Journal of Information Systems Engineering and Management
2025, 10(59s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Governance Strategies for Safeguarding Protected Health Information (PHI) in Healthcare: A Review on Policies, Practices, and Challenges

Seyyed Zair Husain Rizvi [a], Mohammad Faisal [a*]
[a] *Department of Computer Application, Integral University, Lucknow, India*
[a*] *Department of Computer Application, Integral University, Lucknow, India*

ARTICLE INFO

Received: 30 Dec 2024

Revised: 12 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

Purpose & Objective:

Purpose & Objective:

The aim of this review is to evaluate the effectiveness of key international and national regulations in protecting PHI. It also investigates the role of internal governance practices—such as risk management, access control, and employee training—in improving compliance and security, and explores the opportunities and challenges presented by emerging technologies like artificial intelligence (AI) and blockchain.

Methodology:

This review synthesizes evidence from empirical studies, industry reports, and case analyses. Comparative evaluation of regulatory provisions is combined with an assessment of organizational strategies to identify strengths, weaknesses, and gaps in PHI governance and protection.

Outcomes:

Findings indicate that although regulations such as HIPAA, GDPR, DPDPA, and DISHA provide a strong foundation for PHI governance, their effectiveness is hindered by organizational shortcomings. Human error, weak incident response planning, and insufficient staff training remain primary contributors to data breaches. While technologies like AI and blockchain can enhance PHI security, they introduce new compliance and integration challenges.

Conclusion:

The review concludes that effective PHI protection requires a balance between regulatory compliance and strong internal governance. Healthcare organizations must adopt proactive measures, including continuous employee education, regular risk modeling, and responsible integration of advanced technologies. Future governance efforts should remain dynamic and adaptive, evolving alongside technological advancements and emerging threats to ensure robust protection of sensitive patient information.

Keywords— Index Terms: PHI, Governance, GDPR, DISHA, HIPAA, GDPR, Cybersecurity

INTRODUCTION

Protected Health Information (PHI) refers to any patient or personal health data that is generated, saved, or transmitted by organizations providing healthcare services [1]. It contains various types of sensitive information i.e. medical documents and reports, patient billing information, diagnosis reports, treatment plans, and patient identification data. Therefore, PHI is extremely important as it protects patient privacy and builds trust in healthcare [2].

Proper management of PHI helps healthcare professionals to provide the desired care without compromising the confidentiality of patient's personal sensitive data. However, due to its highly sensitive nature, it is also the most lucrative target of cybercriminals for financial gain by stealing the person's identity, insurance fraud, or ransomware attacks [3]. In an increasingly digital healthcare environment, the security of such information is critical to maintaining the privacy and integrity of patient data and maintaining the credibility of the healthcare universe. Even a small PHI violation can have serious consequences for both patients and healthcare providers. For patients, it can lead to mental trauma due to identity theft, economic loss, and misuse of their medical history [4].

Healthcare service providers may face severe consequences, including legal penalties, regulatory penalties, and reputational damage. Therefore, the healthcare sector is consistently considered one of the most cherished prey for cybercriminals, with data breaches costing millions of dollars [5]. In addition, due to advances in healthcare systems delivery complexities with the adoption of Electronic Health Records (EHRs), telemedicine channels, and wearable health devices, complexity of PHI become multifold, making it even more challenging to protect ever before [6]. This precludes the implementation of a robust data privacy governance framework for the security of health data including policies, procedures, and rules that define how PHI is collected, stored, shared, and protected.

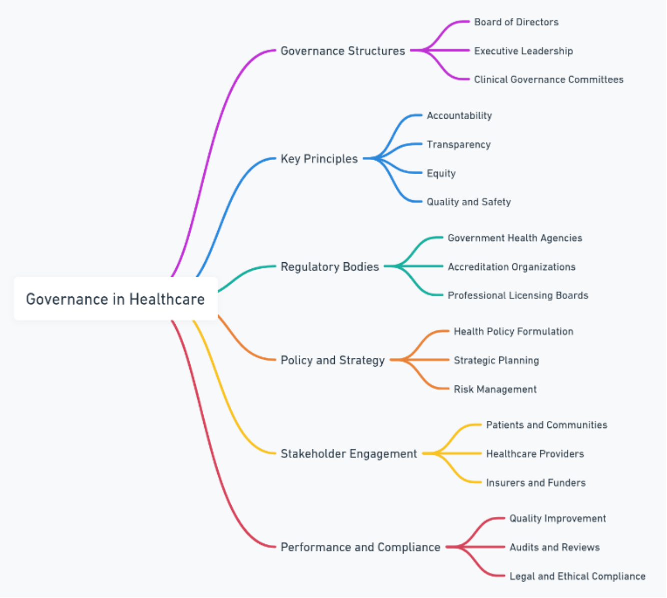

Figure 1: Governance in Healthcare

Objectives of the Review:

The primary purpose of this review is to carry out a comprehensive review of the existing technologies, laws and regulations and industry best practices that determine the foundry or structure for PHI security initiatives, evaluate their effectiveness in mitigating risks and ensure compliance with regulatory standards. The review focuses on several key goals that are important for understanding the current landscape of PHI security and identifying areas for improvement.

- Examining the Governance Framework for PHI Security
- Evaluating the effectiveness of regulatory compliance
- Identifying challenges in implementing governance policies
- Analysis of the role of emerging technologies in PHI conservation
- Assessing incident response and risk management strategies
- Highlighting global governance and cross-border data challenges
- Providing recommendations for improving future governance.

Methodology

Component	Details
Databases Used	PubMed IEEE Xplore Google Scholar ScienceDirect

	ACM Digital Library ProQuest EBSCOhost
Purpose of Each Database	- *PubMed*: Health info systems & cybersecurity - *IEEE Xplore*: AI, blockchain, technical PHI security - *Google Scholar*: General peer-reviewed papers - *ScienceDirect*: Multidisciplinary studies - *ACM DL*: Computer science & data governance - *ProQuest/EBSCO*: Business & management aspects of governance
Search Terms Used	- "PHI Governance" - "PHI Safety in Healthcare" - "Healthcare data breach" - "HIPAA Compliance and Governance" - "GDPR and PHI protection" - "Healthcare Risk Management and Cybersecurity" - "AI/ML in PHI Security Governance" - "Blockchain in Healthcare Governance" - "Incident Response to Healthcare Data Breaches" - "Cross-border data sharing in healthcare"
Boolean Operators	Used operators like AND, OR, NOT to refine searches (e.g., "PHI protection AND healthcare governance")
Inclusion Criteria	- Published between 2014-2024 - Peer-reviewed articles, conference papers, or reports - Direct relevance to PHI governance - Covers India, US, EU, and global regions with governance focus
Exclusion Criteria	- Published before 2013 - Non-peer-reviewed sources (e.g., blogs, opinions) - Redundant or outdated studies
Screening Process	- Manual title & abstract review - Full-text retrieval for qualifying studies - Discrepancies resolved through team discussion
Snowballing Technique	- References from key studies reviewed for additional literature
Data Extraction Focus	- Governance frameworks - Regulatory compliance (HIPAA, GDPR) - Risk management practices - Incident response mechanisms - Role of emerging tech (AI, Blockchain)
Final Outcome	- A synthesized and critical analysis of governance strategies - Identification of literature gaps and areas for improvement in PHI protection

REVIEW OF LITERATURE

The security of sensitive health information and data is governed by a number of regulatory frameworks designed to ensure patient privacy, data security, and ethical handling of sensitive health information. Two of the most prominent regulations are the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union.

The Digital Personal Data Protection Act (DPDPA) provides a much-needed legal framework to address the challenges posed by India's rapidly growing digital health ecosystem, including the integration of electronic health records (EHRs), telemedicine, and health apps. The DPDPA also mandates data localisation for sensitive personal data, which means that PHI must be stored within India, ensuring its own protection against potential breaches [7]. International counterparts, such as HIPAA in the U.S. and the GDPR in the European Union (EU), the DPDPA presents challenges in implementation, particularly for smaller healthcare providers who may struggle with the financial and technical resources needed to comply with its strict requirements. Many researchers, cybersecurity and legal experts questioned that while the DPDPA is a robust framework, it requires continuous review and update to keep it pace with emerging health technologies like artificial intelligence (AI) and Internet of Things (IoT) devices, which poses new threats, risks and challenges for data security governance [8][9][10][11]. The research has emphasised on the extreme importance of a robust and comprehensive risk management frameworks for the Indian healthcare sector. DISHA emphasizes the need for continuous monitoring and third-party risk assessments to protect sensitive personal data as Indian healthcare organizations are adopting cloud-based services due to performance, scalability, availability and reduced cost and management flexibility. Furthermore, small healthcare service providers are facing multiple challenges in establishing advanced risk management, security monitoring and incident response capabilities, due to limited technical and financial resources and a clear framework or regulation in place. This in result is making them more vulnerable to cyber threats. Integrating risk management frameworks are the exigency of the time to aligned with regulations such as DISHA to mitigating cybersecurity risks, especially as Indian healthcare institutions expand their digital infrastructure [12]. In 2015, Anthem Inc., which is a major U.S. health insurance player, experienced a biggest ever data breaches that exposed the personal information of around 78.8 million patients. This breach was launched through a sophisticated phishing attack, which granted unauthorized access to attackers to Anthem's database which was containing unencrypted personal data, including names, Social Security numbers and dates of birth of millions of citizens. Initial probe into the breach revealed that the root cause of this was the absence of encryption controls in place for data at rest and insufficient periodic employee awareness and training on how to recognizing phishing emails. This incident emphasized heavily on the need to implement strong encryption technologies like Attribute-Based Encryption (ABE), Tokenization with Vaultless Architecture together with Hardware Security Modules (HSM) for robust encryption measures and cryptographic key management. Moreover, a comprehensive training and awareness plan for staff and third-party vendors need to be in place as integral components of internal robust and effective governance strategies [13][14][15]. Similarly, the University of California, San Francisco (UCSF) also faced a ransomware attack of same magnitude that disrupted the School of Medicine's critical IT systems and service. The attackers encrypted data on several servers, asking UCSF to pay a heavy ransom of amount $1.14 million to decrypt and regain access to institute data. This incident again highlighted the importance of a robust cybersecurity measures Encryption, of data at rest, motion and in use, periodic and granular access review and regular risk assessments and security audits, up-to-date incident response plans, and comprehensive staff training and awareness plan to mitigate such types of emerging threats [16][17][18].

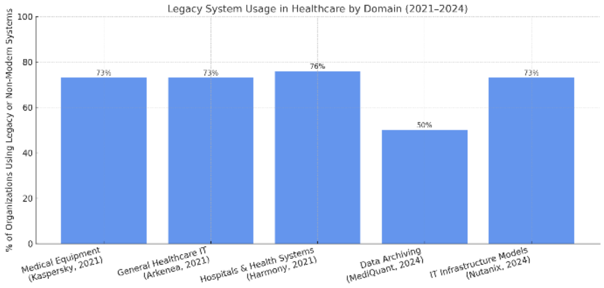

Fig 2: Legacy System Usage in Healthcare (2021–2024)

Recent data from 2021 to 2024 shows that legacy systems are still widely used across different sections of the healthcare industry, despite growing modernization efforts. For example, in 2021, studies by Kaspersky and Arkenea found that around 73% of healthcare providers relied on outdated systems in both medical equipment and general IT infrastructure [19][20]. Similarly, Harmony Healthcare IT reported that 76% of hospitals and health systems were using legacy platforms at that time [21]. MediQuant found that 50% of health systems and 30% of clinics still use inhouse data archiving solutions [22]. Even though more organizations adopt sophisticated and modern IT models, like hybrid multi-cloud systems but a latest report of Nutanix in 2024 showed that 73% of healthcare providers still use mixed infrastructure environments, which often include legacy components. Though these numbers are not encouraging yet can promise a slow but steady pace of healthcare IT transformation and the challenges of moving away from legacy systems entirely [23]. In late 2022, All India Institute of Medical Sciences (AIIMS) experienced a major cyberattack that compromised the health data of millions of patients. The breach exposed the personal and medical data of more than 40 million patients and individuals, exposing serious vulnerabilities in internal security measures and practices. The investigation revealed that AIIMS had inadequate encryption protocols in place and no comprehensive incident response plan. The hackers demanded a hefty ransom in cryptocurrencies, which paralyzed AIIMS IT systems and critical services for days [24].

Another similar incident happened with Indian Council for Medical Research (ICMR) in 2023 in which the organization was targeted by cybercriminals resulting in the detection of sensitive health data of 81 crore Indians. This breach again proved that the existing regime was a significant failure, exacerbating the issue with outdated security infrastructure, unauthorized access, inadequate training & awareness and not having a proper breach notification protocols and ineffective incident management and communication Plan. The incident highlighted the urgent need for Indian health institutions to adopt robust governance frameworks, including encryption, access control, and proper staff training and awareness [25]. In July 2020, Haldiram a prominent Indian food and snack manufacturers also faced ransomware attack that badly affected the operation of its digital operations. Attackers not only infiltrated the company's internal systems rather encrypted the sensitive data and applications. The attackers demanded a ransom of $750,000 to decrypt the encrypted files. An official First Information Report (FIR) was filed in Noida, India, in October 2020. Haldiram's stakeholders refused to pay the ransom due to efficient and tested BCP plan which helped the organization to restore encrypted data from most recent backup [26]. Post-incident analysis revealed the existence of various significant gaps in cybersecurity practices and protocols, including a lack of timely updates, insufficient threat detection systems, and limited employee awareness of phishing and malware risks. This case is often referred as a whistle blower or an eye opener across industries to conduct regular vulnerability assessments, implement robust backup strategies, and proactive incident response plans.

CONCLUSION

This review has examined the various aspect of data breaches and its causes and discussed about the critical role of a robust cybersecurity governance in place to combat emerging data security threat and their change landscape for protecting PHI. It is also found that the organization who doesn't have a decent level of encryption and Access controls in place, updated Incident response and Communication plan, a functional BCP/DR Plan faced data breaches. The emphasis is also given on the very neglecting element in PHI governance i.e. an updated training and awareness plan in place. The review also shed light on various gray areas in focusing on how regulatory policies, organizational strategies, and emerging technologies impact healthcare data protection. The findings show that while frameworks such as HIPAA, GDPR, DPDPA, provide the necessary procedural and administrative controls for the protections of PHI. However, the concern is about how to bring it on the ground and that too in an effective manner. Future research should focus on developing governance frameworks specifically designed for emerging technologies such as AI, blockchain, and IoT. Policymakers and researchers should explore how these technologies can be integrated into health care systems safely and in compliance with privacy regulations. International collaboration is vital for comprehensive patient care cosmos. Additional research is needed to identify the best strategies to help small healthcare organizations enhance their governance capabilities. This includes developing cost-effective solutions for risk management, incident response, and employee training, as well as exploring public-private partnerships to provide the necessary resources.

As cyber threats evolve, there is a pressing need of global information-sharing networks that allow healthcare organizations to exchange real-time threat intelligence. Further research is needed to develop effective models for global collaboration in cybersecurity that can protect PHI from sophisticated attacks. Effective governance is essential to ensure the protection of PHI in an increasingly complex and digital healthcare landscape. As cyber threats and technological innovation continue to evolve, healthcare organizations, policymakers, and international bodies must collaborate to develop governance frameworks that are dynamic, adaptable, and align with the latest advancements.

By addressing gaps in current governance strategies, harmonizing global regulations, and fostering innovation while maintaining data security, the healthcare system can ensure that patient data remains secure in the future.

REFERENCES

[1] Amin, M. A., Tummala, H., Shah, R., & Ray, I. Balancing Patient Privacy and Health Data Security: The Role of Compliance in Protected Health Information (PHI) Sharing, 2024, arXiv preprint arXiv:2407.02766.

[2] Gostin, L. O., Friedman, E. A., Buse, K., Waris, A., Mulumba, M., Joel, M., ... & Sridhar, D. Towards a framework convention on global health. Bulletin of the World Health Organization, 2013, 91, 790-793,.

[3] Tariq, R. A., & Hackert, P. B. Patient confidentiality. In *StatPearls* (Treasure Island, FL:2018, StatPearls Publishing). https://www.ncbi.nlm.nih.gov/books/NBK519545/

[4] Edemekong, P. F., Annamaraju, P., & Haydel, M. J. Health Insurance Portability and Accountability Act. In StatPearls, 2018, StatPearls Publishing. https://www.ncbi.nlm.nih.gov/books/NBK500019/

[5] Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. Healthcare data breaches: insights and implications. In Healthcare, 2020, Vol. 8, No. 2, p. 133, MDPI

[6] Cobrado, U. N., Sharief, S., Regahal, N. G., Zepka, E., Mamauag, M., & Velasco, L. C. Access control solutions in electronic health record systems: A systematic review. Informatics in Medicine Unlocked,2024 101552.

[7] Sood, A., Mishra, D., Surya, V., Singh, H., Sundaresan, R., Pal, D., Dharmaraju, R., Satish, R., Mishra, S., Chavan, N. A., Mondal, S., Duggal, P., & Iyer, V. K. Challenges and recommendations for enhancing digital data protection in Indian medical research and healthcare sector. NPJ Digital Medicine,2025, 8, 48, https://doi.org/10.1038/s41746-025-01448-x

[8] Walia, H., Chandan, A., & Lal, V. Analysing AI and The Digital Personal Data Protection Act 2023. Khaitan & Co, 2024. https://compass.khaitanco.com/analysing-ai-and-the-digital-personal-data-protection-act-2023

[9] Mohamed, B. Five ways in which the DPDPA could shape the development of AI in India. Future of Privacy Forum., 2024. https://fpf.org/blog/five-ways-in-which-the-dpdpa-could-shape-the-development-of-ai-in-india/

[10] Bhat, K. Safeguarding the digital frontier: Indian Digital Personal Data Protection Act 2023 and its approach to emerging technologies, 2023. The Financial Express. https://www.financialexpress.com/business/industry-safeguarding-the-digital-frontier-indian-digital-personal-data-protection-act-2023-and-its-approach-to-emerging-technologies-3318141/

[11] Jamal, M. K., & Faisal, M. Machine learning-driven implementation of workflow optimization in cloud computing for IoT applications. *Internet Technology Letters*, e571.

[12] Seven Step Consulting. DISHA: Transforming Digital Health Data Security in India, 2025 https://www.sevenstepconsulting.com/disha-transforming-digital-health-data-security-in-india/

[13] HIPAA Journal. Anthem Inc. Settles State Attorneys General Data Breach Investigations and Pays $48.2 Million in Penalties, 2020. https://www.hipaajournal.com/anthem-inc-settles-state-attorneys-general-data-breach-investigations-and-pays-48-2-million-in-penalties/

[14] Healthcare Innovation. Anthem Agrees to Record Payment—$16M—for Largest U.S. Health Data Breach, 2018. https://www.hcinnovationgroup.com/cybersecurity/news/13030802/anthem-agrees-to-record-payment16mfor-largest-us-health-data-breach

[15] Threat Intel Report. The Anthem Data Breach of 2015: Navigating the Cybersecurity Landscape, 2020. https://www.threatintelreport.com/2020/07/17/incident_reports/the-anthem-data-breach-of-2015-navigating-the-cybersecurity-landscape/

[16] UCSF News. Update on IT Security Incident at UCSF, 2020. https://www.ucsf.edu/news/2020/06/417911/update-it-security-incident-ucsf

[17] Winder, D. The University Of California Pays $1 Million Ransom Following Cyber Attack. Forbes, 2020. https://www.forbes.com/sites/daveywinder/2020/06/29/the-university-of-california-pays-1-million-ransom-following-cyber-attack/

[18] Miliard, M. UCSF pays $1.14 million to decrypt files after ransomware attack. Healthcare IT News, 2020. https://www.healthcareitnews.com/news/ucsf-pays-114-million-decrypt-files-after-ransomware-attack

[19] Kaspersky. 73% of healthcare providers use medical equipment with a legacy OS, 2021. https://www.kaspersky.com/about/press-releases/2021_legacy-os-healthcare

[20] Arkenea. Legacy systems in healthcare: Challenges and solutions, 2021. https://arkenea.com/blog/legacy-systems-in-healthcare

[21] Harmony Healthcare IT. What is a legacy system in healthcare?, 2021. https://www.harmonyhit.com/what-is-a-legacy-system-in-healthcare

[22] MediQuant. Healthcare data archiving: Still stuck in the past?, 2024. https://www.mediquant.com

[23] Nutanix. Healthcare enterprise cloud index report, 2024. https://www.nutanix.com/enterprise-cloud-index India Times. Explained: What's happening at AIIMS after sensitive ransomware attack?, 2022. https://www.indiatimes.com/explainers/technology/explainer-aiims-ransomware-attack-586542.html

[24] Economic Times. (2023, October 31). ICMR data leak reveals personal info of 81.5 cr Indians: Report, 2023. https://health.economictimes.indiatimes.com/news/health-it/icmr-data-leak-reveals-personal-info-of-81-5-cr-indians-report/104838324

[25]Times of India. Haldiram's hit by ransomware attack, hackers asked for $7.5L, 2020. https://timesofindia.indiatimes.com/city/noida/haldirams-hit-by-ransomware-attack-hackers-asked-for-7-5l/articleshow/78712465.cms

ACKNOWLEDGEMENTS

I would like to thank integural university authorities, the Hon'ble Founder & Chancellor S. W. Akhtar, Vice Chancellor, Javed Musarrat and Head, Department of Computer Application Prof. Mohammad Faisal for their unconditional support. A Manuscript communication number (IU/R&D/2025MCN00032….) for internal communication was also provided by Dean, Doctoral StudiesProf. Wahajul Haq Integral University.