Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2025): 8.619 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 12 | Issue: 11 | November 2025 -Peer-Reviewed Journal

AI-POWERED CYBER RISK PREDICTION MODELS FOR US HEALTHCARE INSTITUTIONS

Barbara Aryeley Aryee[1], Kwadwo Adu Agyemang[2]
[1] *Department of Information Systems, East Tennessee State University (ETSU), Johnson City, TN, USA*
[2] *Department of Information Systems, East Tennessee State University (ETSU), Johnson City, TN, USA*

Article DOI: https://doi.org/10.36713/epra25058
DOI No: 10.36713/epra25058

ABSTRACT
The U.S. healthcare system has been experiencing an increasingly cybersecurity crisis, with more than 276 million individuals having had their data stolen in 2024 and hacking-related breaches accounting for almost 80% of reported incidents. Traditional security measures have failed to combat advanced cyber threats that seek to steal sensitive PII, health insurance information, and medical infrastructure. This study analyzes the creation, deployment and operational outcomes of AI-driven cyber-risk prediction models for U.S. healthcare institutions. A systematic literature review (SLR) design was used to analyze peer-reviewed academic journals and cybersecurity reports between 2012 to 2025 in databases such as IEEE Xplore, PubMed and ACM Digital Library. The study compares machine learning approaches for supervising the learning process, deep learning models and natural language processing tasks in healthcare cybersecurity. The findings indicated that AI models show superior performance in threat and risk prediction, particularly with gradient boosting algorithms, which yield the best accuracy for vulnerability identification. However, there continue to be barriers to implementation such as resource limitations, existing infrastructure needs, workforce skill gaps and regulatory uncertainty. Budget allocation is found to be the most important determinant of AI adoption success. AI technology has the potential to transform health care cybersecurity, but true investment value will only be seen when the necessary infrastructures are in place through strategic investments, training of staff and people with IT expertise, policy harmonization (both regulatory and policy), inclusive collaborative frameworks that support collective defense and are HIPAA compliant, while taking into account patient privacy issues.

KEYWORDS: *Artificial Intelligence, Cyber Risk, Prediction Models, US Healthcare Institutions*

INTRODUCTION

Healthcare in the United States is experiencing a monumental cybersecurity crisis. Healthcare agencies have large repositories of private patient information, including personal health records, as well as financial and social security records, which cybercriminals consider valuable sources for attack (Mrcela & Vuletic, 2018). Last year, cyberattacks on hospitals, clinics, and health insurers surged to disastrous levels; ransomware attacks alone have resulted in losses of billions of dollars amid the disruption to critical patient care. Such types of attacks are growing in number and complexity, and the existing security practices fail to cope with them (Mallick & Nath, 2024). This disturbing rate emphasizes the necessity for proactive means of defence that can stop cyber threats before they develop into full-scale attacks.

Artificial intelligence has recently been recognized as a disruptive technology in cybersecurity, providing levels of security that go beyond traditional rule-based methods. Machine learning models can also power through huge volumes of data to process and recognize both patterns and outliers that are undetectable to human analysts. Deep learning architectures show high proficiency in finding zero-day exploits and predicting cyber-attack campaign trajectories from past threat intelligence (Reddy et al., 2024; Narteh-Kofi et al., 2025). Natural language processing algorithms allow automatic extraction of information on security issues and threats from a variety of reports and threat data sources (Marinho & Holanda, 2023). AI technologies such as these, deployed effectively, may help to change the cybersecurity game from being one of reacting in real time to risk exposure and instead use AI to predict that risk

so it can be managed more accurately than reactionary-based management, which could result in resources being used where they're not needed and detract from potentially responding programmatically before an issue is a problem.

Notwithstanding the potential of AI-powered cybersecurity, companies in the United States healthcare sector encounter obstacles when it comes to integrating new and advanced technologies. The landscape of the health sector is governed by strict legislative frameworks that closely govern data accessibility and appropriateness of use (Isibor, 2024), including HIPAA and HITECH Act rules. Most healthcare providers, especially smaller community hospitals and rural clinics, do not have the technical backbone or cybersecurity know-how to roll out complex AI tools. Many old medical hardware as well as EHR systems are obsolete software-wise and cannot easily blend in with contemporary cybersecurity (Boda & Immaneni, 2022). In addition, as the provision of healthcare is intrinsically urgent, the security framework should not hinder patient care processes and clinical operations. These restrictions result in a complex decision environment where efficient, compliance and operational considerations need to be balanced through innovative security solutions (Singh 2024).

This study provides a comprehensive framework for building and deploying AI-enhanced cyber risk prediction models that are designed for the operational context of U.S. healthcare institutions. The research is focused on several machine learning frameworks in the context of healthcare cybersecurity and tests their suitability for specific categories of healthcare facilities and threat scenarios. We use actual breach data and threat intelligence to determine the most pressing security risks that healthcare institutions are facing. Finally, the study also elaborates on pragmatic policy and planning responses to these limitations within the regulatory, technical and resource ecosystem of healthcare. Filling this void between what is possible in theory with AI and security, and what is needed for pragmatic healthcare security operations, the authors hope that this work will arm healthcare administrators (and security professionals) with actionable insights to help build more robust, predictive cybersecurity programs that can continue to protect patient information while upholding critical medical service delivery.

METHODOLOGY

This research adopts a systematic review approach, which involves reviewing peer-reviewed journal articles, conference proceedings, and cybersecurity reports published from 2012 to 2025 in the search for contemporary AI-based cyber risk prediction methodologies within healthcare environments. The paper aggregates result from several databases, such as IEEE Xplore, PubMed, and ACM Digital Library, with a specific focus on cybersecurity to analyze the efficiency, constraints, and adoption issues of different machine learning models found in academic papers. A comparative framework of comparing AI architectures, supervised, unsupervised and deep learning models, in the context of reported performance measures, computational setting and their adaptability to the healthcare-specific regulatory operational constraints as documented in empirical evidence.

LITERATURE REVIEW

The cybersecurity threats to the U.S. healthcare sector have been studied in depth in research papers from recent years, with an increasing body of work that studies both characteristics of threats and potential technical solutions. A systematic literature review is conducted to identify peer-reviewed papers, industry reports and empirical investigations on the application of AI for cyber risk prediction in the American healthcare setting. We structure the review thematically to orient our future work toward understanding where more is known, less has been studied and so on (sic), while at the same time laying the groundwork for AI-enabled predictive security models in U.S. healthcare institutions.

Cybersecurity Threat Landscape in U.S. Healthcare Institutions

According to a study by Kruse et al. (2017), which took a systematic review of the cybersecurity trends within the healthcare industry, the study found that healthcare institutions are way in adopting sufficient security measures to safeguard important patient information. The authors identified 31 peer-reviewed articles from CINAHL, PubMed, and Nursing and Allied Health databases to determine the existing cybersecurity threats and possible solutions in the healthcare setting. Their results showed that healthcare institutions continue to be excellent targets in medical information theft because they lag in adopting modern security measures and infrastructure upgrades. The research singled out ransomware attacks, malware intrusions, and unauthorized entry as the most prevalent risks to healthcare institutions, and the challenging aspects of the healthcare technology implementation have left a significant disconnect between the current security measures and the emerging threat environment.

Abirami and Parameshwari (2025) studied the cybersecurity threat landscape of smart and integrated healthcare systems, underlining how the digital transformation has brought benefits to patient care but also raised new attack vectors and vulnerabilities. The authors stressed that cyber-criminals target the healthcare industry for its immediate requirements, and they take advantage of this urgency by posing a ransom that cripples vital services or encrypts necessary files until institutions agree to pay. Their work demonstrated that networked medical devices may be at particular risk, as faulty equipment can deliver mistaken doses or have its behavior modified to the detriment of a patient. Their study emphasized that growing and ever-changing cyber threats in healthcare environments require focused security efforts, including frequent vulnerability checks, staff security training, network isolation/segmentation, continual monitoring of the institution's networks/systems and well-developed responses to incidents greatly appropriate for the specific needs of each healthcare facility.

A study carried out by Okafor et al. (2023) utilized a qualitative analytical case study approach to analyze cybersecurity risk mitigation techniques adopted by U.S. healthcare facilities, including such distinguished firms as the Mayo Clinic and Boston Medical Center. What they found in their analysis is that effective healthcare institutions have built well-reinforced defenses through policies and outreach to protect sensitive patient data and digital structures. They found that institutions with mature cybersecurity capabilities saw significant benefits ranging from sustained operations to enhanced stakeholder confidence to billions of dollars in losses averted through cyberattacks. Indeed, their research noted that these enterprises had proved extremely flexible by embracing agile cybersecurity structures that could accommodate a rapidly evolving threat landscape, underlining the urgent requirement for ongoing research, staff education and continued investment in security infrastructure to be maintained throughout all aspects of healthcare institutions.

Another study by Ayo-Farai et al. (2023) offered a thorough investigation of cybersecurity issues and strategies in the USA health care sector, focusing on the collision of advancement in healthcare technology and new cyberthreats. Using a combination of previous studies, case studies, and regulations in the field, the researchers described how threats such as malware attacks, insider threats and unauthorized access attempts have increased within US healthcare institutions. Their research both assessed the effectiveness of existing practices in cybersecurity used in the U.S. healthcare regulatory environment and examined how emerging technologies, AI and blockchain could boost security postures. Their research noted that the healthcare sector is facing risks that have never been seen before due to its digitalization and must adopt multi-tiered defense systems through a collaborative approach involving lawmakers and staff, healthcare professionals, as well as cybersecurity experts, to secure this field against ever-increasing cyber threats, which threaten not only the integrity of patient data but also patient care delivery.

Machine Learning and AI Techniques Applied to Healthcare Cybersecurity in the United States

The application of machine learning algorithms to healthcare cybersecurity has emerged as a critical research domain, with scholars increasingly focusing on intrusion detection and anomaly identification systems tailored to medical environments (Aryee et al, 2025). Supervised learning techniques, including support vector machines, decision trees, and neural networks, have been extensively documented in the literature as effective methods for classifying network traffic and identifying malicious activities within healthcare information systems (Somvanshi et al, 2019; Sani & Aryee, 2025). Recent literature emphasizes that ensemble learning approaches, which combine multiple algorithms to improve predictive accuracy, demonstrate promise in healthcare settings where the diversity of connected devices and communication protocols creates complex network ecosystems (Naderalvojoud & Hernandez-Boussard, 2024). Researchers have consistently noted that traditional signature-based detection systems prove inadequate against sophisticated threats, now making machine learning pattern recognition capabilities essential for identifying previously unknown attack vectors that specifically target medical devices and electronic health record platforms (AIZubi et al., 2021; Armah et al., 2025; Narteh-Kofi et al., 2025).

Deep learning models have received considerable attention in cybersecurity literature due to their ability to process huge amounts of healthcare interaction data and uncover subtle signs of compromise that are hidden from traditional security defenses. Sources such as convolution grids and RNNs have been proposed to be strong candidates for the temporal analysis of system behaviors, predicting ransomware attacks or data exfiltration attempts before they materialize (Redhu et al., 2024; Gokah et al., 2025). It is shown that deep learning models are effective in the analysis of file access patterns, user behavior analytics, and network traffic flows to establish baseline normalcy and signal

deviations as signs of cyber threats (Alfawareh, 2020). However, academic researchers uniformly cite the computational burdens and data needs in deploying deep learning methods at scale, and many U.S. healthcare providers, including small community hospitals and rural facilities, find practical implementation challenges to bringing high-resource models into production without impairing their clinical systems (Brown, 2022; Narteh-Kofi et al., 2025).

Natural language processing approaches have been widely investigated in related literature as solutions to automate threat intelligence analysis and vulnerability management for healthcare systems. Studies indicate that NLP models can effectively parse security advisories, vendor bulletins and threat databases for vulnerabilities specific to the medical devices and healthcare information systems used in U.S.-based institutions (Silvestri et al., 2023). The literature highlights that AI-powered automated threat intelligence capabilities by means of NLP can relieve pressure on healthcare security teams that are overburdened and help them to prioritize alerts by relevance, context and possible patient safety risks (Gupta et al., 2025; Adukpo & Bethel, 2025). Gradually, researchers have asserted the potential of transformer-based language like BERT and GPT to understand the sophisticated terminology used in cybersecurity and health care, which makes it possible to correlate more accurately between new threats with institutional vulnerabilities (Ali & Ghanem, 2025). The research conclusion appears to suggest that NLP-based threat intelligence solutions are best when fully trained and updated with medical lexicons for accurate interpretation of the security challenges faced by healthcare institutions.

The emergent work in federated learning and collaborative AI architectures fills a key deficiency of healthcare cybersecurity literature, which provides insight into how multi-institutional threat intelligence sharing could be achieved while adhering to HIPAA standards and patient privacy requirements. It is reported in the literature that federated learning architectures can assist healthcare institutions to collaboratively train machine learning models on distributed datasets; however, they must avoid centralization of private data and bypassing legal and ethical obstacles to data sharing, which have traditionally impeded collective defense strategies (Teo et al., 2024). Analysts suggest that these privacy-preserving ML approaches will fundamentally transform cybersecurity healthcare by enabling smaller facilities with limited security capabilities to leverage knowledge of threat activity gleaned from larger hospital networks (Khalid et al., 2023; Armah et al., 2025). New releases have emphasized that blockchain-facilitated federated learning systems give rise to further security guarantees in the form of tamper-evident audit trails for model updates and by maintaining shared threat intelligence integrity (Dommari & Vashishtha, 2025). The literature is unanimous about the encouragement of adopting an industry-wide common collaborative AI framework as the foundation to develop collective resilience against cyber actors that are more focused on exploiting the systemic vulnerabilities in healthcare, rather than a hospital's own specific weaknesses (Iancu, 2024).

Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2025): 8.619 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 12 | Issue: 11 | November 2025 -Peer-Reviewed Journal

Figure 1: HHS Healthcare Cybersecurity Defense Matrix

Healthcare IT Asset Protection Matrix

IT Asset	Examples	Common Attack Vectors	Potential Impact
Devices	Laptops, Servers, Medical Devices	Malware, Compromised credentials	Operational disruption, Lateral movement
Applications	EHR, Custom apps, Email tools	Software vulnerabilities, Supply chain attacks	Service disruption, Data theft
Networks	Cloud infrastructure, WiFi	Misconfiguration, Denial of service	Network unavailability
Data	PHI, PII, Claims data	Data theft, Ransomware encryption	Patient fraud, Data unavailability
Users	Employees, Patients	Phishing, Social engineering	Unauthorized access, Credential theft

Source: U.S. Department of Health and Human Services - Healthcare and Public Health Sector-Specific Cybersecurity Performance Goals (2024)

The diagram maps the NIST Cybersecurity Framework functions from (1) Identify, (2) Protect, (3) Detect, (4) Respond and (5) Recover to a healthcare IT asset protection matrix that identifies devices, applications, user networks and data. It contrasts modes of attack by type of asset for common attack vectors, including malware, stolen credentials, software vulnerabilities, misconfigurations, ransomware and phishing. The potential consequences of these threats, e.g., operational/service interruptions, data breaches, unauthorized access and network unavailability, as well as patient safety, are summarized in the table to further demonstrate how cybersecurity has to be considered through all aspects of healthcare environments.

Regulatory and Compliance Frameworks Governing Healthcare Cybersecurity in the U.S.

The US healthcare industry exists within an intricate network of compliance regulations for patient health information and cybersecurity. The Health Insurance Portability and Accountability Act (HIPAA) is the predominant legislative policy that deals with preservation mechanisms for PHI and PII in healthcare institutions (Subramanian et al., 2024). The HIPAA requires healthcare institutions to maintain robust administrative, physical, and technological safeguards to protect patient data from unauthorized access and cyber threats. The Health Information Technology for Economic and Clinical Health (HITECH) Act, passed in 2009 established HIPAA with more stringent notification requirements and a stronger penalty framework for failures to comply, placing more accountability on those healthcare providers (Redhead, 2009).

Healthcare institutions struggle with a lack of funding, outdated technologies and the constantly changing threat landscape when it comes to maintaining compliance with dynamic cybersecurity laws. Studies show that budget allocation rises as the most influential forecaster of the success level of compliance, where firms have failed to maintain a balance between functional requirements and investment in cybersecurity (Hossain et al., 2025). Non-compliance has significant economic and operational consequences, such as fines, loss of reputation and patient

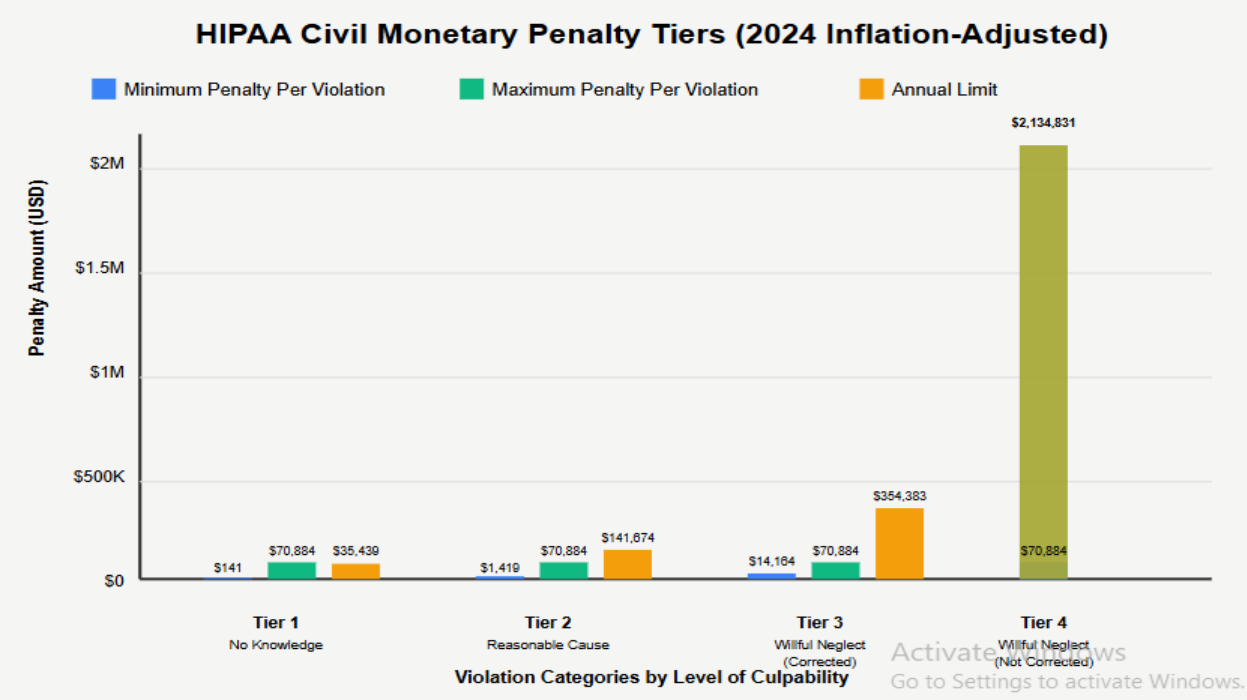
Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2025): 8.619 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 12 | Issue: 11 | November 2025 -Peer-Reviewed Journal

defiance in healthcare providers. Haleem et al. (2024) also point out that many healthcare institutions even operate with restricted resources, but at the same time, they must handle growing numbers of electronic health records, connected medical devices and telemedicine platforms, which enlarge their regulatory burden. These limitations result in sustained exposure to vulnerabilities that healthcare institutions need to quickly fix for compliance.

The adoption of standardized cybersecurity frameworks has become a must for healthcare institutions that wish to address regulatory demands and improve their security stance. The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and Health Information Trust Alliance (HITRUST) framework have emerged as complementary solutions for ensuring HIPAA compliance in the context of healthcare (Udroiu et al., 2022). These are systematic approaches to assessing risk, implementing security controls, and monitoring security so that it complies with Regulations. The NIST and HITRUST frameworks have great potential in healthcare institutions. This is because they provide a clear method for compliance with evolving U.S. cybersecurity regulations while also having effective safeguarding of data privacy (Balogun, 2025). Kozubtsova et al. (2024) show that the use of a risk-management-oriented assessment criterion for cybersecurity frameworks' selection allows companies to cover not only overall regulatory compliance.

When multiple compliance obligations coincide, it becomes imperative to adopt a cohesive method for cybersecurity governance within healthcare institutions, while still managing to be efficient and maintain a high quality of care. Institutions must juggle the competing demands from HIPAA, state-based legislation and industry standards. Rocha et al. (2024) highlight the policy harmonization and adoption of maturity models like the CMMC to help improve security postures and the ease with which compliance requirements are met. Adoption of continuous training programs for staff and investment in state-of-the-art cybersecurity tools appear as necessary ingredients towards the growth of a strong compliance culture (Folorunso et al., 2024). Future regulations will probably seek to ensure health care providers can prove they have forward-thinking, flexible cybersecurity measures in place to defend against new strains of attacks yet adhere to known standards.

Figure 2: HIPAA Civil Monetary Penalty Tiers (2024 Inflation-Adjusted)



Source: U.S. Department of Health and Human Services

The chart presents the tiered penalty structure established by the U.S. Department of Health and Human Services for HIPAA violations, which demonstrates the escalating financial consequences based on the level of institutional

culpability. The penalty framework reflects the HITECH Act's intent to differentiate between violations resulting from lack of knowledge versus those stemming from willful neglect, with penalties dramatically increasing from Tier 1 to Tier 4. These escalating penalty structures show the key importance of proactive compliance measures and the potential financial risks facing healthcare institutions that fail to adequately protect patient health information, with maximum annual penalties reaching over $2.1 million for uncorrected willful neglect violations.

Implementation Challenges and Barriers to AI Adoption in U.S. Healthcare Institutions

There are significant implementation issues for U.S. health care institutions to consider when it comes to artificial intelligence technology, even though the potential benefits of predicting cybersecurity risk are acknowledged. Resource constraints are one of the most important barriers, as health care institutions must share a limited budget among different competing needs such as patient treatments, building maintenance, compliance with regulations and investment in innovative technology. Balogun (2025) points out that funding is the most influential indicator in realizing the causes of effectiveness. Not only does a lack of funds handicap an entity when it comes to purchasing, installing and running complex AI-enabled systems. Most healthcare systems work with outdated technologies or legacy systems, which do not contain sufficient computing power and data-linking capacity that is necessary for the successful implementation of AI (Blessing & Hubert, 2024). These financial and technical limitations yield a persistent gulf between the promise of AI applications in theory and their actual application in resource-constrained health care facilities.

Integration of AI systems to interoperate with legacy healthcare IT forms an additional technical and institutional challenge for institutions that are looking to improve cybersecurity measures. Healthcare institutions often run an assortment of technologies for electronic health records, medical device data, administration systems and clinical applications that were not built to share data between them, let alone for AI integration. Sarkar et al. (2025) argue that the adoption of EHR and telemedicine has led to a fragmented data ecosystem, making it increasingly difficult to implement enterprise-wide AI-based cybersecurity solutions. The absence of standard data formats, varying documentation practices, and isolated information systems are obstacles to the creation of high-quality training datasets also required by machine learning models. Businesses spend an enormous amount of time and resources to cleanse, normalize, and integrate this data before they start getting reliable predictions on risk and insights on security from AI systems.

There are challenges in terms of the workforce that make it difficult to implement AI cybersecurity in healthcare. Not only are healthcare institutions perennially short of experts who have knowledge in both IT security and artificial intelligence, but the skill shortage is also impeding their ability to create, deploy and manage sophisticated predictive models. Sposato (2024) highlighted that ongoing professional development of staff is necessary to develop the institutional capacity for utilizing AI in practice effectively, but many institutions face difficulty in providing training and education. With the fast pace of AI methods and security threats, it is necessary for healthcare workers to constantly be learning new skills as a part of their workflow, in addition to their main clinical roles. This skills deficit also results in reliance on external vendors and consultants with “worries about the knowledge walking out the door, or whether there is sufficient depth of expertise to adapt AI solutions.”

Regulatory ambiguity and governance issues are further obstacles to the deployment of AI in healthcare cybersecurity. Providers must guarantee that their AI systems adhere to data privacy laws such as HIPAA, though there remains no specific guidance on algorithmic accountability, bias mitigation and automated decision-making in the realm of security (Mbah, 2024). The compliance risks presented by the "black box" nature of many of these post-COVID-19 AIs spell further liability concerns for healthcare providers, who need to be able to explain (to both clinicians and regulators/auditors) why certain patient populations receive varying treatments, not only as a matter of care delivery best practices, but also from a legal standpoint. Gozman and Currie (2015) note that companies will need to leverage integrated, risk-based compliance solutions if they are to be able to address new technologies while also satisfying existing regulatory demands. The dearth of industry-wide norms around validating AI outputs, benchmarking the performance of models and testing them for security makes decisions about which to adopt particularly difficult, with institutions finding it hard to assess rival systems or show due diligence in front of regulators and stakeholders.

Journal DOI: 10.36713/epra1013 | SJIF Impact Factor (2025): 8.619 ISSN: 2347-4378
EPRA International Journal of Economics, Business and Management Studies (EBMS)
Volume: 12 | Issue: 11 | November 2025 -Peer-Reviewed Journal

Table 1: Healthcare Data Breaches Reported to HHS Office for Civil Rights (2020-2024)

Year	Number of Large Breaches (≥500 records)	Total Individuals Affected	Hacking/IT Incidents (%)	Primary Location
2020	663	~42 million	~80%	Network Servers, Email
2021	714	~45 million	~82%	Network Servers, Email
2022	712	~48.6 million	~78%	Network Servers, Email
2023	725	~172.8 million	~79.7%	Network Servers, Email
2024	725	~276.8 million*	~80%	Network Servers, Email

Source: U.S. Department of Health and Human Services Office for Civil Rights Breach Portal (2025); HIPAA Journal Healthcare Data Breach Statistics (2025)

Note: 2024 figures include the Change Healthcare breach affecting 190+ million individuals

The data suggests that hacking and IT-related events are responsible for roughly 80% of all reported breaches between 2015-2020, with network servers and email systems being the two principal targets for attack. The shocking increase in people impacted, especially the jump to 276.8 million in 2024, reinforces the increasing seriousness and scope of cybersecurity risks for U.S. healthcare providers and underscores the urgent requirement for more advanced AI-based systems to predict and prevent such threats.

Performance Evaluation and Efficacy of AI-Powered Risk Prediction Models in American Healthcare Settings

A study by Haque et al. (2023) studied the performance of AI algorithms for predicting readmissions in the U.S. national health care system, which focuses on a common and yet important problem that affects most of us as patients and drives up costs. Based on a large electronic health records dataset with diagnosis codes, treatment history, laboratory test results and medication prescription information, the authors proposed and tested a range of machine learning models, including Random Forest Classifier, Logistic Regression and XGBoost Classifier. Their research used accuracy, precision, recall, F1-score and ROC-AUC as performance metrics to measure model efficacy. The Gradient Boosting model outperformed the others by scoring the highest on all metrics with the best accuracy and F1-score, which meant better all-around performance for prediction. These results demonstrate that AI-enabled predictive models are well-suited to identify high-risk patients for readmissions and therefore help healthcare providers deploy specific interventions to lower the significant load of avoidable hospital readmission.

Similarly, Adedinsewo et al. (2021) explored the use of deep learning models to non-invasively diagnose cardiac allograft rejection in heart transplant patients from an electrocardiogram-based approach. Their analysis included 7,590 unique ECG-biopsy pairs from 1,427 heart transplant patients at three Mayo Clinic sites between 1998 to 2021 and data were divided into training, validation and test sets to allow for rigorous model assessment. The AI-ECG model was able to identify moderate-severe acute cellular rejection (ACR) with an area under the receiver operating characteristic curve of 0.84 and achieved a sensitivity of 95% in the test set. A proof-of-concept screening study also confirmed the model sensitivity of up to 100% in predicting cardiac allograft rejection. Their study shows that deep learning models can convert common diagnostic tools into a powerful triage tool to identify patients in need of further intervention. It provides highly scalable screening options that can be applied to a frontline response for American healthcare systems.

A study by Siontis et al. (2021) has recently summarized the disruptive potential that artificial intelligence-based EC applications present in managing cardiovascular diseases (CVD) across clinical settings. It indicates the capability of sophisticated deep-learning convolutional neural networks to rapidly "read" ECGs like humans and identify signals and patterns that appear unintelligible yet also have become interpretable with an extremely high degree of accuracy by human interpreters. Large databases of linked digital ECGs and comprehensive clinical information were used to develop artificial intelligence (AI) models for detecting left ventricular dysfunction, silent atrial fibrillation, hypertrophic cardiomyopathy, as well as determining demographic features such as age, sex and race. The work highlighted how multilayer AI networks may have the capability to abuse ECG, being a strong non-invasive biomarker, as well as elevating a universal and frequently employed diagnostic test into an effective predictive instrument. These results emphasize the clinical and population relevance of AI-based ECG phenotyping, especially with the growing presence of mobile/wearable ECG devices in the US healthcare landscape.

Sarker (2024) examined the adoption of AI technologies for the improvement of patient care delivery in top US hospitals, including their benefits and challenges. The study observed that a range of AI technologies, such as predictive analytics, natural language processing and computer vision, have proved useful in supporting screening and diagnosis, speeding drug discovery and improving treatment protocols. AI-based chatbots and virtual assistants have been used successfully for patient triage and remote care delivery with demonstrated feasibility in several clinical disciplines. Yet the study also stressed that despite the gains of integrating AI into medicine, there are real hurdles that need to be addressed through meticulous deployment and ethical considerations. The outlined examples of AI adoption by top US hospitals in the case study sections, in this research paper show that successful deployment of an AI model requires strategically thought through integration processes and considerations for levels of technology-enabled activities needed vs. clinical workflows, institutional readiness factors, patient safety constraints to address a spectrum of factors to be accounted for when moving towards bringing impact at the point-of-care with increased complexity on translating model performance gains into meaningful healthcare delivery improvements.

CONCLUSION

This systematic review demonstrates that AI-based cyber risk prediction models are increasingly developed in the U.S healthcare sector and that their use enhances security through the ability to detect threats before such tools are detected. Machine learning and deep learning and natural language processing have demonstrated good performance in identifying aberrant activity, information about threats and assisting in predictive decision-making. Simultaneously, cyberattacks in healthcare have been on the increase, with over 276 million individuals affected in 2024 and almost 80 percent of all breaches being hacked. The impact of these attacks is severe in the form of fines levied by HIPAA as well as legal actions, which cost more than 2.1 million USD annually. Nevertheless, a multitude of healthcare organizations cannot implement AI due to insufficient funds, the use of outdated systems, a lack of data integration and a lack of qualified cybersecurity and AI specialists. Regulatory issues regarding the fairness of the algorithms, the responsibility of algorithms and the application of automated decision-making also exist. In the future, healthcare organizations must have a consistent investment in cybersecurity technologies, regular staff education and improved methods of disseminating threat intelligence without further compromising patient confidentiality. Greater direction by the government, more rigorous standards such as NIST CSF and HITrust and new investigations of lightweight and privacy-oriented AI frameworks will also assist in this respect. Having collaborative partnerships among healthcare leaders, security experts, AI researchers, and policymakers enables the U.S. healthcare system to safeguard patient data, minimize cyber risks, facilitate efficient workflow, and ensure the public is not achieving their goal.

REFERENCES

1. *Abirami, T., & Parameshwari, V. Cybersecurity Threat Landscape of Smart and Interconnected Healthcare Systems. In Cybersecurity and Data Science Innovations for Sustainable Development of HEICC (pp. 76-92). CRC Press.*
2. *Adedinsewo, D., Hardway, H. D., Morales-Lara, A. C., Wieczorek, M. A., Johnson, P. W., Douglass, E. J., ... & Yamani, M. (2023). Non-invasive detection of cardiac allograft rejection among heart transplant recipients using an electrocardiogram based deep learning model. European Heart Journal-Digital Health, 4(2), 71-80.*
3. *Adukpo, T. K., & Bethel, J. O. (2025). Impact of macroeconomic factors on government spending in Ghana. American Journal of Applied Statistics and Economics, 4(1). https://doi.org/10.54536/ajase.v4i1.5833*
4. *Alfawareh, M. D. (2020). Cyber threat intelligence using deep learning to detect abnormal network behavior (Master's thesis, Princess Sumaya University for Technology (Jordan)).*
5. *Ali, A., & Ghanem, M. C. (2025). Beyond detection: large language models and next-generation cybersecurity. SHIFRA, 2025, 81-97.*
6. *AlZubi, A. A., Al-Maitah, M., & Alarifi, A. (2021). Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques. Soft Computing, 25(18), 12319-12332.*
7. *Armah, A., Abankwa, B., & Minnoh, P. K. (2025). Ethical and sustainable deployment of AI for critical mineral extraction in the U.S.: A multi-objective optimization framework for advancing energy transition and environmental stewardship. **World Journal of Advanced Research and Reviews, 28**(1), 1780–1792. https://doi.org/10.30574/wjarr.2025.28.1.3608*
8. *Armah, A., Whajah, J., & Annankra, J. A. (2025). The geomechanical behavior of mine waste rock slopes under climate-induced stressors: A global perspective. **Sarcouncil Journal of Engineering and Computer Sciences, 4**(9), 1–??. https://doi.org/10.5281/zenodo.17526797*
9. *Aryee, B. A., Agyemang, K. A., & Mahmoud, M. (2025). Enhancing operational efficiency of U.S. healthcare data centers through advanced analytics and automation. Finance & Accounting Research Journal, 7(10), 524–539. https://doi.org/10.51594/farj.v7i10.2102*

10. *Aryee, B. A., Agyemang, K. A., & Mahmoud, M. (2025). Enhancing operational efficiency of U.S. healthcare data centers through advanced analytics and automation. **Finance & Accounting Research Journal, 7(10)**, 524–539. https://doi.org/10.51594/farj.v7i10.2102*
11. *Ayo-Farai, O. Cybersecurity in healthcare: a review of strategies and challenges in the usa. Acta Electronica Malaysia, 25-33.*
12. *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.*
13. *Blessing, E., & Hubert, K. (2024). Technological Infrastructure and Challenges: Integration challenges in implementing AI solutions in legacy systems.*
14. *Boda, V. V. R., & Immaneni, J. (2022). Optimizing CI/CD in Healthcare: Tried and True Techniques. International Journal of Emerging Research in Engineering and Technology, 3(2), 28-38.*
15. *Brown, C. J. (2022). Rural Hospital Sustainability: Meeting the Challenges of Healthcare Transformation and Strategies for Effective Implementation: Perspectives of Rural Healthcare Leaders (Doctoral dissertation, The University of North Carolina at Chapel Hill).*
16. *Dommari, S., & Vashishtha, S. (2025). Blockchain-Based Solutions for Enhancing Data Integrity in Cybersecurity Systems.*
17. *Folorunso, A., Wada, I., Samuel, B., & Mohammed, V. (2024). Security compliance and its implication for cybersecurity. World Journal of Advanced Research and Reviews, 24(01), 2105-2121.*
18. *Gokah, B. E., Amoako, E. K., Adom, S. G., Abakah, L. K., & Sampson, E. (2025). AI-driven user experience (UX) frameworks to enhance trust and security in U.S. online banking. Finance & Accounting Research Journal, 7(9), 465–478. https://doi.org/10.51594/farj.v7i9.2069*
19. *Gozman, D., & Currie, W. (2015, January). Managing governance, risk, and compliance for post-crisis regulatory change: A model of IS capabilities for financial institutions. In 2015 48th Hawaii International Conference on System Sciences (pp. 4661-4670). IEEE.*
20. *Haleem, A., Javaid, M., Singh, R. P., & Suman, R. (2021). Telemedicine for healthcare: Capabilities, features, barriers, and applications. Sensors international, 2, 100117.*
21. *Haque, M. M., Hossain, S. F., Akter, S., Islam, M. A., Ahmed, S., Liza, I. A., & Al Amin, M. (2023). Advancing Healthcare Outcomes with AI: Predicting Hospital Readmissions in the USA. Journal of Medical and Health Studies, 4(5), 94-109.*
22. *Hossain, M. A., Raza, M. A., & Rahman, T. Y. (2023). Resource allocation and budgetary constraints for cybersecurity projects in small to medium sized banks. Available at SSRN 5207138.*
23. *Iancu, S. (2024). Resilience–a Step Forward in an Era of Artificial Intelligence. Annals–Series on Military Sciences, 16(3), 48-62.*
24. *Isibor, E. (2024). Regulation of healthcare data security: Legal obligations in a digital age. Available at SSRN 4957244.*
25. *Khalid, N., Qayyum, A., Bilal, M., Al-Fuqaha, A., & Qadir, J. (2023). Privacy-preserving artificial intelligence in healthcare: Techniques and applications. Computers in Biology and Medicine, 158, 106848.*
26. *Kozubtsova, L., Ali, R. H., Kozubtsov, I., Lishchyna, V., Yashchuk, A., Hassan, N. B., & Lukashenka, V. (2024, April). Approach To Risk Management Based On The Assessment Of The Cost Of Quality Of Implementation Of Cybersecurity Measures Of The Institution. In 2024 35th Conference of Open Innovations Association (FRUCT) (pp. 399-406). IEEE.*
27. *Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25(1), 1-10.*
28. *Mallick, M. A. I., & Nath, R. (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. World Scientific News, 190(1), 1-69.*
29. *Marinho, R., & Holanda, R. (2023). Automated emerging cyber threat identification and profiling based on natural language processing. IEEE Access, 11, 58915-58936.*
30. *Mbah, G. O. (2024). Data privacy in the era of AI: Navigating regulatory landscapes for global businesses. Int. J. Sci. Res. Anal, 13(2), 2396-2405.*
31. *Mrcela, M., & Vuletic, I. (2018). Healthcare, Privacy, Big Data and Cybercrime: which one is the weakest link?. Annals Health L., 27, 257.*
32. *Naderalvojoud, B., & Hernandez-Boussard, T. (2024, January). Improving machine learning with ensemble learning on observational healthcare data. In AMIA Annual Symposium Proceedings (Vol. 2023, p. 521).*
33. *Narteh-Kofi, E., Asamoah, E., Adukpo, T. K., Mensah, N. (2025). Mergers and Acquisitions in the U.S. Capital Market: Theoretical Foundations, Market Dynamics and Strategic Implications. EPRA International Journal of Economics, Business and Management Studies (EBMS), 12(3), 71-80. https://doi.org/10.36713/epra20500*
34. *Narteh-Kofi, E., Raji, Y. M., Asamoah, E., & Adukpo, T. K. (2025). The role of artificial intelligence in enhancing decision-making and efficiency in mergers and acquisitions: A case study approach within the U.S. capital market. International Journal for Multidisciplinary Research (IJFMR), 7(3). https://doi.org/10.36948/ijfmr.2025.v07i03.44171*
35. *Narteh-Kofi, E., Sampson, E., Hattoh, E., Akingbade, R., & Agbeve, V. (2025, July 30). Optimizing target identification in the U.S. capital market mergers and acquisitions through artificial intelligence: Implications for financial efficiency, compliance, and national economic competitiveness. International Journal for Multidisciplinary Research (IJFMR), 7(4). https://doi.org/10.36948/ijfmr.2025.v07i04.51702*

36. *Okafor, C. M., Kolade, A., Onunka, T., Daraojimba, C., Eyo-Udo, N. L., Onunka, O., & Omotosho, A. (2023). Mitigating cybersecurity risks in the US healthcare sector. International Journal of Research and Scientific Innovation (IJRSI), 10(9), 177-193.*
37. *Reddy, S. P. K., Nagavelli, U., Kiran, Y. S., Kondoju, C. S., Bushmoni, S., & Yashaswi, A. (2024, December). Deep Learning for Zero-Day Threat Detection and Mitigation. In 2024 International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS) (pp. 1362-1368). IEEE.*
38. *Redhead, C. S. (2009, February). The Health Information Technology for Economic and Clinical Health (HITECH) Act. Congressional Research Service, Library of Congress.*
39. *Redhu, A., Choudhary, P., Srinivasan, K., & Das, T. K. (2024). Deep learning-powered malware detection in cyberspace: a contemporary review. Frontiers in physics, 12, 1349463.*
40. *Rocha, A., Alaba, F. A., Musa, H., Sousa, M. J., de Vasconcelos, J. B., & Pereira, R. (2024, October). Cybersecurity Maturity Models: A Systematic Literature Review. In The International Conference on Strategic Innovative Marketing and Tourism (pp. 179-206). Dordrecht: Springer Netherlands.*
41. *Sani, Z. N., & Aryee, B. A. (2025). Optimizing drug supply chains to prevent shortages in rural U.S. hospitals. EPRA International Journal of Economics, Business and Management Studies. https://doi.org/10.36713/epra24022*
42. *Sarkar, N. M., Dey, N. R., & Mia, N. M. T. (2025). Artificial Intelligence in telemedicine and remote patient monitoring: Enhancing virtual healthcare through AI-driven diagnostic and predictive technologies. International Journal of Science and Research Archive, 15(2), 1046-1055.*
43. *Sarker, M. (2023). Assessing the integration of AI technologies in enhancing patient care delivery in US hospitals. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 2(2), 338-351.*
44. *Silvestri, S., Islam, S., Papastergiou, S., Tzagkarakis, C., & Ciampi, M. (2023). A machine learning approach for the NLP-based analysis of cyber threats and vulnerabilities of the healthcare ecosystem. Sensors, 23(2), 651.*
45. *Singh, B. (2024). Unmanned aircraft systems (UAS), surveillance, risk management to cybersecurity and legal regulation landscape: unraveling the future analysis, challenges, demand, and benefits in the high sky exploring the strange new world. Unmanned aircraft systems, 313-354.*
46. *Siontis, K. C., Noseworthy, P. A., Attia, Z. I., & Friedman, P. A. (2021). Artificial intelligence-enhanced electrocardiography in cardiovascular disease management. Nature Reviews Cardiology, 18(7), 465-478.*
47. *Somvanshi, M., Chavan, P., Tambade, S., & Shinde, S. V. (2016, August). A review of machine learning techniques using decision tree and support vector machine. In 2016 international conference on computing communication control and automation (ICCUBEA) (pp. 1-7). IEEE.*
48. *Sposato, M. (2024). Leadership training and development in the age of artificial intelligence. Development and Learning in Institutions: An International Journal, 38(4), 4-7.*
49. *Subramanian, H., Sengupta, A., & Xu, Y. (2024). Patient health record protection beyond the health insurance portability and accountability Act: mixed methods study. Journal of Medical Internet Research, 26, e59674.*
50. *Teo, Zhen Ling, Liyuan Jin, Nan Liu, Siqi Li, Di Miao, Xiaoman Zhang, Wei Yan Ng et al. "Federated machine learning in healthcare: A systematic review on clinical applications and technical architecture." Cell Reports Medicine 5, no. 2 (2024).*
51. *Udroiu, A. M., Dumitrache, M., & Sandu, I. (2022, June). Improving the cybersecurity of medical systems by applying the NIST framework. In 2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) (pp. 1-7). IEEE.*