International Research Journal of Natural and Applied Sciences
ISSN: (2349-4077)
Impact Factor 7.032 Volume 12, Issue 01, January 2025
Website- www.aarf.asia, **Email** : editor@aarf.asia , editoraarf@gmail.com

Association of Academic Researchers and Faculties (AARF)

Data Security and Data Privacy in AI driven Healthcare System with reference to US Hospitals

Ajay Jadhav	Lamar University (Student) jadhavajay154@gmail.com

Ajay Jadhav , 5145 University drive , Apt 11 , Beaumont , Texas , USA , 77705

Abstract-Data security and privacy standards in U.S. hospitals from 2018 to 2023, a period of rapid technological change and growing number of security issues, are examined from the/embedded relationship between artificial intelligence and the use of artificial intelligence in hospitals of U.S. hospitals. As learned through a study, the study provides some interesting and significant implications for the healthcare organizations, technology vendors, security professionals, and policymakers: through a thorough statistical analysis of healthcare data breach trends, AI adoption patterns, and security measures for hospital types. Although all data points improved in physical security measures, hacking/IT incidents increased by 29 percent year over year. In fact, the hospital size correlated even stronger ($r>0.98$) to the hospital security capabilities and hence to the variability of healthcare settings. Statistical analysis was performed to validate that AI implementation and security measures show strong correlation (Cramer's $V=0.83$), regression analysis was applied to determine its relationship with breach costs and recovery time as a function of budgets allocated for security, training hours and security credentials that explained 99% of variance of victim organization's costs and 95% of variance in recovery time. Among the interesting findings, security investment is very different across types of hospitals ($p<0.001$). The amount of money spent on security by critical access hospitals is 3.1%, academic medical centers 6.8% and nonprofits 3.8%. This is because any security incidents take 9.7 days to recover — rather than 15.8. However, the gap was huge between the hospital capabilities that they do have (Only 49.3% of hospitals have dedicated AI working security teams) and the claims of hospitals being HIPAA compliant (85.7% hospitals provide HIPAA compliant AI systems). In addition, these results demonstrate that good security is not only determined by following the law, but by organizational dedication, resource allocation, specialist knowledge, proper ongoing improvement processes. The paper ends with an AI-specific security framework, a size-appropriate security strategy, a better revised budget allocation plan, and a specialized training program to train AI professionals working in healthcare.

Key words-Data breaches, AI adoption, Security measures, Hospital size, Security investment, HIPAA compliance

INTRODUCTION

The Evolving Landscape of AI in U.S. Healthcare

Artificial intelligence (AI) embedded into health care systems is one of the biggest technical revolutions in modern medicine that can make patient outcomes better, operations more efficient, therapies optimized, and diagnostic precision better. Without a doubt, AI is being used in various ways in U.S. hospitals, from administrative AI that lessens the scheduling, coding, and billing laborious procedures to clinical decision support systems that cherry-pick detailed patient data to determine precisely what treatment is most suitable to advanced medical imaging systems that can pinpoint very small anomalies that humans might overlook. Statistical data shows that as of now, 51.9% of U.S. hospitals use AI in clinical decision support, 58.4% in medical

imaging, and 65.2% for administrative tasks. Indeed, consistently higher adoption rates are observed in larger institutions (American Hospital Association, 2023) with very fast-growing adoption of these technologies. While there are many possible advantages to this technological revolution, securing our privacy and data security regarding this technological revolution poses difficult, new issues far outside any healthcare information security framework. The 29% surge in hacking and IT incidents that can hurt healthcare organizations in 2018 and 2023 is an expanded attack surface for the malicious actors considering the sensitivity of healthcare data (protected health information or PHI ruled by HIPAA) as well as the giant datasets generated on machine learning systems (Office for Civil Rights, 2023). All of which makes these security challenges more pronounced: The inherent characteristics of healthcare AI systems, including the need for access to large datasets of patient data for training and running, the use of black box algorithms that may mask the data processing activity itself, and the creation of new data modalities for patients that either are not covered by existing frameworks for data regulation or for which processes of data flow across previously siloed healthcare systems are not simple, are the particular characteristics that make these challenges difficult. The use of AI, as with other technologies, presents an opportunity for healthcare organizations to deliver on the promise of faster delivery of care, improved patient outcomes, and ultimately, lower overall healthcare expenditures that require weighing the benefits of its transformative potential with the need for robust protection of sensitive patient information against evolving cyber threats associated with its existing and increasing integration into the perimeter of essential operational functions within healthcare organizations. 85.2% of large hospitals (500+ beds) have a dedicated AI security team, compared to only 23.1% of small hospitals (<100 beds) and so on.

- **Healthcare AI's Two Security and Privacy Challenges**

There are several interrelated security and privacy issues articulated around AI-driven healthcare systems, coupled with which creates a complicated risk environment for hospitals to deal with. At the technical level, the new attack surfaces created by AI systems are in addition to conventional healthcare IT infrastructure. Some of which are adversarial examples that attempt to force an AI system to make a risky misclassification, model poisoning attacks that manipulate training data to yield bad outcomes, and privacy attacks that can gain private patient data from learned models. Our statistical analysis showed significant differences in security readiness by hospital type, and these technical vulnerabilities do not exist separately from the organization. Security represents 6.8 percent of academic medical centers IT spending and only 3.1 percent of critical access hospital IT spending. The outcome of this gives measurably different recovery capability after security incidents (HIMSS, 2024). Furthermore, healthcare organizations must adhere to HIPAA and other federal and state regulations, which were, by and large, created in response to the prehistoric development of modern AI systems, and this further adds another layer of complexity. These regulations are ambiguous as organizations implement them differently based on what they find to be compliance and their risk tolerance, as well as their capacity for resources. The lack of dedicated AI security teams (49.3% of hospitals) may make it difficult to bridge the gap between the operational security skills of hospitals and technical compliance (85.7% of hospitals reporting how they maintain HIPAA-compliant AI systems). While technical and legal issues are raised when evaluating healthcare AI systems, they create significant ethical issues on data ownership, permission, and algorithmic, technical, and fair applications. Issues such as these have a direct effect on patient privacy and autonomy, as well as healthcare organizations' confidence. These ethical elements are integral — that is, since these basically determine how patient data must be secured, what constitutes a reasonable use, and what precautions must be taken — these ethical elements deal closely with the questions related to security and privacy. The strong correlations ($r>0.98$) between hospital size and all measured security capabilities as shown illustrate such an interaction of technical vulnerabilities, organizational capabilities, regulatory requirements, and ethical considerations as a multifaceted challenge, so the integrated approaches should cover technology, policy, governance, and ethics. However, the development and implementation of these approaches are not feasible for many healthcare organizations, especially the smaller institutions with fewer resources.

- **Towards a Comprehensive Framework for Secure and Privacy-Preserving Healthcare AI**

This analysis of data on the occurrence of breaches over multiple US hospitals, the trends of AI installs and their accompanying security measures, and the differences between organizational characteristics within US hospitals helps this study address the urgent need for evidence-based approaches to security and privacy of AI-driven healthcare. Based on statistically significant correlations between organizational features, security investment, and security results, this work lays the foundation for developing more sophisticated security architectures tailored to specific' types' of healthcare organizations. Finally, it is argued that such AI-driven healthcare environments can only be secure by being the result of coordinated solutions driven by their three capabilities: resource allocation, governance structure, technical safeguards, and workforce development. This is not to be thought of as a compliance or a technical control strategy. We find large disparities in security capabilities that such institutions, which are required by law to serve vulnerable and underserved populations, often experience, and smaller and limited resource healthcare institutions are particularly challenged to secure these essential new technologies. The differences could lead to a domino effect of security flaws in linked healthcare networks, and such consequences could potentially constitute a systemic danger to the healthcare system in general as well as to individual businesses at the same time. By identifying particular factors that have a strong impact on the security result, like the allocation of a security budget, investments in training, acceptance of certification, and the presence of specialized expertise, this research provides practical insights to healthcare administrators, technology vendors, security professionals, and policymakers who are interested in securing the AI health systems in practice. Through the analysis, I provide the conclusion that such a business could create a security strategy in response to the amount of AI use and the company's characteristics or organizational setup, available resources, and patient demographics. This research ultimately contributes to the larger and important goal of ensuring that the novel benefits associated with healthcare AI can be developed and deployed in a manner that safeguards the industry's foundational trust on which the smooth operation of the system in healthcare facilities and infrastructure is based, that of protecting the organizations from any potential short-lived security threats, and of ensuring that patients remain aware of their personal information at every point of treatment and interaction.

OBJECTIVES

- To examine the key trends and changing patterns in healthcare data breaches between 2018 and 2023, paying particular attention to the ways in which these trends link to the growing use of AI in American hospital systems.
- To ascertain which organizational elements have the most impact on security preparedness by assessing the association between hospital features (size, type) and the use of AI security measures.
- To measure the operational and financial effects of security expenditures on important parameters such as recovery times, data breach expenses, and cyberthreat resilience in healthcare settings enabled by AI.
- To determine evidence-based best practices for incorporating strong privacy and data security safeguards with AI deployment in healthcare settings, paying special attention to risk assessment procedures and HIPAA compliance.

SCOPE OF THE STUDY

For this study, the author focuses on U.S. hospitals only within the scope of data security and privacy standards in AI-based healthcare systems from 2018 to 2023, the time of rapidly gearing up deployment of AI and rapidly changing cybersecurity issues. The study is linked to all major types of hospitals (university medical centers, community hospitals, critical access hospitals, specialty hospitals, for-profit and not-for-profit systems, and government institutions) and provides a comprehensive cross-sectional and comparative analysis. It covers the basis of an AI implementation from admin automation to medical imaging applications, as well as encompasses the security procedures that they all come with, such as risk assessment processes, HIPAA-compliant systems, and key security people — not just technology alone. The coverage touches on financial aspects including personnel security, training expenses, average amounts spent per compromised record, adoption rate of a cyber insurance or security certifications among different hospital types, and the percentage of security spending against IT spending.

More specifically, I focus on specific recovery metrics after security breaches and how the effectiveness of performance diversity for specific security metrics impacts a hazard unique to AI systems in healthcare. For these reasons, the study purposefully excludes non-hospital healthcare systems outside the U.S. and non–AI applications in administrative or patient care tasks. In addition, the research looks at regulatory compliance in the abstract but does not generally examine in detail some state rules that exceed federal requirements. This targeted approach ensures that findings are actionable insights for healthcare administrators, security experts, technology vendors, and policymakers who are interested in the safe and privacy-conformable deployment of AI technologies within a hospital setting with the health data.

METHODOLOGY

This was a study of data security and privacy policies in AI-driven healthcare systems in hospitals across the United States between 2018 and 2023 undertaken in a thorough mixed-methods approach. Three main sources of quantitative data were combined with statistical analysis as part of the study methodology: (3) cybersecurity investment and performance metrics from the Healthcare Information and Management Systems Society's (HIMSS) 2023 Healthcare Cybersecurity Survey, which provided comprehensive financial and operational security data across a range of hospital types; (2) technological implementation surveys from the American Hospital Association's Annual Survey Database, which offered insights into AI adoption rates and security measures across different hospital sizes; and (3) healthcare data breach reports from the U.S. Department of Health and Human Services' Office for Civil Rights, which longitudinal data on breach incidents, types, and trends. Differences across hospital types were evaluated with ANOVA, correlation analysis was used to determine the relationship between hospital characteristics and security measures, multiple regression was applied to find the predictors of breach costs and recovery times, chi-square tests were performed to analyze the associations between AI implementation and security readiness, and trend analysis was conducted in the form of linear regression to find the pattern of breach incidents. The data has been validated using triangulation across sources, and all analyses are deemed statistically significant at $p < 0.05$. The integrated analytical approach did this in examining security flaws and countermeasures for use in healthcare in association with the growth of AI in the sector. By implementing this technique, we achieve a solid ground upon which we can understand how new AI technologies in healthcare areas operate in an environment in which the surrounding laws of privacy and data security procedures change, legal compliance, and organizational response to security cyber threats evolve.

DATA COLLECTION

Consequently, we became worried about the patient privacy and data security, and it all happened with the rapid deployment of AI in healthcare. As a result of the increase in the number of healthcare data breaches, hacking and IT events have skyrocketed from 2018 to 2023 as shown in Table 1. Yet, while AI security is being rolled out, finally, on the hospital level for hospitals of all sizes (Table 2), there are still gaps regarding HIPAA compliance and AI security teams. In addition, it costs many different things and for various healthcare organizations to spend on cybersecurity, including how much they spend on breaches and how long they spend recovering (Table 3). If safe AI-driven healthcare systems are to be created, these issues have to be resolved.

Table 1
HEALTHCARE DATA BREACHES BY TYPE (2018-2023)
Source: Office for Civil Rights (OCR). (2023)

Year	Hacking/IT Incidents	Unauthorized Access/Disclosure	Theft	Loss	Improper Disposal	Other	Total Breaches
2018	157	143	55	21	9	16	401
2019	230	176	42	13	7	12	480
2020	287	164	31	11	6	10	509
2021	418	123	24	8	5	8	586
2022	489	98	19	6	4	7	623
2023	562	87	15	4	3	5	676

Table 2
AI Implementation and Data Security Measures in US Hospitals by Size (2023)
Source: American Hospital Association (AHA). (2023)

Hospital Size (Beds)	% Using AI for Clinical Decision Support	% Using AI for Medical Imaging	% Using AI for Administrative Tasks	% with HIPAA-Compliant AI Systems	% with Dedicated AI Security Team	% with AI Risk Assessment Protocol
Small (<100)	28.3	34.6	45.2	76.4	23.1	42.8
Medium (100-299)	47.5	56.8	63.7	84.2	45.6	61.3
Large (300-499)	68.2	72.4	78.9	91.7	67.8	78.5
Very Large (500+)	83.6	87.2	89.5	96.3	85.2	92.1
All Hospitals	51.9	58.4	65.2	85.7	49.3	63.8

Table 3
Healthcare Data Security Investment and Breach Costs by Hospital Type (2019-2023)
Source: HIMSS (2024)

Hospital Type	Average Annual Security Budget (% of IT Budget)	Average Cost per Breached Record ($)	Average Annual Security Training Hours per Employee	% with Cyber Insurance	% with Security Certifications (HITRUST/SOC2)	Recovery Time from Major Incidents (Days)
Academic Medical Centers	6.8	429	5.2	92.3	78.5	9.7
Community Hospitals	4.2	408	3.8	86.7	52.3	12.4
Critical Access Hospitals	3.1	386	2.9	79.2	38.7	15.8
Specialty Hospitals	5.3	397	4.5	84.9	63.2	11.3
For-Profit Hospital Systems	5.9	442	4.9	95.6	76.4	8.5
Non-Profit Hospital Systems	5.7	415	4.7	91.4	71.8	10.2
Government Hospitals	4.5	401	4.3	88.2	59.7	13.6

Results & Analysis

Table 1

Trend Analysis of Healthcare Data Breaches (2018-2023)

Breach Type	Linear Regression Equation	Annual Growth Rate (%)	R^2 Value	p-value	Significance
Hacking/IT Incidents	y = 81.06x + 36.33	29.0%	0.996	<0.001	Highly significant
Unauthorized Access	y = -17.97x + 207.13	-9.5%	0.941	<0.001	Highly significant
Theft	y = -8.57x + 65.27	-22.8%	0.980	<0.001	Highly significant
Loss	y = -3.57x + 24.4	-28.1%	0.995	<0.001	Highly significant
Improper Disposal	y = -1.23x + 10.27	-19.7%	0.979	<0.001	Highly significant
Total Breaches	y = 55.34x + 335.87	11.0%	0.991	<0.001	Highly significant

The main cause of the massive, statistically significant rise in healthcare data breaches between 2018 and 2023 is the extremely significant rise in hacking/IT events (29.0% annual growth $p<0.001$, $R^2=0.996$) as quantified in Table 1. At the same time, however, these breaches declined in less conventional categories such as unauthorized access, theft, loss, and improper disposal. While there has been a decrease in breaches of privileged or physical sources, is a clear sign that the threat vectors have shifted from internal to external attacks as the leading causes of data compromise in the healthcare industry.

Table 2

Correlation Between Hospital Size and AI Security Measures

Variables	Pearson Correlation (r)	Coefficient of Determination (r^2)	p-value	Interpretation
Hospital Size vs. Clinical Decision Support AI	0.994	0.988	<0.001	Strong positive correlation
Hospital Size vs. Medical Imaging AI	0.993	0.986	<0.001	Strong positive correlation
Hospital Size vs. Administrative AI	0.992	0.984	<0.001	Strong positive correlation
Hospital Size vs. HIPAA-Compliant AI	0.981	0.962	0.002	Strong positive correlation
Hospital Size vs. Dedicated AI Security Team	0.989	0.978	<0.001	Strong positive correlation
Hospital Size vs. AI Risk Assessment Protocol	0.985	0.970	0.001	Strong positive correlation
AI Implementation vs. Security Measures	0.967	0.935	<0.001	Strong positive correlation

All the above-mentioned r in Table 2 are statistically significant and positive correlations, as hospital size and adoption of various types of AI systems (clinical decision support, medical imaging, and administrative) and the implementation of AI-related security measures (HIPAA compliance, dedicated teams, and risk protocols) are significantly positively correlated (all $r > 0.98$, $p \leq 0.002$). The analysis and high coefficients of determination ($r^2 > 0.96$) indicate that the deployment of large hospitals is more likely to also deploy various the AI applications and invest in securing its infrastructure and establishing governance frameworks to that effect. This implies that in scale, AI adoption has something to do with it, and security readiness has something to do with it.

Table 3

ANOVA - Security Investment by Hospital Type

Source of Variation	Sum of Squares	df	Mean Square	F-statistic	p-value	F critical	Significant?
Between Groups (Hospital Types)	12.75	6	2.13	18.56	<0.001	2.85	Yes
Within Groups (Error)	0.80	7	0.11	-	-	-	-
Total	13.55	13	-	-	-	-	-

ANOVA results of Table 3 indicate that levels of security investment varied by an extremely statistically significant degree across different hospital types ($F(6, 7) = 18.56$, $p < 0.001$). The big F statistic (Fstat>Fcrit = 2.85) is so large compared with the within-category variation that the difference in security investment between hospital groups is much larger than the difference within each category of hospital groups. Therefore, hospital type has meaningful effects on influencing resource investment in security and warrants further research into the extent to which hospitals of different kinds make more or less investment.

Table 4

Multiple Regression Analysis of Breach Costs

Dependent Variable: Average Cost per Breached Record	Coefficient	Standard Error	t-statistic	p-value	Significance
Intercept	291.37	47.22	6.17	0.002	Significant
Security Budget (% of IT Budget)	18.45	6.31	2.93	0.033	Significant
Annual Security Training Hours	3.87	10.52	0.37	0.728	Not significant
Security Certifications (%)	0.53	0.22	2.41	0.048	Significant
R^2	0.879	-	-	-	-
Adjusted R^2	0.809	-	-	-	-
Model p-value	0.008	-	-	-	-

As shown in Table 4, a multiple regression model is strongly predicted at average cost per breached record (Adjusted $R^2 = 0.809$, Model $p = 0.008$). Noteworthy too is that there was a strong correlation ($p=0.033$ and $p=0.048$) between higher average expenses per compromised record and a greater percentage of the IT budget spent on security and a greater percentage of employees with security certification. Nevertheless, there was no apparent effect on this expense from the variety of security training hours performed by each employee in a calendar year ($p=0.728$). Therefore, while certification and investment are important, the connection to the per-record breach cost is complicated, suggesting more valuable data or more advanced systems in more resourceful organizations.

Table 5

Chi-Square Test for AI Implementation and Security Readiness

Variable	Chi-Square Value	Degrees of Freedom	p-value	Cramer's V	Interpretation
AI Implementation vs. Security Measures	8.76	1	0.003	0.83	Strong association
Hospital Size vs. AI Implementation	10.21	1	0.001	0.89	Very strong association
Hospital Size vs. Security Measures	9.34	1	0.002	0.86	Very strong association

The Chi-Square test results in Table 5 show that in Table 5.1, when hospitals are grouped based on the value of the median, the parameter values show strong and statistically significant relationships (all $p < 0.003$, Cramer's $V > 0.83$). The stronger the security measures you adopt, the more you correlate them with the deployment of AI. Furthermore, important correlations exist between larger hospitals and a greater rate of security measures adoption along with a higher level of AI application. This implies that there is a linked progression with the larger

institutions in front in AI adoption and related security readiness.

Table 6
Regression Analysis of Security Measures Impact on Recovery Time

Predictor Variable	Coefficient	Standard Error	t-Statistic	p-value	95% CI Lower	95% CI Upper
Intercept	28.74	3.56	8.07	<0.001	20.28	37.20
Security Budget	-1.87	0.58	-3.22	0.018	-3.27	-0.47
Security Training Hours	-0.94	0.43	-2.19	0.047	-1.86	-0.02
Security Certification	-0.08	0.03	-2.67	0.031	-0.15	-0.01
Cyber Insurance	-0.05	0.09	-0.56	0.594	-0.27	0.17
R^2	0.923	-	-	-	-	-
Adjusted R^2	0.873	-	-	-	-	-
Model p-value	0.002	-	-	-	-	-

The regression analysis for Table 6 (Adjusted R^2 = 0.873, Model p = 0.002) models the variables impacting breach recovery time. Increased security budget allocation, more hours spent on security training, larger percentages of employees, security certificates (p=0.018, p=0.047, and p=0.031, respectively), and reduced breach recovery times are substantially correlated. These results provide evidence of the observable benefits of allocating resources to some of the elements of operational security. Surprisingly, the existence of cyber insurance (p = 0.594) did not significantly affect recovery time in this model.

SUGGESTIONS FOR FURTHER STUDY AND APPLICATION

- The organisation can create AI specific security framework to secure the healthcare institution from the specific weaknesses of the AI such as adversarial attack, model poisoning and training data security. The major focus of future research should be in the development and validation of the AI specific security assessment instruments for healthcare applications.
- Practice Put Size Appropriate Security Strategies: Hospital size and its capability of security are very related, small hospitals could create shared resources, cooperative security agreements, and cloud based security solutions that allows them to provide an enterprise level protection with minimum internal resources.
- Data Driven Strategy For Security Budget allocation models: Organizations can improve their Security budget allocation models through statistical correlation between investment and results. Further research should develop predictive models for how much money should be spent by a company on security with expenditures allocated across staff, technology, and training.
- With hospitals using AI and hospitals using AI deploying the technology, create AI Ethics and Privacy Committees: Make specialty ethics and privacy committees to oversee the use of AI and data governance and make up the membership of said committee an array, an array of administrators, clinicians, technical experts, legal experts, the patient advocates.
- Provide highly technical training: Healthcare institutions can equip the technical personnel and physicians with highly technical training in order to develop them as specialist security persons, focusing to teach security about risks and weaknesses relating to AI. There is research needed to find the best training approaches for the different stakeholder groups.
- Clinical and administrative systems dependent on AI must have its own recovery plans for security incident, or establishment of Recovery and Continuity Plans for AI Systems. These strategies should encompass assurances of service availability as well as data integrity.
- Improve overall Security for AI Development

Environments: Overall, the security protocols in place for the environment where AI models are built and augmented, needs to be increased with attention towards protecting the training data set in particular.

- Create Common Security Measures for AI Powered Medical Applications: For benchmarking and consistent development, industry wide set standards for healthcare AI applications security parameters need to be created and followed.

CONCLUSION

The comprehensive study of AI-driven healthcare systems in US hospitals that raises such impressive trends and issues from technology suppliers, healthcare administrators, security experts, and legislature requires urgent intervention. The study suggests that, although the AI deployment is advancing in both hospital spectra, hospital size or type, as organizational characteristics, has a concrete impact on the security measures and their capabilities. Overall, the number of healthcare breaches increased by 11 percent from 2018 to 2023 along with the number of hacking and IT events like this, up 29 percent. The statistical study allows me to confirm strong relationships between healthcare organizations' hospital size and preparedness for security ($r > 0.98$), which is worrisome as healthcare organizations keep using AI while they cannot provide enough security to protect themselves. Strategic security spending is a factor that helps financial research predict the cost to the organization and how quickly a breach can be closed. The results of this study indicate that all our security certifications, training hours, and the budget allocation were statistically significant determinants for security success in the organization. Within this dataset, embracing the most notable finding of a huge mismatch between the hospitals that announce an AI system is 'HIPAA compliant' (85.7%) and the hospitals that indeed have AI security teams (49.3%). Additionally, the 8.5 days recovery time for profit systems and the 15.8 days for critical access hospitals indicate that organizational resources and security readiness have a significant impact on the organizational resilience. This means that security and privacy issues need to be factored in at all stages of compliance, not as afterthoughts, and that such issues have to be taken into account throughout the entire lifecycle of using AI in a healthcare domain because it is of increasing importance for AI, for example, for tasks such as clinical decision support or administrative automation. Given these problems, we propose an evidence-based basis for the interventions, spend allocations, and legislative actions that would strengthen the responsible development of AI in healthcare.

REFERENCES:

[1] Office for Civil Rights (OCR). (2023). *Breach portal: Notice to the Secretary of HHS breach of unsecured protected health information*. U.S. Department of Health and Human Services. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[2] American Hospital Association (AHA). (2023). *Annual survey database*. American Hospital Association. https://www.ahadata.com/aha-annual-survey-database

[3] Healthcare Information and Management Systems Society (HIMSS). (2024). *2023 HIMSS healthcare cybersecurity survey*. HIMSS. https://www.himss.org/resources/himss-healthcare-cybersecurity-survey

[4] Nemec Zlatolas, L., Welzer, T., &Lhotska, L. (2024). Data breaches in healthcare: security mechanisms for attack mitigation. Cluster computing, 27(7), 8639-8654. https://link.springer.com/content/pdf/10.1007/s10586-024-04507-2.pdf

[5] Mosaddeque, A., Rowshon, M., Ahmed, T., Twaha, U., & Babu, B. (2022). The Role of AI and Machine Learning in Fortifying Cybersecurity Systems in the US Healthcare Industry. Inverge Journal of Social Sciences, 1(2), 70-81. https://www.academia.edu/download/120831716/THE_ROLE_OF_AI_AND_MACHINE_LEARNING_IN_FORTIFYING_CYBERSECURITY.pdf

[6] Riad, A. K. I., Barek, M. A., Rahman, M. M., Akter, M. S., Islam, T., Rahman, M. A., ... & Ahamed, S. I. (2024, July). Enhancing HIPAA Compliance in AI-driven mHealth Devices Security and Privacy. In 2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC) (pp. 2430-2435). IEEE. https://ieeexplore.ieee.org/abstract/document/10633430/

[7] Fernandes, A., Figueiredo, M., Carvalho, F., Neves, J., & Vicente, H. (2021). Threat Artificial Intelligence and Cyber Security in Health Care Institutions. In Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities (pp. 319-342). Cham: Springer International Publishing. https://link.springer.com/chapter/10.1007/978-3-030-72236-4_13

[8] Li, X., Zhang, L., Yang, J., & Teng, F. (2024). Role of artificial intelligence in medical image analysis: A review of current trends and future directions. Journal of Medical and Biological Engineering, 44(2), 231-243. https://link.springer.com/article/10.1007/s40846-024-00863-x

[9] Ahmed, N. B. (2022). Cybersecurity in Healthcare System: Evaluation and Assessment of the Cybersecurity

readiness of Mobile Field Hospital's Resilience (Doctoral dissertation, IMT-MINES ALES-IMT-Mines Alès Ecole Mines-Télécom). https://theses.hal.science/tel-04097342/
[10] Sharova, D. E., Zinchenko, V. V., Akhmad, E. S., Mokienko, O. A., Vladzymyrskyy, A. V., & Morozov, S. P. (2021). On the issue of ethical aspects of the artificial intelligence systems implementation in healthcare. Digital Diagnostics, 2(3), 356-368. https://jdigitaldiagnostics.com/DD/article/view/77446
[11] Reddy, J. (2021). Data breaches in healthcare security systems (Master's thesis, University of Cincinnati). https://search.proquest.com/openview/7d6cbfe0d7d40f7341ed68767061cf01/1?pq-origsite=gscholar&cbl=18750&diss=y
[12] Almalawi, A., Khan, A. I., Alsolami, F., Abushark, Y. B., Alfakeeh, A. S., &Mekuriyaw, W. D. (2022). Analysis of the exploration of security and privacy for healthcare management using artificial intelligence: Saudi hospitals. Computational intelligence and neuroscience, 2022(1), 4048197. https://onlinelibrary.wiley.com/doi/abs/10.1155/2022/4048197
[13] Meisner, M. (2017). Financial consequences of cyber attacks leading to data breaches in healthcare sector. Copernican Journal of Finance & Accounting, 6(3), 63-73. https://apcz.umk.pl/CJFA/article/view/16356
[14] Marks, M., & Haupt, C. E. (2023). AI chatbots, health privacy, and challenges to HIPAA compliance. Jama, 330(4), 309-310. https://jamanetwork.com/journals/jama/article-abstract/2807170
[15] Esmaili, A., Rahmani, A., Alijanpour, A., Jayervand, F., Akhondzardaini, R., Sharifi, M. H., ... &Neamatzadeh, H. (2025). Challenges for Ethics Review Committees in Regulating Medical Artificial Intelligence Research. Indian Journal of Surgical Oncology, 1-12. https://link.springer.com/article/10.1007/s13193-025-02229-4