeks to address that challenge by examining the existing threat landscape, developing trends, dangers, and national implications of cybersecurity in the United States healthcare industry. By focusing on the United States, the evaluation takes into account the specific regulatory, institutional, and governance backdrop of the U.S. healthcare system. In doing so, the scope is purposely limited to the United States healthcare sector, capturing the digital-health acceleration caused by the pandemic, the expansion of remote care and connected-device adoption, as well as the developing regulatory and threat environment throughout that time.

2.0 OVERVIEW OF THE U.S. HEALTHCARE CYBERSECURITY LANDSCAPE

The healthcare system in the United States is complex and unique in terms of organizational structure. It incorporates public and private enterprises, is heavily regulated, and maintains close relationships among providers, payers, suppliers, and technology vendors. Economically, the system does not adhere to a single nationalized model. Instead, it combines employer-based private insurance, government programs, non-profit and for-profit hospitals, and a wide range of supplementary services (Mondal, R., & Sameer, M., 2025). This diversified structure presents significant obstacles to cybersecurity governance. Policymakers and administrators must deal with a variety of ownership types, budgets, and regulatory frameworks. The increasing interconnectedness of digital health systems adds a new element of complication. Hospital networks, outpatient clinics, telemedicine platforms, medical device vendors, and cloud services are all part of the same digital ecosystem. A weakness in one section of the network might easily spread to others. Because many public and private entities are interconnected, the attack surface is large, and accountability for breaches is frequently ambiguous (Tabari et al., 2025).

At the same time, the healthcare sector has undergone a significant digital shift. This shift has enabled new kinds of treatment while also increasing the sector's vulnerability to cybersecurity threats. The growing use of electronic health records (EHRs) has revolutionized the way healthcare data is kept and made accessible (Mohammad et al., 2025). At the same time, many health IT systems have moved to the cloud, altering how data is maintained and shared. The fast expansion of telemedicine, particularly during the COVID-19 epidemic, has transformed how care is delivered throughout the healthcare system. The rise of the Internet of Medical Things (IoMT) has expedited this trend. Healthcare organizations can now benefit from better care coordination, remote monitoring, and enhanced data analytics. However, the same technologies create new security threats. IoMT devices include wearable sensors, infusion pumps, and remote monitoring tools. These devices push the boundaries of healthcare networks, providing more entry opportunities for attackers (Mulo et al., 2025). Many of them rely on hardware, software, and network connections that were not intended with strong cybersecurity features.

These technological and structural characteristics create cybersecurity concerns that are exclusive to the healthcare industry. First, healthcare systems provide support for life-critical operations. Even slight delays or disruptions, such as a faulty infusion pump, missed access to imaging data, or a telemedicine platform outage, can have a direct impact on patient safety and treatment results (Balogun et al., 2025). Secondly, many healthcare organizations still rely on legacy infrastructure and apps. This reliance is frequently motivated by financial restrictions, regulatory constraints, or the need to maintain continuity of treatment. According to one analysis, old systems continue to be used because changing them would disrupt clinical operations, although these systems include known security flaws (Bedi et al., 2025). Thirdly, confidentiality, integrity, and availability of patient data remain top priorities. This includes electronic health records, diagnostic pictures, genetic data, and billing records. Healthcare organizations must adhere to stringent regulatory standards, such as HIPAA in the United States, while also ensuring data accessibility for clinical workflows and interoperability (Turkstani et al., 2025).

This balance results in a persistent conflict between usefulness and security. In addition, patient care and data management involve a number of suppliers, device manufacturers, and external service providers. This extensive network heightens third-party risk and exposes the supply chain to potential attackers. Healthcare cybersecurity is more than just securing IT systems. It is about protecting patient safety, maintaining privacy, and assuring continuity of treatment (Turkstani et al., 2025, Ahmed et al, 2025c). Because multiple vendors, device manufacturers, and external service providers partake in providing care or managing data, third-party risk and supply-chain exposures are substantial. Hence, healthcare cybersecurity is not only about protecting a business’s IT assets but safeguarding patient safety, privacy, and continuity of care (Lemlouma et al., 2024).

When compared to other essential infrastructure sectors, such as finance or energy, major differences emerge, explaining why healthcare frequently lags or exhibits unusual risk patterns.
The financial services and energy sectors are often highly resourced and have sophisticated cybersecurity governance. They also have longer regulatory histories and more experience with incident response and resilience planning. As a result, these sectors have higher cybersecurity postures. While financial and energy industries confront significant cyber threats, they frequently benefit from more standardized regulatory regimes and economies of scale. Their long-term investments in cybersecurity infrastructure have also improved their ability to coordinate resilience plans (Brilhante et al., 2025).

However, healthcare continues to be very diverse. It comprises governmental and private enterprises, local clinics, large hospital systems, device manufacturers, and telemedicine providers. This heterogeneity leads to unequal cybersecurity maturity, limited budgets, and fragmented vendor ecosystems (Akram, S. 2025). Healthcare systems cannot tolerate downtime without jeopardizing patient safety. As a result, patching and maintenance procedures are occasionally postponed, leaving systems vulnerable for longer durations. These variables combine to make the healthcare industry a weaker link in national cyber resilience, although it is equally and potentially more important to society. The US healthcare cybersecurity landscape is formed by a distinct structural and digital-transformation context, susceptible to life-critical operational demands, and hampered by legacy systems, complicated vendor ecosystems, and resource restrictions. When compared to other vital sectors, healthcare demonstrates both increased susceptibility and different risk exposure, demanding tailored cybersecurity policies and governance frameworks that understand its unique characteristics (Bedi et al 2025).

3.0 MAJOR CYBERSECURITY THREATS AND TRENDS

Ransomware, phishing, insider risks, IoMT device vulnerabilities, and supply-chain exposures dominate the threat environment in the United States healthcare sector, while new capabilities (AI, deepfakes, quantum threats) are reshaping the horizon. The following is a subsection-by-subsection synthesis based on sector reports and peer-reviewed literature.

Ransomware and Data Extortion: Ransomware has become the greatest disruptive cyber threat to the healthcare industry. In recent years, attacks have progressed from simple, opportunistic infections to highly targeted operations employing double- and triple-extortion techniques. These attacks not only encrypt computers but also steal important data, threatening to reveal it unless additional payments are made. High-profile cases have demonstrated how an attack on a single vendor can destabilize the entire healthcare system. Such attacks have disrupted claims processing, pharmacy operations, and patient care procedures, revealing how intertwined and fragile the system has become (Jiang et al., 2025).

Ransomware has far-reaching operational implications. They include extended IT outages, patient diversion, delays in treatment delivery, and significant financial and reputational harm. Some examples have also included hefty ransom payments and costly system recovery efforts.

In response, healthcare companies have implemented a variety of protective methods, including secure data backups, network segmentation, incident response playbooks, and zero-trust principles (Jiang et al., 2025). However, adoption remains uneven across the industry. These advances also create significant policy issues. Should ransom payments be allowed? How can the healthcare system effectively encourage security practices among vendors and partners? Recent events show the continuous importance of solid cybersecurity practices, such as multifactor authentication and comprehensive third-party risk management (Balogun, A. Y. 2025).

Phishing and Social Engineering: Phishing remains the most common human-targeted attack vector in the healthcare industry. It is frequently used as the entry point for more serious attacks, such as credential theft, lateral movement, and ransomware deployment. A variety of factors contribute to vulnerability in hospital settings. High clinical workloads, deskless staff, and frequent use of shared credentials or remote access tools make it simpler for attackers to take advantage of human mistakes (Jiang et al., 2025).

Insider Threats and Human Error: Insider events in healthcare can include both purposeful behavior and unintended mistakes. Malicious insiders may purposefully exfiltrate protected health information (PHI), but inadvertent exposures are frequently caused by human error, such as sending emails to the incorrect recipients, leaving file sharing insecure, or misplacing devices (Tabari et al., 2025).

Although external hacking, such as credential theft and vulnerability exploitation, is responsible for many breaches, insider activity nevertheless accounts for a sizable proportion of them. Because insiders frequently have privileged access, their acts, whether intentional or unintentional, can result in widespread data exposure (Ewoh et al., 2025). Effective mitigation necessitates a combination of technological and organizational methods. These include behavioral monitoring systems with adequate privacy measures, tight least-privilege access regulations, regular access evaluations, and data loss prevention (DLP) technologies (Khallaf et al., 2025). Cultural initiatives are also vital, such as maintaining strong onboarding and offboarding protocols and offering ongoing staff training. Several breach investigations have identified misconfiguration and human mistakes as common root causes of high-impact security events (Lemlouma et al., 2024).

Internet of Medical Things (IoMT) and Medical Device Vulnerabilities: IoMT devices greatly increase the cyber-physical attack surface in healthcare contexts. Many of these devices were built for healthcare purposes rather than cybersecurity. As a result, they frequently have lengthy operational lifecycles, limited patching capabilities, and complex vendor update procedures (Mulo et al., 2025). Potential attack scenarios include firmware compromise, which changes device behavior. For example, attackers could alter dose delivery. Other vulnerabilities include exploitation of maintenance interfaces. Insecure or inadequately segregated devices can also allow lateral movement into core hospital networks. Incomplete device inventories, weak default credentials, insufficient logging, and vendor support models all contribute to delays or complications in timely patching (Cramer, P. J. 2025). To solve these issues, numerous controls are required. Network segmentation, secure provisioning, coordinated vulnerability disclosure, and increased vendor accountability are all necessary. Furthermore, coordinated vulnerability-management activities and procurement policies that mandate baseline security standards are becoming increasingly popular across the industry (Harizaj et al., 2025).

Supply Chain and Third-Party Risks: Third-party breaches are a key cause of widespread record exposure. When suppliers such as billing processors, cloud providers, or imaging service partners are compromised, the consequences might spread to several healthcare companies. This is because numerous suppliers rely on common platforms and related services (Tabari et al., 2025). Effective supply chain risk management is critical. This includes enforcing contractual security standards, continuous monitoring, regular audits, and contingency planning for temporary offline or manual operation. Recent policy trends call for increased third-party control in healthcare contracts (Avanzi et al., 2025; Opoku and Filani, 2025).

Emerging Threats: AI, Deepfakes, Quantum: Emerging technologies are altering cyber offense and defense. Attackers are increasingly using AI to generate more convincing phishing messages, automate vulnerability scanning, and accelerate exploit development. Deepfakes also introduce new concerns, such as compromising identity verification and facilitating fraud against clinicians or administrative workers (Agrawal et al., 2025). Defenders, on the other hand, can use AI to detect anomalies, look for threats, and respond to incidents automatically. Quantum computing raises long-term concerns since it has the potential to disrupt current encryption techniques such as RSA and ECC. Healthcare institutions should prepare for a post-quantum transition by identifying cryptographic assets, particularly for patient records that require long-term confidentiality (Balogun et al., 2025).

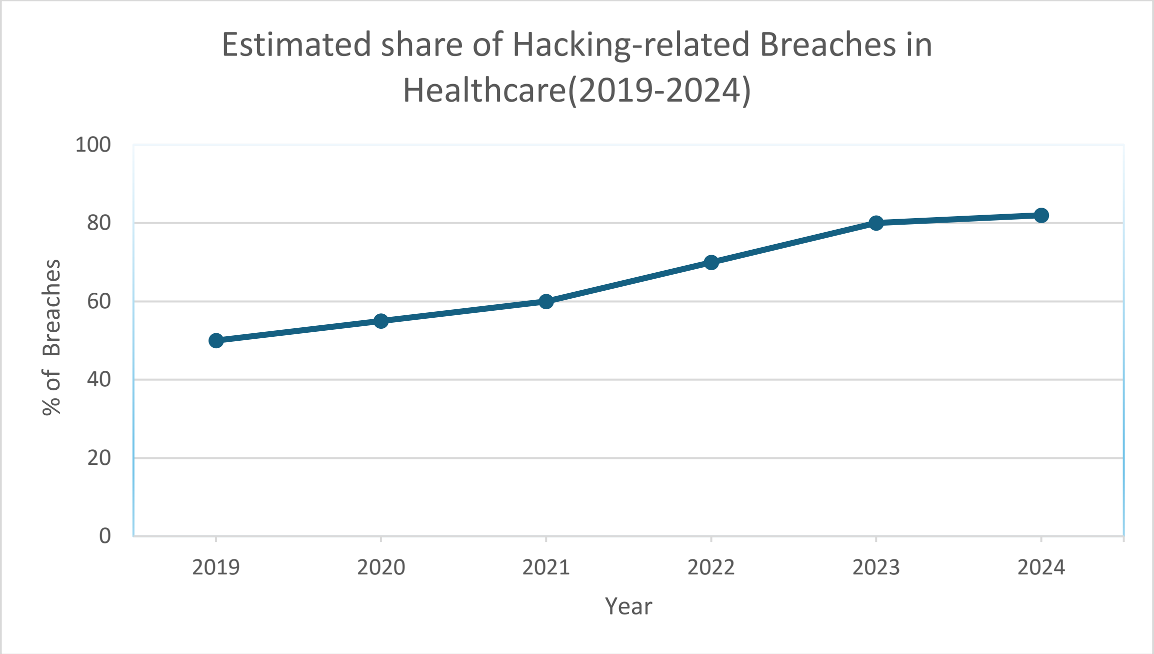

Figure 1: Annual growth in reported cybersecurity incidents in the US Healthcare sector (2019-2024, HIPAA Journal, 2025, October 26).

4. KEY VULNERABILITIES IN U.S. HEALTHCARE SYSTEMS

The cybersecurity vulnerability in the United States healthcare sector arises from a combination of technical, organizational, regulatory, human, and interconnection issues. These vulnerabilities, both structural and operational, have left many organizations unprepared for the complexity of modern cyber threats.

Technical flaws remain among the most serious drawbacks. A significant percentage of healthcare systems still use out-of-date or unsupported operating systems, such as Windows 7, or antiquated medical devices with obsolete firmware. Many of these devices cannot be patched without jeopardizing clinical operations. Hospitals sometimes postpone or skip software updates due to fears that patching could invalidate FDA approvals or interrupt mission-critical operations. According to the US Department of Health and Human Services, approximately 60% of reported healthcare breaches involve the exploitation of known but unpatched vulnerabilities, indicating a chronic technical debt in hospital IT infrastructures (Khan et al., 2025).

Organizational flaws enhance technical vulnerability. Healthcare IT departments are severely underfunded in relation to the criticality of their operations, with cybersecurity accounting for only 5-7% of total IT spending, compared to 10-15% in the financial industry. This financial imbalance restricts investment in contemporary defenses, incident response teams, and 24-hour surveillance. According to the (ISC)² Cyber Workforce Report (2023), the U.S. healthcare industry has one of the most significant cybersecurity staffing shortfalls compared to other critical infrastructure sectors. Many hospitals rely on third-party contractors for cybersecurity services, generating additional dependencies and inconsistencies in defense posture.

Policy and regulatory deficiencies persist. While the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act were instrumental in establishing data privacy standards, they were conceived before the era of ransomware, cloud computing, and AI-driven threats (Mason et al., 2024). These policies prioritize administrative compliance over proactive risk management. Furthermore, HIPAA's "addressable" implementation criteria often result in disparate security procedures among covered entities. There is no uniform federal framework that requires real-time threat reporting or standardized cybersecurity baselines for healthcare vendors. The lack of consequences for insecure older equipment and third-party misconfigurations has resulted in severe compliance gaps (Shay, D. F. 2025).

Human and cultural factors exacerbate the structural challenges. Clinicians, nurses, and administrative staff frequently prioritize patient care over digital hygiene. Time constraints and high cognitive burdens contribute to errors such as clicking on phishing emails or using shared passwords (Mondal, R., & Sameer, M., 2025). Furthermore, many healthcare institutions lack established cybersecurity awareness programs or provide training infrequently, decreasing their usefulness. Cultural reluctance to change, particularly for new security protocols that may impair clinical workflows, impedes the implementation of security best practices.

Finally, hazards associated with networked systems have emerged as a distinguishing vulnerability in today's healthcare environment. The fast digital change, driven by cloud migration, EHR interoperability, and the expansion of third-party interfaces, has exponentially increased the attack surface. While cloud-based systems are scalable and efficient, they can expose data if not correctly configured. The complexity of integrating Electronic Health Record (EHR) platforms across numerous vendors, insurers, and hospital networks has resulted in incompatible encryption standards and data-sharing procedures (Verma et al., 2025).

Together, these vulnerabilities highlight a paradox: although healthcare technology usage has increased for patient benefit, cybersecurity resilience has lagged. Addressing these flaws necessitates a comprehensive strategy that combines legislative change, labor capacity building, and technological modernization, ensuring that digital innovation in healthcare does not jeopardize patient safety or national security (Bedi et al., 2025).

5. NATIONAL IMPLICATIONS OF HEALTHCARE CYBER THREATS

The growth in cyberattacks against US healthcare businesses has far-reaching repercussions beyond individual IT breakdowns. Attacks increasingly jeopardize patient safety and public health while incurring significant economic and operational consequences. They also undermine patient trust and data privacy, raise national security concerns when nation-state actors are involved, and disproportionately damage rural and marginalized communities (Koul et al., 2025).

Cyberattacks have both short- and long-term economic and operational implications. In 2024, the average cost of a healthcare data breach was among the highest of any industry, at over USD 9.77 million per occurrence. Ransomware assaults add to the financial strain, with estimated recovery costs ranging approximately USD 2.6 million and admitted ransom payments of up to USD 4.4 million. Beyond these immediate costs, downtime exacerbates the harm by disrupting operations and causing further losses (Mohammed, et al., 2025). Apart from direct compensation and remediation, downtime causes significant financial loss. According to industry estimates, healthcare institutions lose millions of dollars per day due to downtime. These figures are likely to underestimate the broader economic ripple effects, which include vendor remediation costs, insurer losses, and higher premiums or reduced insurance coverage (Akram, 2025).

Data privacy and ethical concerns are serious and ongoing. Large breaches of protected health information (PHI), such as diagnoses, prescriptions, genetic data, and billing records, pose substantial concerns. They jeopardize patients' autonomy, confidentiality, and confidence.

High-profile vendor events have compromised hundreds of millions of documents, affecting enormous populations (Turkstani et al., 2025). These instances have generated major concerns about the use of secondary data, as well as a rising reluctance among patients to disclose sensitive information to healthcare providers. Ethical problems include whether patients provided genuine agreement for their data to be shared with third parties and whether the harm caused by breaches is evenly distributed. There are also concerns about whether present regulatory and permission structures can still ensure long-term confidentiality in an age of large, aggregated datasets (Harizaj et al., 2025).

Healthcare is specifically designated as a key infrastructure in terms of national security. Adversarial nation-states and state-sponsored entities have demonstrated a clear desire and capability to target healthcare systems. These activities jeopardize public health readiness and lower national morale. Such attacks can interrupt critical healthcare functions and extract intelligence, which has major national security consequences. Disruptions to huge interconnected systems can have severe implications. These include national claim processors, pharmaceutical supply chain management systems, and public health surveillance platforms. Such disturbances can jeopardize emergency response, impede epidemic tracking, and complicate crisis coordination (Verma et al., 2025).

Rural and underserved areas are more vulnerable to cyber disruptions. Smaller hospitals and clinics sometimes have low IT budgets, insufficient cybersecurity staff, outdated equipment, and inadequate incident response capabilities (Brilhante et al., 2025). These features make them far less resistant to attacks. When regional vendors or laboratories that serve remote areas fail, vital services like test reports, diagnostic imaging, and pharmacy fulfillment may be delayed or unavailable. This exacerbates existing health inequities. Research and industry surveys underscore these disproportionate effects, emphasizing the importance of targeted funding, shared service arrangements, and enhanced federal support to reduce resilience gaps (Khan et al., 2025).

6 CURRENT REGULATORY, POLICY, AND MITIGATION FRAMEWORKS

Several significant government regulations and guidance documents serve as the foundation for the cybersecurity posture of the United States healthcare industry. These include the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule and the Health Information Technology for Economic and Clinical Health Act (HITECH Act). They create national standards that govern the safeguarding of electronic protected health information (ePHI) by covered entities and business partners. The HIPAA Security Rule requires administrative, physical, and technical protection that ensures confidentiality, integrity, and availability of electronic protected health information (Shay, D. F. 2025). HITECH broadens the scope of liability while strengthening breach notification and enforcement mechanisms. In addition to these laws, the Food and Drug Administration (FDA) has provided cybersecurity recommendations for medical devices. This guidance requires manufacturers to include secure-by-design methods, threat modeling, patch management, and software bill of materials disclosures in their premarket submissions (Ekeneme et al., 2025).

Furthermore, the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) offers voluntary, risk-based best practices. Many healthcare companies use the framework to link their security programs with best practices (Carello et al., 2023). Together, these policies and guidelines form a multilayered compliance and defense architecture for the healthcare industry. However, this architecture confronts difficulties in keeping up with quickly changing threats.

At the federal and state levels, organizations such as the Cybersecurity and Infrastructure Security Agency (CISA) and the United States Department of Health and Human Services (HHS) have launched projects aimed primarily at healthcare cybersecurity resilience. The HHS 405(d) Program (Health Industry

Cybersecurity Practices) develops consensus-based guidelines to assist providers in implementing high-impact measures. CISA, on the other hand, provides sector-specific threat advisories, manages incident response, and fosters interagency collaboration. Furthermore, the Health Sector Coordinating Council (HSCC) functions as a public-private partnership, promoting strategic initiatives, sharing threat intelligence, and encouraging best-practice adoption among providers, payers, and vendors. Such programs promote collaboration and awareness; nevertheless, their implementation at the state and local levels varies (Ekeneme et al., 2025).

Health ISAC, for example, helps to facilitate public-private collaboration. Other cross-sector collaborations play an important role, bringing together hospitals, device makers, insurers, cybersecurity firms, and government agencies. These groups collaborate to share threat intelligence, coordinate responses, and create common tools. These systems have proven particularly useful in a variety of ways. They help to broadcast actionable indicators of compromise and exchange incident response playbooks. They also highlight the importance of smaller suppliers in collective defense. According to studies on healthcare cybersecurity, firms that participate in ISACs and similar networks shift more quickly from reactive to proactive security postures (Koul et al., 2025).

Despite the creation of this complex regulatory and collaborative ecosystem, adoption issues remain. The regulatory landscape is rather fragmented. Federal regulations, like HIPAA, intersect with state-level data-privacy legislation, varied device-security requirements, and disparate enforcement mechanisms, resulting in divergent practices among providers (Harizaj et al, 2025). Many healthcare organizations, particularly smaller or rural hospitals, cite financing constraints, workforce difficulties, and a lack of developed governance frameworks as major impediments to establishing controls. Furthermore, while many frameworks are optional (such as the NIST CSF) or non-prescriptive, the lack of universally enforced vendor security requirements (especially for medical devices) adds to sector-wide unequal readiness (Khan et al., 2025).

In assessing effectiveness, there are both encouraging signals and noticeable gaps. On the positive side, healthcare businesses that implemented basic technical protections like multifactor authentication, asset inventorying, and network segmentation experienced fewer successful breaches. Organizations that actively participated in ISACs and guidance programs also showed gains, demonstrating that practical actions can result in demonstrable improvements in cybersecurity (Akram, S. 2025). Nonetheless, serious flaws persist. Many analysts believe that regulatory laws, particularly HIPAA, are out of date in dealing with growing risks like ransomware, supply chain attacks, and AI-driven exploits. For example, device cybersecurity vulnerabilities persist as a significant issue. This is due in part to weaker regulatory enforcement and less stringent patching requirements. Rules alone are insufficient. Sustained finance, staff development, vendor accountability, and crisis preparedness are required to put policy into action. Without these, many healthcare organizations are reactive rather than resilient (Balogun, A. Y. 2025).

7. DISCUSSION AND FUTURE DIRECTIONS

The evolving cybersecurity landscape in the United States' healthcare sector presents a complex combination of technological innovation, legislative delays, and systemic vulnerabilities. As healthcare businesses undergo digital transformation, the surface area for cyber attacks has grown due to interconnected electronic health record (EHR) systems, telehealth platforms, and Internet of Medical Things (IoMT) devices (Khallaf et al., 2025). Despite significant legislative and technological advancements, the sophistication of cyberattacks, such as ransomware and supply chain exploitation, is outpacing defensive solutions. The friction between emerging threats and ongoing structural vulnerabilities highlights the vital need for integrated, adaptive security frameworks that address both technology and human elements (Ewoh et al., 2024; Carello et al., 2023).

While the healthcare sector has increased its understanding of cybersecurity concerns, a significant gap remains between awareness and action. Many institutions still use legacy systems that lack current encryption, endpoint detection, and patch management capabilities (Mohammad et al., 2025). Furthermore, healthcare businesses face the unique challenge of ensuring patient care availability while also preserving data security, creating an operational quandary that makes downtime mitigation and incident containment especially difficult (Brilhante et al., 2025).

Policy gaps remain, particularly in underexplored areas such as IoMT device vulnerabilities, the cybersecurity posture of small and rural providers, and the interdependence of healthcare and other essential sectors such as energy, finance, and logistics. Although large hospitals have made significant progress in establishing zero-trust systems and enhanced monitoring, smaller facilities frequently lack the technological capacity and finances to do so. There has been little longitudinal study into how security maturity develops in these institutions or how resource-constrained settings adapt to national cybersecurity frameworks. Furthermore, empirical research assessing the real-time impact of cyber events on patient outcomes is limited, indicating an issue that needs rapid academic attention (Akram et al., 2025).

Moving forward, research must focus on predictive threat modeling and the creation of healthcare-specific cyber maturity models capable of assessing readiness and resilience. Predictive analytics with AI and machine learning can predict attack patterns, allowing for proactive interventions rather than reactive remediation (Ewoh et al., 2024). Future research should also stress cross-disciplinary collaboration among data scientists, clinicians, and legislators to ensure cybersecurity solutions are appropriate for healthcare operations.

In terms of policy and practice implications, continued investment in cybersecurity worker training is critical. The lack of trained experts in the healthcare industry continues to impede the deployment of effective defenses. Initiatives spearheaded by the Cybersecurity and Infrastructure Security Agency (CISA) and HHS should go beyond guidance documents to include national training programs and standardized certification for healthcare IT personnel (Ekeneme et al., 2025). Furthermore, improved national threat intelligence coordination through organizations like Health-ISAC would enable faster, more coordinated responses to new threats. The implementation of zero-trust security models, which validate every device and user regardless of network location, provides a viable solution to minimize insider and lateral-movement threats (Carello et al., 2023).

Emerging technologies offer promising opportunities for progress. Artificial intelligence can improve intrusion detection systems by detecting subtle behavioral irregularities in network traffic, whereas blockchain technology can guarantee the integrity and traceability of medical data over distributed networks (Agrawal et al., 2025). Furthermore, the notion of secure-by-design, which involves building security into software and hardware development from the start, should become a statutory requirement rather than an aspirational objective. Implementing these technologies, however, would necessitate coordinated investment, revised standards to promote fair adoption across all levels of the healthcare system.

8. CONCLUSION

Cybersecurity in the United States healthcare sector has become a vital pillar of patient safety and national resilience. As digital transformation accelerates through EHRs, telehealth, and IoMT devices, the attack surface grows, exposing systemic vulnerabilities caused by antiquated infrastructure, fragmented governance, and inadequate resources. Despite existing legal frameworks such as HIPAA, HITECH, and the NIST CSF, the sector is struggling to stay up with sophisticated threats such as ransomware, supply chain breaches, and AI-driven attacks. Addressing these difficulties requires a collaborative, proactive approach that combines technological innovation, legislative reform, and workforce development.

Embracing zero-trust architectures, increasing vendor accountability, and investing in predictive analytics are all critical steps towards resilience. Finally, securing healthcare systems is more than a technical requirement; it is a strategic imperative to protect public health, ensure operational continuity, and maintain trust in the country's healthcare infrastructure.

REFERENCES:

1. Agrawal, R., Rathore, P. S., Deverajan, G. G., & Divivedi, R. R. (Eds.). (2025). *Artificial Intelligence and Cybersecurity in Healthcare*. John Wiley & Sons.
2. Ahmed, Z., Filani, A., Osifowokan, A. S., & Hutchful, N. (2025). The Impact of Data Breaches in US Healthcare: A Cost-Benefit Analysis of Prevention vs. Recovery.
3. Ahmed, Z., Osifowokan, A. S., Filani, A., & Donkor, A. A. Comprehensive analysis of cyber attacks and data breaches in the US health sector: Identifying vulnerabilities and developing proactive defense strategies.
4. Ahmed, Z., Suleiman, A. M., Filani, A., Ocansey, I. T., & Donkor, A. A. (2025). The Role of Advanced Machine Learning Algorithms in Detecting and Mitigating Cybersecurity Threats within United States Healthcare Digital Infrastructure: A Comprehensive Vulnerability Analysis. *Journal Of Engineering And Computer Sciences*, *4*(10), 218-226.
5. Akram, A., Ismail, M., Hussan, S. T., Arshad, A., Qureshi, S. I., & Iqbal, J. (2025). Securing IoT Devices in Healthcare: Challenges and Solutions. *Spectrum of Engineering Sciences*, *3*(5), 133-142.
6. Akram, S. (2025). Application of Binomial Theory in Determining the Relationship Between Importance and Impact of Risks in Hospital Projects. *Dijlah Journal of Engineering Sciences ISSN: 3078-9664, e-ISSN: 3078-9656*, *2*(3).
7. Avanzi, B., Tan, X., Taylor, G., & Wong, B. (2025). On the evolution of data breach reporting patterns and frequency in the United States: a cross-state analysis. *North American Actuarial Journal*, 1-32.
8. Balogun, A. Y. (2025). Strengthening compliance with data privacy regulations in US healthcare cybersecurity. *Asian Journal of Research in Computer Science*, *18*(1), 154-173.
9. Balogun, A. Y., Olaniyi, O. O., Olisa, A. O., Gbadebo, M. O., & Chinye, N. C. (2025). Enhancing incident response strategies in US healthcare cybersecurity. *Available at SSRN 5117971*.
10. Bedi, S., Liu, Y., Orr-Ewing, L., Dash, D., Koyejo, S., Callahan, A., ... & Shah, N. H. (2025). Testing and evaluation of health care applications of large language models: a systematic review. *Jama*.
11. Brilhante, M. F., Mendonça, S., Pestana, P., Rocha, M. L., & Santos, R. (2025). Economic impact of healthcare cyber risks. *Health and Technology*, *15*(3), 635-650.
12. Carello, M. P., Spaccamela, A. M., Querzoni, L., & Angelini, M. (2023). A Systematization of Cybersecurity Regulations, Standards and Guidelines for the Healthcare Sector. *arXiv preprint arXiv:2304.14955*.
13. Cramer, P. J. (2025). Bridging the Privacy Gap: Integrating Social Determinants of Health with HIPAA. *Annals Advance Directive*, *34*, 117.
14. Ekeneme, J., Ucheji, C., Ezekwem, C., & Chughtai, M. S. (2025). Policy Framework for Responsible AI Deployment in the National Cybersecurity Strategy. *Asian Journal of Advanced Research and Reports*, *19*(10), 183-194.
15. Ewoh, P., Vartiainen, T., & Mantere, T. (2025). Sociotechnical Cybersecurity Framework for Securing Health Care From Vulnerabilities and Cyberattacks: Scoping Review. *Journal of Medical Internet Research*, *27*, e75584.

16. Harizaj, M., Qafa, R., & Idrizi, O. (2025, May). Strategic Vulnerability Analysis of Cybersecurity Frameworks: Toward a Hybrid Model for Governance and Resilience. In *International Conference on Intelligence-Based Transformations of Technology and Business Trends* (pp. 84-96). Cham: Springer Nature Switzerland.
17. HIPAA Journal. (2025, October 26). *Healthcare data breach statistics*. https://www.hipaajournal.com/healthcare-data-breach-statistics/
18. Jiang, J. X., Ross, J. S., & Bai, G. (2025). Ransomware Attacks and Data Breaches in US Health Care Systems. *JAMA Network Open*, *8*(5), e2510180-e2510180.
19. Khallaf, F., El-Shafai, W., El-Rabaie, E. S. M., & Abd El-Samie, F. E. (2025). A Systematic Review of New Technologies for Cybersecurity Healthcare Applications: A Systematic and Comprehensive Study. *Transactions on Emerging Telecommunications Technologies*, *36*(7), e70183.
20. Khan, S., Majdalawieh, M., Kharadi, D., Verma, T., Farhin, T., & Kumar, A. (2025). From Digital Disruption to AI Revolution: The Evolution of Healthcare Transformation. *Artificial Intelligence in Medicine and Healthcare*, 31.
21. Koul, A., Gochhait, S., Hamood, S. A., & Seedi Abdulghani, H. (2025). Healthcare cyber risk and its impact on healthcare. In *Intelligent Biomedical Technologies and Applications for Healthcare 5.0* (pp. 245-253). Academic Press.
22. Lemlouma, T., Hassnaa, M., & Rachedi, A. (2024). Advancing Cybersecurity in Healthcare: Challenges and Solutions. *Frontiers in Digital Health*.
23. Mohammad, A. A. S., Alzyoud, M., Samara, E. I. M., Al-shanableh, N., Salameh, W. E. M. K. B., Alshurideh, M. T., ... & Al-Hawary, S. I. S. (2025). Electronic health records adoption: a bibliometric analysis. In *Intelligence-Driven Circular Economy: Regeneration Towards Sustainability and Social Responsibility–Volume 1* (pp. 301-314). Cham: Springer Nature Switzerland.
24. Mohammed, N., Mohammed, A. F., & Balammagary, S. (2025). Ransomware in Healthcare: Reducing Threats to Patient Care. *Journal of Cognitive Computing and Cybernetic Innovations*, *1*(2), 27-33.
25. Mondal, R., & Sameer, M. (2025). Connected healthcare system technology interventions to improve patient safety by reducing medical errors: a systematic review. *Global Journal on Quality and Safety in Healthcare*, *8*(1), 43-49.
26. Mulo, J., Liang, H., Qian, M., Biswas, M., Rawal, B., Guo, Y., & Yu, W. (2025). Navigating Challenges and Harnessing Opportunities: Deep Learning Applications in Internet of Medical Things. *Future Internet*, *17*(3), 107.
27. Opoku, Jochebed & Filani, Abimbola. (2025). Protecting Electronic Health Records (EHRs): Advances and Challenges in Data Security and Privacy. 10.5281/zenodo.17806051.
28. Shay, D. F. (2025). HIPAA Enforcement: Understanding the Process. *Journal of Health Care Compliance*, *27*(3).
29. Tabari, P., De Rosa, M., Costagliola, G., & Fuccella, V. (2025, June). Invisible Threats: Rethinking Privacy in Digital Healthcare. In *International Conference on Computational Science and Its Applications* (pp. 267-284). Cham: Springer Nature Switzerland.
30. Turkstani, H. A., Almutawah, F. N., AlZamel, N. A., Zaid, M., Alshammari, A. A. A., Algharbi, M. T., ... & Aljuwayed11, N. H. (2025). Privacy and Confidentiality in Healthcare: Best Practices for Protecting Patient Information. *J. Healthc. Sci*, *5*.
31. Verma, N., Kumar, N., Verma, C., Illés, Z., & Singh, D. (2025). A systematic review on cybersecurity of robotic systems: vulnerabilities trends, threats, attacks, challenges, and proposed framework: N. Verma et al. *International Journal of Information Security*, *24*(3), 127.