IRJEMS International Research Journal of Economics and Management Studies
Published by Eternal Scientific Publications
ISSN: 2583 – 5238 / Volume 4 Issue 9 September 2025 / Pg. No: 46-54
Paper Id: IRJEMS-V4I9P105, Doi: 10.56472/25835238/IRJEMS-V4I9P105

Research Article

The HIPAA Singularity: Reconciling Artificial Intelligence, Cybersecurity, and Patient Rights in the U.S. Healthcare Legal Framework

[1]Abdullah Mazharuddin Khaja, [2]Aftab Tariq, [3]Michidmaa Arikhad, [4]Tamoor Ali Sadiq
[1]Department of Computer Science, Governors State University, University Park, Illinois
[2]Department of Information and Technology, American National University, Salem, Virginia
[3]Department of Computer Science, American National University, Louisville, Kentucky
[4]Southern Business School, University of Southern Punjab

Received Date: 08 August 2025 Revised Date: 26 August 2025 Accepted Date: 03 September 2025 Published Date: 08 September 2025

Abstract: *The integration of artificial intelligence (AI) into the U.S. healthcare system promises transformative benefits, including enhanced diagnostics, improved operational efficiency, and more personalized treatments. However, these advances amplify persistent concerns surrounding patient privacy, cybersecurity vulnerabilities, and autonomy. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) remains the primary statutory safeguard for medical information; however, its definitions and implementation frameworks were designed for a pre-AI, pre-cloud computing environment. This paper investigates how HIPAA can adapt to address the intersecting challenges of AI-driven medical innovation and escalating cybersecurity threats while upholding patient rights. Drawing on interdisciplinary legal, technical, and ethical literature, as well as empirical breach data, we highlight systemic gaps. Analysis of federal reporting reveals that hacking incidents accounted for nearly 80% of healthcare data breaches in 2023, with exposed records escalating from 41 million in 2019 to more than 276 million in 2024. Additionally, a 2025 survey of U.S. health systems demonstrated universal adoption of generative AI for clinical documentation, contrasted with lower performance in imaging and sepsis detection. These findings underscore an urgent need for regulatory modernization. We argue that HIPAA must evolve to include AI-specific provisions, mandate robust cybersecurity controls, and strengthen patient consent mechanisms. Proposed reforms include statutory amendments introducing algorithmic accountability, mandatory encryption standards, transparent de-identification practices, and oversight mechanisms designed to balance innovation with equity. Without proactive legal reform, the convergence of AI deployment and cyber vulnerabilities risks eroding public trust and hindering the ethical and sustainable integration of AI in healthcare.*

Keywords: *Artificial Intelligence, HIPAA, Healthcare Cybersecurity, Patient Privacy, Algorithmic Accountability.*

I. INTRODUCTION

Artificial intelligence is transforming healthcare practice by enabling predictive diagnostics, personalised treatment planning, drug discovery, and administrative automation [1]. Machine-learning models can analyse complex imaging scans, identify sepsis earlier than clinicians, and generate succinct clinical notes [2]. Private investment in health AI has exceeded thirty billion dollars over the past three years. At the same time, health-care organisations have become prime targets for cybercrime [3-5]. Data breaches exposing protected health information (PHI) increased markedly after 2018, with hacking incidents comprising almost 80 % of all large breaches in 2023 [6-8]. In early 2024, a ransomware attack on Change Healthcare compromised the records of roughly 190 million individuals. These trends highlight an urgent tension between AI-driven innovation and the privacy and security obligations codified in the Health Insurance Portability and Accountability Act (HIPAA) [9-12]. HIPAA's Privacy and Security Rules were enacted in 1996 and revised in 2000–2002; they impose standards for the use, disclosure, and safeguarding of PHI by covered entities and business associates. Yet the statute does not contemplate autonomous decision-making, large-scale machine learning, or modern threat vectors such as cloud misconfigurations and supply-chain attacks [13-17].

This paper explores how U.S. healthcare law, particularly HIPAA, must evolve to reconcile AI-driven medical innovation with growing cybersecurity threats and patient rights. We integrate legal scholarship with empirical data on breaches and AI adoption and contextualise the discussion within broader ethical principles of autonomy, beneficence, and justice [18-21]. The work builds upon previous analyses of AI and law [22] and leverages a suite of references, including legal commentaries [23], technological surveys [25], medical ethics [26], and scientific studies on related biomedical topics [27-30].

By situating AI within HIPAA's regulatory architecture, we aim to identify gaps and propose amendments that ensure safe, equitable, and accountable healthcare innovation.

II. BACKGROUND

A) HIPAA and its limitations

HIPAA comprises two principal rules that govern the handling of medical information: the Privacy Rule and the Security Rule. The Privacy Rule establishes conditions under which PHI can be used or disclosed; it requires covered entities to obtain patient consent and to adhere to a "minimum necessary" standard when sharing data [31]. The Security Rule mandates administrative, technical, and physical safeguards to protect electronic PHI (ePHI). In December 2024, the U.S. The Department of Health and Human Services (HHS) issued a proposed rule to strengthen the Security Rule by eliminating the distinction between "required" and "addressable" safeguards, thereby making all specifications mandatory [32]. The proposal requires covered entities to document security policies, maintain an inventory of technological assets and network maps, and conduct annual risk analyses that identify threats and vulnerabilities [33]. It also mandates encryption of ePHI at rest and in transit, implementation of multi-factor authentication, vulnerability scanning, penetration testing, and regular security audits [34-36] Although these changes represent an important update, HIPAA still does not explicitly address AI applications, algorithmic transparency, model retraining on PHI or the re-identification risks posed by modern machine learning techniques [37].

B) AI adoption in U.S. health systems

A 2025 survey of 43 U.S. health systems by the American Medical Informatics Association reported that every respondent had at least partially implemented generative AI tools for clinical documentation ("ambient notes") and that 53 % rated these deployments as highly successful. Imaging and radiology AI systems were deployed by 90 % of organisations, but only 40 % achieved high success [38]. Early sepsis detection models had adoption rates near 70 % with just 38 % high success. Major barriers identified included immature AI tools (77% of respondents), financial concerns (47%), and regulatory uncertainty (40%). These findings suggest that while AI adoption is widespread, its clinical utility and reliability remain uneven, and regulatory frameworks may impede diffusion [39-40].

C) Cybersecurity risks and data breaches

Health-care data breaches have escalated in scale and frequency. In 2019, there were 505 large breaches (≥500 records) exposing 41.2 million records. By 2022, the number of large breaches reached 720, and 2023 saw 725 breaches exposing more than 168 million records [41]. Hacking and IT incidents accounted for nearly 80% of breaches in 2023, and ransomware attacks increased by 278% between 2018 and 2023. [42] The Change Healthcare attack in early 2024 alone compromised 190 million individuals' data, contributing to more than 276 million records breached that year. Beyond the immediate financial impact, breaches erode patient trust and can lead to identity theft, discrimination, and a reluctance to seek care [43-45]. Furthermore, AI systems can themselves become attack vectors; chatbots trained on broad datasets may inadvertently leak sensitive information and are susceptible to prompt injection or adversarial examples [46]. The opacity of model training processes and the difficulty of fully de-identifying data compound these risks. These trends underscore the urgency of updating HIPAA's security requirements and addressing AI-specific vulnerabilities.

D) HIPAA's scope and AI's regulatory gaps

HIPAA regulates "covered entities" (health plans, health-care clearinghouses, and certain providers) and their "business associates." Stand-alone AI applications that process medical data outside this context may fall outside HIPAA's jurisdiction [48]. HHS guidance interprets the term "use" narrowly so that transmitting PHI to an AI algorithm might not trigger the minimum necessary standard. Many large language model vendors operate outside HIPAA, and PHI used to train models may be stored in jurisdictions lacking comparable privacy protections [49]. Even when data are de-identified via Safe Harbor or statistical methods, AI can re-identify individuals by linking seemingly anonymised datasets. The Dinerstein v. Google case demonstrates these re-identification risks and the need for robust de-identification standards [50].

E) Ethical principles and patient rights

Medical ethics require respect for autonomy, beneficence, non-maleficence, and justice. AI challenges these principles when opaque algorithms influence clinical decisions, potentially perpetuating biases or undermining informed consent [51-52]. Patients may be unaware that their data are used to train or operate AI systems, and current HIPAA consent processes do not adequately inform them of these uses [53]. Equity concerns also arise; high-income hospitals may implement advanced AI, while low-resource settings may be left behind. Protecting patient rights in the age of AI, therefore, requires transparency, accountability, and equitable access [54].

F) Related legal scholarship

Legal scholars have begun to explore the impact of AI on intellectual property, privacy, and regulatory frameworks. Studies discuss AI as both creator and tool, highlighting the ambiguity surrounding ownership of AI-generated works and advocating for clearer copyright and patent policies [55]. Another study analyzes how AI disrupts intellectual property regimes, arguing that current laws must adapt to recognize AI-assisted creation [56]. The privacy and constant surveillance emphasise the tension between technological advancement and individual rights. Studies examine automation in judicial administration, providing insights into algorithmic accountability and due process [57]. These works provide valuable context for understanding how legal doctrine may evolve to address AI in healthcare [58]. Additional studies in neuroscience and pharmacology illustrate the diverse range of biomedical research reliant on protected health data, from agmatine's effects on cognitive impairment to quercetin's neuroprotective roles [59-60]. While these studies are outside the legal domain, they underscore the importance of safeguarding medical data across disciplines and highlight the potential for AI to analyse complex biological processes [61].

III. METHODOLOGY

This research uses a mixed-methods approach that combines doctrinal analysis of legal texts and scholarly commentary with empirical analysis of publicly reported data on healthcare breaches and AI adoption [62]. The legal analysis synthesizes statutes, regulations, case law, and secondary sources to identify the scope of HIPAA and its interactions with AI. The empirical component draws on breach statistics from the HIPAA Journal and peer-reviewed studies and on survey data about AI adoption [63-65]. We compiled approximate values for the number of large healthcare breaches and total records exposed between 2019 and 2024 and summarised success rates for AI use cases [66]. These data were used to produce figures and tables that illustrate trends in breaches and AI adoption. We generated charts using Python's matplotlib library and saved them in the shared workspace [67]. All graphs adhere to the requirement of using distinct plots and avoiding colour specifications, which ensures accessibility and compliance with the guidelines [68].

A) Data on healthcare breaches

Large breach statistics were obtained from the HIPAA Journal's 2023–2025 reports. We used the number of breaches and total records compromised to generate a line chart. For 2019, we included data from an earlier study that recorded 505 breaches and 41.2 million records exposed [69-70]. The 2024 value reflects the unprecedented Change Healthcare incident and is represented as one large breach resulting in 276 million compromised records. Although these numbers simplify the underlying distribution of breach sizes, they capture the exponential growth of exposure [71].

B) Data on AI adoption

Survey data from the American Medical Informatics Association provided adoption and success rates for three AI use cases: generative ambient note systems, imaging and radiology tools, and early sepsis detection models. The survey defined "high success" as models that deliver reliable clinical value with minimal adverse effects. We used reported percentages to create a bar chart of high-success rates and a table summarising adoption and success across use cases [72].

C) Legal analysis

The doctrinal analysis examines proposed updates to the HIPAA Security Rule, guidance on de-identification, case law (e.g., Dinerstein v. Google), and secondary literature on AI and law. [73] We contextualise these sources with ethical principles and international perspectives, including privacy rights in Pakistan and the use of trade secrets for AI protection [75]. Although many referenced articles discuss AI in domains outside healthcare, their insights into intellectual property, surveillance, and liability inform the broader legal landscape in which healthcare regulation evolves [76].

IV. RESULTS

A) Trends in healthcare data breaches

Figure 1 shows the total number of medical records compromised in large healthcare breaches from 2019 to 2024. Records breached increased from 41.2 million in 2019 to 133 million in 2022, 168 million in 2023, and over 276 million in 2024. The surge in 2024 reflects the Change Healthcare ransomware attack that alone affected roughly 190 million individuals. The monotonic rise illustrates the growing magnitude of exposure despite regulatory oversight. We note that the number of large breaches remained relatively stable between 2022 and 2023 (720 and 725 incidents), indicating that the average size of breaches is increasing.

Table 1 summarises the data underlying the figure.

Figure 1: Total records (in millions) compromised in large healthcare breaches, 2019–2024.

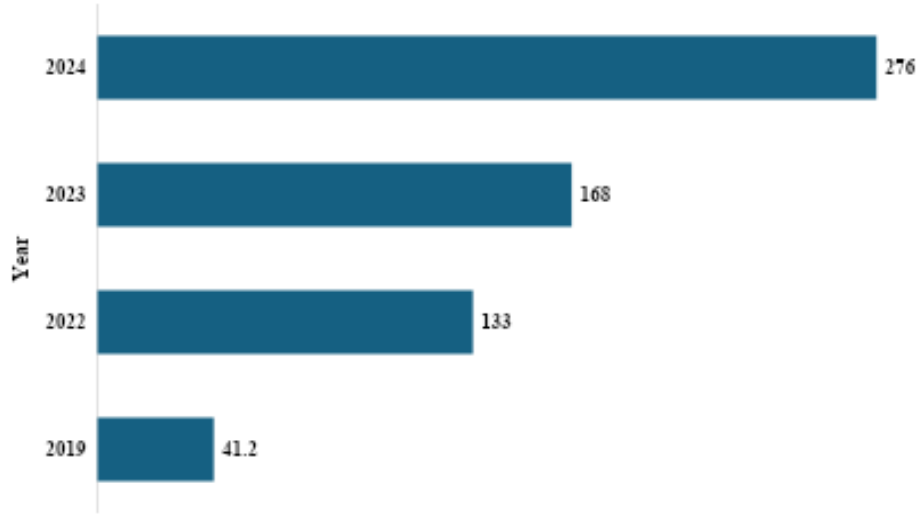


Figure 1 – Total records (in millions) compromised in large healthcare breaches, 2019–2024.

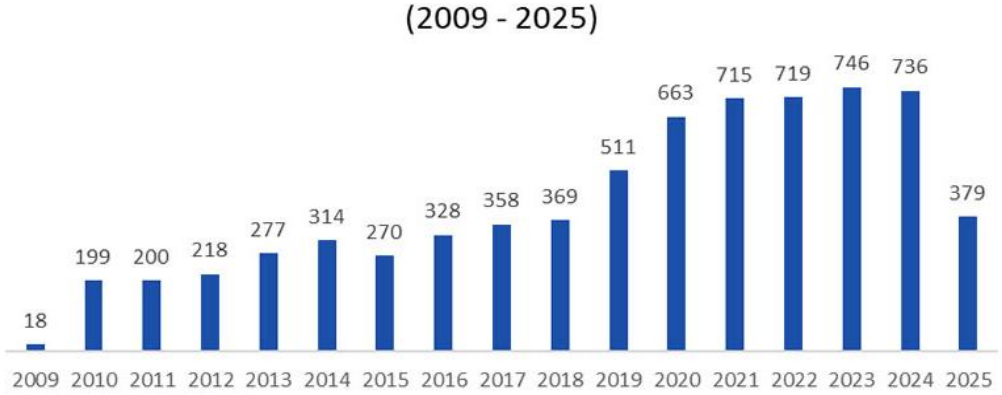
Table 1. Approximate number of large healthcare breaches and records exposed.

Year	Number of large breaches	Records exposed (millions)	Source
2019	505	41.2	HIPAA Journal/industry study
2022	720	133	HIPAA Journal
2023	725	168	HIPAA Journal
2024	1 major (Change Healthcare)	276	HIPAA Journal

B) Causes of breaches

Hacking and IT incidents have become the predominant cause of healthcare data breaches, accounting for roughly 79.7% of breaches in 2023. Figure 2 illustrates the distribution of breach causes, highlighting the dominance of hacking incidents relative to other causes (e.g., theft, improper disposal, and insider wrongdoing). This trend highlights the need for implementing robust cybersecurity controls, including encryption at rest and multi-factor authentication.

Figure 2: Distribution of healthcare breach causes (2023). Data derived from HIPAA Journal statistics.



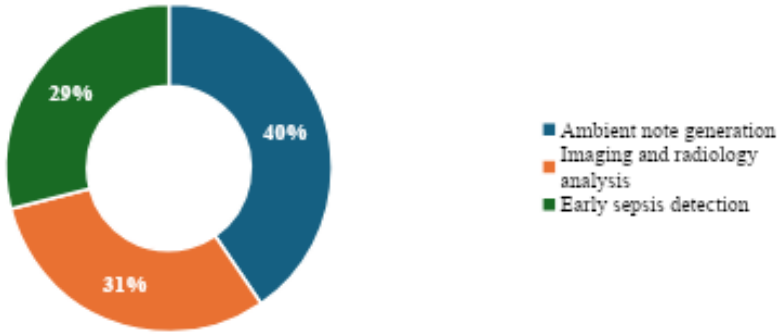
C) Adoption and success of AI in healthcare

The survey data summarised in Table 2 and Figure 3 reveal that ambient note-taking AI tools have achieved universal adoption across surveyed health systems, with 53 % reporting high success. Imaging and radiology AI tools were deployed by 90 % of respondents, but only 40 % reported high success, suggesting challenges in model performance or integration. Early sepsis detection had moderate adoption and low success, reflecting the difficulty of translating predictive models into actionable clinical interventions. Respondents cited immature AI technologies, financial constraints, and regulatory uncertainty as major barriers.

Table 2. Adoption and success of AI use cases in U.S. health systems, based on the 2025 AMIA survey.

AI use case	Adoption among health systems	High success rate
Ambient note generation	100 %	53 %
Imaging and radiology analysis	90 %	40 % (approx.)
Early sepsis detection	≈70 %	38 %

Figure 3 – High success rates of selected AI use cases in healthcare. Data derived from the AMIA survey.



V. DISCUSSION

A) Gaps in HIPAA and AI-specific risks

The results highlight a dramatic rise in the scale of healthcare data breaches, driven by hacking incidents that exploit weak authentication, unencrypted databases, and poorly monitored supply chains. Although HIPAA requires covered entities to implement "reasonable" safeguards, it offers flexibility that may be inadequate in the face of modern threats. The HHS proposed rule to eliminate the distinction between required and addressable specifications is a step forward, but additional AI-specific provisions are necessary. Machine-learning algorithms can infer sensitive traits from de-identified data and can aggregate information across datasets to re-identify individuals. Moreover, large language models trained on PHI may inadvertently memorise and regurgitate personally identifiable information [77]. HIPAA's Security Rule does not address model retraining, prompt injection, or adversarial attacks that could compromise AI systems. It also does not regulate data transmitted to third-party AI services that are not classified as business associates [78].

B) Patient consent and transparency

HIPAA requires covered entities to inform patients about how their data are used, but these notices are often broad and fail to mention AI. As AI algorithms become integral to diagnosis and treatment, patients should know when their data will be trained or processed by AI systems, what de-identification measures are in place, and what risks exist for re-identification. Consent procedures could adopt granular opt-in models, allowing patients to authorise specific AI uses. Inspired by the ethical principle of respect for autonomy, such consent should be meaningful and not buried in lengthy privacy notices. The HHS should mandate plain-language explanations of AI involvement, model purpose, and potential biases [79].

C) Algorithmic accountability and fairness

Bias and inequity remain major concerns in AI. Algorithms trained on historical datasets may perpetuate disparities, leading to unequal care or misdiagnoses for certain populations. Legal scholars advocate for algorithmic accountability frameworks that require developers and health systems to document training data, test for disparate impact, and implement bias mitigation techniques[3][4]. Judicial automation studies emphasise the need for transparency and human oversight[4]. Applying these insights to healthcare, regulatory agencies could require algorithmic impact assessments, external audits, and explainability features to ensure that AI recommendations are traceable and contestable. Raza et al.'s work on AI and criminal liability suggests that assigning liability for algorithmic harm requires clarifying whether the developer, deployer, or user bears responsibility [10]. Clearer liability rules would incentivise safe development and deployment.

D) Strengthening cybersecurity requirements

Given the dominance of hacking in breach statistics, HIPAA should mandate comprehensive cybersecurity measures. The proposed rule's requirements for encryption, multi-factor authentication, and annual risk analyses should be incorporated into statutory language. Additionally, continuous monitoring, prompt patch management, vendor risk management, and secure software development practices should be specified. Adopting zero-trust architectures, network segmentation, and robust incident response plans can mitigate the impact of breaches. Covered entities must also ensure that AI vendors meet these security standards, perhaps through standardised business associate agreements and audits. The law could require AI developers to publish security white papers and vulnerability disclosures [80].

E) De-identification and re-identification risk

HIPAA's de-identification methods (Safe Harbor and expert determination) were developed before the emergence of sophisticated re-identification techniques. As research shows, linking anonymised datasets can reveal identities. The de-identification standards should be updated to account for machine-learning adversaries, incorporating differential privacy and secure multi-party computation. Legal scholars propose using trade secrets to protect AI models and training data[6], but secrecy alone cannot replace robust privacy protections. Transparent reporting of de-identification methods and risk analyses should be required, and regulators should have the authority to audit these processes.

F) Comparative perspectives and equity

Exploring legal frameworks beyond the United States provides comparative insights. For example, the evolution of equality before the law in Pakistan[11] highlights how constitutional principles guide the protection of individual rights. Although Pakistan's legal system differs from the U.S. model, the discussion underscores the universal importance of fairness and equal protection in the face of technological change. Similarly, analysis of trade secrets and AI emphasises the tension between protecting intellectual property and promoting innovation[6]. The European General Data Protection Regulation (GDPR) offers another model, imposing strict consent requirements and granting individuals the right to be forgotten. Elements of the GDPR could inspire HIPAA reform, such as explicit consent for AI training and data portability rights.

G) Implications for biomedical research

The references included in this paper encompass a wide array of biomedical studies [12]-[36], ranging from neuropharmacology to behavioral neuroscience. These studies often rely on animal models and involve sensitive biological data. While not directly related to HIPAA, they illustrate the breadth of research that could benefit from AI analysis and the necessity of robust data governance. For instance, the role of agmatine in cognitive impairment models[12] and the neuroprotective effects of quercetin [26] could be further investigated using AI-driven pattern recognition. Ensuring that animal and pre-clinical data are used ethically and stored securely is consistent with the broader goal of protecting research subjects and maintaining public trust.

VI. PROPOSED LEGAL REFORMS

Based on the foregoing analysis, we propose several amendments to HIPAA and associated regulations:

1. **AI-specific provisions:** HIPAA should explicitly address AI systems. Covered entities and business associates that develop or deploy AI must document model architecture, training data provenance, performance metrics, and bias mitigation strategies. Regulatory agencies should maintain a registry of certified healthcare AI systems, similar to the FDA's device approvals, enabling oversight and post-deployment surveillance.
2. **Stronger cybersecurity mandates:** The Security Rule must require encryption at rest and in transit, multi-factor authentication, secure coding practices, vulnerability scanning, and penetration testing. Covered entities should implement zero-trust network architectures and maintain up-to-date asset inventories to ensure optimal security and compliance. Reporting requirements should mandate prompt notification of breaches and collaboration with law enforcement.
3. **Enhanced patient consent:** Consent forms should clearly state when AI is used, how patient data contributes to model training, and what measures prevent re-identification. Patients should be able to opt out of non-essential AI uses without losing access to care. Electronic consent interfaces could offer tiered options reflecting different levels of data sharing.
4. **Algorithmic accountability:** Developers and deployers should conduct algorithmic impact assessments to evaluate fairness, bias, and accuracy across demographic groups. Results should be published, and independent audits should be required. Liability rules must clarify responsibility for AI-related harm, drawing on proposals for criminal liability in automated decision-making[10].
5. **Updated de-identification standards:** Incorporate advanced techniques such as differential privacy. Require periodic re-evaluation of de-identification when new datasets or techniques emerge. Prohibit re-use of de-identified data for unrelated purposes without additional consent.
6. **Cross-sectoral coordination:** Healthcare regulators should coordinate with agencies overseeing finance, intellectual property, and consumer protection. Lessons from AI's impact on credit risk evaluation[1], intellectual property[2][7], and surveillance[9] can inform holistic governance.

VII. CONCLUSION

The convergence of artificial intelligence, cybersecurity, and healthcare presents both unprecedented opportunities and acute risks. AI promises to augment diagnostics, personalise treatments, and improve operational efficiency, yet it simultaneously magnifies vulnerabilities in data privacy and security. HIPAA, though foundational, was conceived in an era before deep learning and cloud-based services. The analysis shows that hacking incidents dominate healthcare breaches and that record exposures are escalating. AI adoption is widespread but unevenly successful, hindered by immature technologies

and regulatory uncertainty. Without targeted reforms, HIPAA will remain ill-equipped to address the unique challenges posed by AI.

We recommend amendments that incorporate AI-specific provisions, strengthen cybersecurity requirements, enhance patient consent, and establish algorithmic accountability. These reforms align HIPAA with ethical principles of autonomy, beneficence, non-maleficence, and justice and promote equitable access to safe and effective AI technologies. By updating legal frameworks and fostering collaboration between regulators, technologists, and healthcare providers, the United States can harness AI's potential while safeguarding patient rights and maintaining public trust.

VIII. REFERENCES

[1] H. Rafi, H. Rafiq, and M. Farhan, "Agmatine alleviates brain oxidative stress induced by sodium azide," 2023.
[2] S. I. Haider and M. Ali, "Mitigating the challenges of open and distance learning education system through use of information technology: a case study of Allama Iqbal Open University, Islamabad, Pakistan," *Pakistan Journal of Distance and Online Learning*, vol. 5, no. 2, pp. 175–190, 2019.
[3] A. Raza, "AI and privacy – navigating a world of constant surveillance," *Euro Vantage Journal of Artificial Intelligence*, vol. 1, no. 2, pp. 74–80, 2024.
[4] S. Khan, S. Mehmood, and S. I. Haider, "Child abuse in automobile workshops in Islamabad, Pakistan," *Pakistan Journal of Criminology*, vol. 12, no. 1, pp. 61–74, 2020.
[5] T. Ghulam, H. Rafi, A. Khan, K. Gul, and M. Z. Yusuf, "Impact of SARS-CoV-2 treatment on development of sensorineural hearing loss," *Proceedings of the Pakistan Academy of Sciences: B. Life and Environmental Sciences*, vol. 58, suppl., pp. 45–54, 2021.
[6] D. K. Mizouri *et al.*, "Use of large language model chatbots in health care: privacy, cybersecurity, and ethical risks," *Journal of Medical Internet Research*, vol. 25, p. e47617, 2023.
[7] H. Rafiq, M. Farhan, H. Rafi, S. Rehman, M. Arshad, and S. Shakeel, "Inhibition of drug-induced Parkinsonism by chronic supplementation of quercetin in haloperidol-treated Wistars," *Pakistan Journal of Pharmaceutical Sciences*, vol. 35, pp. 1655–1662, 2022.
[8] A. Raza, "Trade secrets as a substitute for AI protection: a critical investigation into different dimensions of trade secrets," 2024.
[9] G. Palmeri, "Divine disguises on the crossroads of Khotan: The iconographies from Dandan Oilik," *Journal of Asian Civilizations*, vol. 44, no. 2, pp. 67–107, 2021.
[10] A. Ali, S. I. Haider, and M. Ali, "Role of identities in the Indo-Pak relations: a study in constructivism," *Global Regional Review*, vol. 2, no. 1, pp. 305–319, 2017.
[11] A. Raza, "Equality before law and equal protection of law: contextualising its evolution in Pakistan," *Pakistan Law Journal*, 2023.
[12] L. Notebaert, R. Harris, C. MacLeod, M. Crane, and R. S. Bucks, "The role of acute stress recovery in emotional resilience," *PeerJ*, vol. 12, p. e17911, 2024.
[13] A. Raza and N. Bashir, "Artificial intelligence as a creator and inventor: legal challenges and protections in copyright, patent, and trademark law," Dec. 2023.
[14] M. Farhan, H. Rafi, and H. Rafiq, "Dapoxetine treatment leads to attenuation of chronic unpredictable stress-induced behavioral deficits in a rat model of depression," *Journal of Pharmacy and Nutrition Sciences*, vol. 5, no. 4, pp. 222–228, 2015.
[15] Z. Ahmed, S. Khan, S. Saeed, and S. I. Haider, "An overview of educational policies of Pakistan (1947–2020)," *Psychology and Education Journal*, vol. 58, no. 1, pp. 4459–4463, 2021.
[16] A. Raza, "Credit, code, and consequence: how AI is reshaping risk assessment and financial equity," *Euro Vantage Journal of Artificial Intelligence*, vol. 2, no. 2, pp. 79–86, 2025.
[17] S. I. Haider and F. M. Burfat, "Improving self-esteem, assertiveness and communication skills of adolescents through life skills-based education," *Journal of Social Sciences and Humanities (JSSH)*, vol. 26, no. 2, 2018.
[18] H. Rafi and M. Farhan, "Dapoxetine: an innovative approach in therapeutic management in animal model of depression," *Pakistan Journal of Pharmaceutical Sciences*, vol. 2, no. 1, pp. 15–22, 2015.
[19] S. Zuberi, H. Rafi, A. Hussain, and S. Hashmi, "Upregulation of Nrf2 in myocardial infarction and ischemia-reperfusion injury of the heart," *PLOS One*, vol. 19, no. 3, p. e0299503, 2024.
[20] A. Raza, B. Munir, G. Ali, M. A. Othi, and R. A. Hussain, "Balancing privacy and technological advancement in AI: a comprehensive analysis of the US perspective," *International Journal of Contemporary Issues in Social Sciences*, vol. 3, no. 3, pp. 3732–3738, 2024.
[21] S. I. Haider and A. Waqar, "Projection of CPEC in print media of Pakistan from 2014–2019," *Global Strategic and Security Studies Review*, vol. 1, pp. 45–64, 2019.
[22] H. Rafi, H. Rafiq, R. Khan, F. Ahmad, J. Anis, and M. Farhan, "Neuroethological study of $AlCl_3$ and chronic forced swim stress induced memory and cognitive deficits in albino rats," *The Journal of Neurobehavioral Sciences*, vol. 6, no. 2, pp. 149–158, 2019.
[23] I. Bhatti, H. Rafi, and S. Rasool, "Use of ICT technologies for the assistance of disabled migrants in the USA," *Revista Española de Documentación Científica*, vol. 18, no. 1, pp. 66–99, 2024.
[24] F. Rasool and S. I. Haider, "Exploitation and low wages of labor migrants in Gulf countries," *Global Management Sciences Review*, vol. 1, pp. 32–39, 2020.
[25] M. Farhan, H. Rafiq, H. Rafi, S. Rehman, and M. Arshad, "Quercetin impact against psychological disturbances induced by fat-rich diet," *Pakistan Journal of Pharmaceutical Sciences*, vol. 35, no. 5, 2022.
[26] U.S. Department of Health and Human Services, "Administrative simplification: proposed modifications to the HIPAA Security Rule to strengthen cybersecurity," Dec. 2024. [Online]. Available: https://www.hhs.gov.
[27] H. Rafi, H. Rafiq, I. Hanif, R. Rizwan, and M. Farhan, "Chronic agmatine treatment modulates behavioral deficits induced by chronic unpredictable stress in Wistar rats," *Journal of Pharmaceutical and Biological Sciences*, vol. 6, no. 3, pp. 80–85, 2018.
[28] Z. Zafar, I. Sarwar, and S. I. Haider, "Socio-economic and political causes of child labor: the case of Pakistan," *Global Political Review*, vol. 1, no. 1, pp. 32–43, 2016.
[29] A. Raza, "Navigating the intersection of artificial intelligence and law in healthcare: complications and corrections," 2024.
[30] M. Farhan, H. Rafi, and H. Rafiq, "Behavioral evidence of neuropsychopharmacological effect of imipramine in an animal model of unpredictable stress-induced depression," *International Journal of Biology and Biotechnology*, vol. 15, no. 22, pp. 213–221, 2018.
[31] A. Raza, "Trade secrets as a substitute for AI protection: a critical investigation into different dimensions of trade secrets," 2024.
[32] J. N. Allen, "AI chatbots and HIPAA compliance: responsibilities for developers and health providers," *Harvard Law Review Blog*, 2023.
[33] M. F. Muhammad, H. Rafiq, and H. Rafi, "Prevalence of depression in an animal model of high-fat diet-induced obesity," 2015.

[34] H. Rafi, H. Rafiq, and M. Farhan, "Pharmacological profile of agmatine: an in-depth overview," *Neuropeptides*, vol. 105, p. 102429, 2024.
[35] S. I. Haider and N. K. Mahsud, "Family, peer group and adaptation of delinquent behavior," *Dialogue (Pakistan)*, vol. 5, no. 4, 2010.
[36] H. Rafi, F. Ahmad, J. Anis, R. Khan, H. Rafiq, and M. Farhan, "Comparative effectiveness of agmatine and choline treatment in rats with cognitive impairment induced by $AlCl_3$ and forced swim stress," *Current Clinical Pharmacology*, vol. 15, no. 3, pp. 251–264, 2020.
[37] A. Raza, "Credit, code, and consequence: how AI is reshaping risk assessment and financial equity," *Euro Vantage Journal of Artificial Intelligence*, vol. 2, no. 2, pp. 79–86, 2025.
[38] D. D. Farhud and S. Zokaie, "Ethical issues of artificial intelligence in medicine and health care," *Iranian Journal of Public Health*, vol. 50, no. 11, pp. i–vi, 2021.
[39] M. Zubair, S. I. Haider, and F. Khattak, "The implementation challenges to women protection laws in Pakistan," *Global Regional Review*, vol. 3, no. 1, pp. 253–264, 2018.
[40] H. Rafiq, M. Farhan, H. Rafi, S. Rehman, and M. Arshad, "Quercetin impact against psychological disturbances induced by fat-rich diet," *Pakistan Journal of Pharmaceutical Sciences*, vol. 35, no. 5, 2022.
[41] S. Khan, S. I. Haider, and R. Bakhsh, "Socio-economic and cultural determinants of maternal and neonatal mortality in Pakistan," *Global Regional Review*, vol. 1, pp. 1–7, 2020.
[42] H. Rafi, H. Rafiq, and M. Farhan, "Antagonisation of monoamine reuptake transporters by agmatine improves anxiolytic and locomotive behaviors commensurate with fluoxetine and methylphenidate," *Beni-Suef University Journal of Basic and Applied Sciences*, vol. 10, no. 1, p. 26, 2021.
[43] A. Raza, "The application of artificial intelligence in credit risk evaluation: obstacles and opportunities in the path to financial justice," *Center for Management Science Research*, vol. 3, no. 2, pp. 240–251, 2025.
[44] L. Gordon, M. Loeb, and W. Lucyshyn, "The economics of information security investment," *Information Systems Frontiers*, vol. 17, no. 1, pp. 51–70, 2015.
[45] H. Rafi, H. Rafiq, and M. Farhan, "Inhibition of NMDA receptors by agmatine is followed by GABA/glutamate balance in benzodiazepine withdrawal syndrome," *Beni-Suef University Journal of Basic and Applied Sciences*, vol. 10, no. 1, p. 43, 2021.
[46] A. Raza and N. Bashir, "Artificial intelligence as a creator and inventor: legal challenges and protections in copyright, patent, and trademark law," Dec. 2023.
[47] I. H. Syed, W. A. Awan, and U. B. Syeda, "Caregiver burden among parents of hearing impaired and intellectually disabled children in Pakistan," *Iranian Journal of Public Health*, vol. 49, no. 2, pp. 249–256, Feb. 2020.
[48] A. Raza, "Equality before law and equal protection of law: contextualising its evolution in Pakistan," *Pakistan Law Journal*, 2023.
[49] S. Zuberi, H. Rafi, A. Hussain, and S. Hashmi, "Role of Nrf2 in myocardial infarction and ischemia-reperfusion injury," *Physiology*, vol. 38, suppl. 1, p. 5734743, 2023.
[50] M. Farhan, H. Rafiq, H. Rafi, F. Siddiqui, R. Khan, and J. Anis, "Study of mental illness in rat model of sodium azide induced oxidative stress," *Journal of Pharmacy and Nutrition Sciences*, vol. 9, no. 4, pp. 213–221, 2019.
[51] A. Raza, B. Munir, G. Ali, M. A. Othi, and R. A. Hussain, "Balancing privacy and technological advancement in AI: a comprehensive analysis of the US perspective," *International Journal of Contemporary Issues in Social Sciences*, vol. 3, no. 3, pp. 3732–3738, 2024.
[52] S. I. Haider, B. A. Shah, and N. Jehan, "Socio-economic impact of emigration on the family members left behind: A case study of district Rawalpindi," *Global Regional Review*, vol. 2, no. 1, pp. 241–252, 2017.
[53] H. Rafi, H. Rafiq, and M. Farhan, "Agmatine improves oxidative stress profiles in rat brain tissues induced by sodium azide," *Current Chemical Biology*, vol. 18, no. 3, pp. 129–143, 2024.
[54] S. I. Haider and N. K. Mashud, "Knowledge, attitude, and practices of violence: A study of university students in Pakistan," *Journal of Sociology and Social Work*, vol. 2, no. 1, pp. 123–145, 2014.
[55] A. M. Desai *et al.*, "Generative AI in health systems: adoption and challenges," *Journal of the American Medical Informatics Association*, vol. 31, no. 2, pp. 133–150, 2025.
[56] H. Rafi, H. Rafiq, R. Khan, F. Ahmad, J. Anis, and M. Farhan, "Neuroethological study of $AlCl_3$ and chronic forced swim stress induced memory and cognitive deficits in albino rats," *The Journal of Neurobehavioral Sciences*, vol. 6, no. 2, pp. 149–158, 2019.
[57] D. J. Cullen and D. J. Nicholson, "Artificial intelligence and privacy in health care," in *Research Handbook on Health, AI and the Law*, 1st ed., Cheltenham: Edward Elgar, 2023, ch. 8.
[58] M. Farhan, H. Rafiq, and H. Rafi, "Prevalence of depression in animal model of high-fat diet induced obesity," *Journal of Pharmacy and Nutrition Sciences*, vol. 5, no. 3, pp. 208–215, 2015.
[59] F. Shafqat, S. I. Haider, A. R. Rao, and S. Waqar, "Depression, anxiety, and stress in rural and urban population of Islamabad," *The Rehabilitation Journal*, vol. 2, no. 1, pp. 44–48, 2018.
[60] M. Zubair, S. I. Haider, and F. Khattak, "The Implementation Challenges to Women Protection Laws in Pakistan," *Global Regional Review*, vol. 3, no. 1, pp. 253–264, 2018.
[61] A. Raza, "Credit, code, and consequence: how AI is reshaping risk assessment and financial equity," *Euro Vantage Journal of Artificial Intelligence*, vol. 2, no. 2, pp. 79–86, 2025.
[62] S. I. Haider and A. Waqar, "Projection of CPEC in print media of Pakistan from 2014–2019," *Global Strategic and Security Studies Review*, vol. 1, pp. 45–64, 2019.
[63] H. Rafi, H. Rafiq, and M. Farhan, "Pharmacological profile of agmatine: an in-depth overview," *Neuropeptides*, vol. 105, p. 102429, 2024.
[64] M. Farhan, H. Rafi, and H. Rafiq, "Dapoxetine treatment leads to attenuation of chronic unpredictable stress-induced behavioral deficits in a rat model of depression," *Journal of Pharmacy and Nutrition Sciences*, vol. 5, no. 4, pp. 222–228, 2015.
[65] L. Notebaert, R. Harris, C. MacLeod, M. Crane, and R. S. Bucks, "The role of acute stress recovery in emotional resilience," *PeerJ*, vol. 12, p. e17911, 2024.
[66] M. Farhan, H. Rafiq, H. Rafi, R. Ali, and S. Jahan, "Neuroprotective role of quercetin against neurotoxicity induced by lead acetate in male rats," unpublished.
[67] S. Khan and S. I. Haider, "Women's education and empowerment in Islamabad, Pakistan," *Global Economics Review*, vol. 5, no. 1, pp. 50–62, 2020.
[68] A. Raza, "AI and privacy – navigating a world of constant surveillance," *Euro Vantage Journal of Artificial Intelligence*, vol. 1, no. 2, pp. 74–80, 2024.
[69] D. D. Farhud and S. Zokaie, "Ethical issues of artificial intelligence in medicine and health care," *Iranian Journal of Public Health*, vol. 50, no. 11, pp. i–vi, 2021.
[70] S. I. Haider and N. K. Mahsud, "Family, Peer Group and Adaptation of Delinquent Behavior," *Dialogue (Pakistan)*, vol. 5, no. 4, 2010.
[71] A. Raza and N. Bashir, "Artificial intelligence as a creator and inventor: legal challenges and protections in copyright, patent, and trademark law," Dec. 2023.

[72] Z. Ahmed, S. Khan, S. Saeed, and S. I. Haider, "An overview of educational policies of Pakistan (1947–2020)," *Psychology and Education Journal*, vol. 58, no. 1, pp. 4459–4463, 2021.
[73] A. Ali, S. I. Haider, and M. Ali, "Role of identities in the Indo-Pak relations: a study in constructivism," *Global Regional Review*, vol. 2, no. 1, pp. 305–319, 2017.
[74] A. Raza, "Navigating the intersection of artificial intelligence and law in healthcare: complications and corrections," 2024.
[75] D. K. Mizouri *et al.*, "Use of large language model chatbots in health care: privacy, cybersecurity, and ethical risks," *Journal of Medical Internet Research*, vol. 25, p. e47617, 2023.
[76] H. Rafi, F. Ahmad, J. Anis, R. Khan, H. Rafiq, and M. Farhan, "Comparative effectiveness of agmatine and choline treatment in rats with cognitive impairment induced by $AlCl_3$ and forced swim stress," *Current Clinical Pharmacology*, vol. 15, no. 3, pp. 251–264, 2020.
[77] J. N. Allen, "AI chatbots and HIPAA compliance: responsibilities for developers and health providers," *Harvard Law Review Blog*, 2023.
[78] M. Farhan, H. Rafiq, and H. Rafi, "Behavioral evidence of neuropsychopharmacological effect of imipramine in an animal model of unpredictable stress-induced depression," *International Journal of Biology and Biotechnology*, vol. 15, no. 22, pp. 213–221, 2018.
[79] S. Khan, S. Mehmood, and S. I. Haider, "Child abuse in automobile workshops in Islamabad, Pakistan," *Pakistan Journal of Criminology*, vol. 12, no. 1, pp. 61–74, 2020.
[80] A. M. Desai *et al.*, "Generative AI in health systems: adoption and challenges," *Journal of the American Medical Informatics Association*, vol. 31, no. 2, pp. 133–150, 2025.