Commentary

Navigating Data Governance in Digital Health: Balancing Privacy and Innovation in Global South

Pradeep Nair[1]

1. Sabin Center for Climate Change Law, Columbia Climate School, Columbia University, United States

In recent time, the cases of data breaches in healthcare sector has increased largely in comparison to other care/service sectors because healthcare data is more in demand in the black market than any other type of data as it takes more time to discover healthcare fraud and the stolen data can be used for longer period in the cases of chronic diseases. Healthcare sector is also vulnerable in terms of immediate breach notification measures which delay the process of estimating the volume of data compromised due to ransomware attacks. The data breach challenges in health systems have revealed that there is an enormous amount of personal patient data lying with various health agencies which are vulnerable and prone to cyber-attacks. This brief urges that if these health-data were collected, stored, analysed and secured properly, they could help the populous countries like India, China and Brazil to focus on long-term measures to build a resilient health governance system to prevent, prepare and respond to future health-related challenges along with maintaining essential health services.

Corresponding author: Pradeep Nair, nairdevcom@hpcu.ac.in

Digital health has evolved rapidly since its inception. In countries like India, China and Brazil, healthcare data governance is an emerging concept whereas in USA, UK and Japan it has now advanced in terms of regulatory frameworks, standardized protocols, information technology infrastructure, and semantic models. In developing economies like India, China, Brazil, Indonesia, the Ministries of Health and other public agencies are working hard in developing policies and regulations to ensure the safe and secure use of healthcare data. The digital health priorities focus on a safe and secure digital environment to manage the handling, storing and sharing of real-time patient data 24x7 across hospitals and healthcare

 doi.org/10.32388/FKC58C

institutions with clearly defined policies and procedures. The efforts aim to create a national digital health ecosystem, which includes a personal health ID for every citizen, a digital repository of health records, and federated health data architecture to enable secure sharing of data among different stakeholders.

The Data Breach Challenges of Global South

In 2025, the healthcare data sector in Global South faced significant cyber threats in terms of cross-border data privacy and a high volume of ransomware attacks. The healthcare sector of India, China and Brazil faced an all-time high data breach cases by a 30% surge in ransomware attacks and intensified targeting of hospital infrastructure. The average total organizational cost of data breach in India reached INR 200 million in 2025, 13% higher than 2024. Whereas, for Brazil it reached R$ 7.19 million, a 6.5% increase from the previous year. Interestingly, the healthcare sector in Brazil is the hardest hit with average data breach costs hitting R$ 11.43 million. The average global breach costs in China increased from $7.42 million to $10 million per incident and have been considered as the costliest among other care/service industries over a decade [1].

The Post-Covid Challenges

The pandemic Covid-19 has taught both the developed and developing economies across the globe that all of us are living in an interdependent world. The challenge is not only to ensure robust data privacy and security but to foster innovation in digital health solutions. The concern is to set high standards for the protection of patient data confidentiality, maintaining the legal and ethical considerations, and to redefine the role of technologies such as artificial intelligence (AI) and machine learning (ML) in mitigating risks and safeguarding sensitive information through strict regulatory compliance [2]. While delivering her key note address at the Regional Open Digital Health Summit 2025 convened in New Delhi, India on 19th and 20th November 2025, Paula Salila Srivastava, Union Health Secretary, Government of India urged that – “many countries, particularly those with diverse healthcare infrastructures like India, China are navigating these challenges in the wake of COVID-19 through harmonized regulatory frameworks, advanced technological tools, and inter-regional collaboration. They are taking various actionable insights at the policy and governance level to protect sensitive health data, ensure compliance, and fostering public trust in digital healthcare systems,”. She further states that the post-Covid challenges in health systems are to explore the potential of the enormous amount of personal patient data available

with various health agencies. Their collection, storage, analysis and security helps populous countries like India, China and Brazil to focus on long-term measures to build a resilient health governance system to prevent, prepare and respond to future health-related challenges along with maintaining essential health services [3]. The prioritisation of digital health by these countries are pressing the use of cutting-edge digital tools for healthcare with a more specialized and efficient oversight system to spot irregularities and opportunities in real-time fitting well within the data governance plan. This compels these countries to regulate the efficient and intentional movement of data throughout a healthcare system [4].

Balancing Privacy and Innovation

Data privacy in healthcare is all about protecting sensitive patient information, including diagnostic and treatment records, personal identifiers, clinical outcomes from unauthorised access, misuse, or disclosure. Sharing of this information needs a warranty from the healthcare agencies to be protected under legal regulations and ethical standards [5]. The World Health Organization (WHO) has clearly defined that healthcare data privacy as the implementation of measures that guarantee the confidentiality, integrity, and availability of patient information. Since, medical data is directly connected to patient care; it requires robust safeguards and stricter protection.

Thibaut Kleiner, Director, Communication Networks, Content and Technology DC Connect, at the European Commission argued that many countries of Global North like the United States, Spain, Belgium, France, Germany, Japan, South Korea emphasizes on explicit consent, data minimization, and comprehensive technical and system safeguards while sharing patent data [6]. Whereas, in contrast, countries from Global South like India, China, Brazil, Indonesia, South Africa emphasizes on interoperable and culturally tailored privacy protection mechanisms. While addressing the International AI Summit at Brussels, Belgium in December 2025, Niamh Smyth TD, Minister of State at the Department of Enterprise, Tourism and Employment with special responsibility for Trade Promotion, AI and Digital Transformation, Irish Government advocated that the diverse regulatory approaches shows how Global South and Global North countries interact and negotiate with digital healthcare systems and cyber security infrastructures to protect patient healthcare data [7]. She highlighted that “the US, Japan and South Korea with established regulations were somehow successful in safeguarding sensitive patient information through regulatory frameworks mandating measures to access restrictions to patient data, encryption protocols, and immediate breach notification while sharing electronically protected health

information". Despite efforts to expand the integration of Electronic Health Records (EHRs) in an increasingly digitalized healthcare landscape, the healthcare systems of countries like India, China, Singapore is still vulnerable to the risk of data breaches and unauthorized access [8]. They are facing the challenges related to inadequate encryption and resource constraints.

Pragmatic Strategies – Toward a harmonized future

While looking at the legal, ethical, and technical dimensions of data privacy, it was observed that there are diverse regulatory frameworks adaptable to regional nuances and system requirements. The technological solutions like blockchain and AI can help to safeguard data integrity and transparency by enabling real-time breach detention, predicting risk assessment and by automating compliance monitoring. But technological innovations need to be aligned well with stringent privacy protection to bridge the current security gaps [9]. Many health data experts like Kieu Quang Tuan from National Health Informatics Center, Ministry of Health, Vietnam; Jai Ganesh Udayasankaran, the Executive Director of Asia eHealth Information Network (AeHIN) advocate that "a detailed analysis of regulatory policies and frameworks of both Global South and Global North could certainly help the healthcare providers and data experts to understand the diversity in data compliance and enforcement in the context of governing healthcare data privacy in different geographical regions. It will be useful to understand the barriers in system innovation to work on strategies for overcoming resistance". The identification of system vulnerabilities and the loopholes of cyber-security in countries like India, China and Brazil are useful in exploring the potential of AI, ML and blockchain to mitigate these vulnerabilities and to design customized solutions through policy recommendations [2]. This further helps in finding regionally adaptable regulatory approaches to manage data privacy among healthcare stakeholders.

The only understanding of technological dimensions of data privacy challenges is not enough to negotiate and maintain patient trust in digital health environments. The critical role of healthcare institutions and social mechanism shall also be considered to examine how and on what basis patient share their sensitive health information. Preserving the confidentiality and trust of the patient, the ethical decision-making, the patient-provider relationship dynamics, and respecting patient rights is foremost important in an era of pervasive digital connectivity [10][5]. A comprehensive understanding of regulatory frameworks, cross-border collaboration, integration of technologies, trust-building, and ethical decision-making would be useful to adapt a harmonized data protection strategy for countries

like India, China and Brazil to reinforce trust, accountability, and data protection to sustain and strengthen their digital health innovations in an interconnected world [9].

Moving Forward

In an evolving data-driven era, effective health data management in terms of ensuring data privacy and compliance is a growing concern for developing countries who are still struggling to deal with the complexities of modern digital healthcare. The healthcare system reforms in countries like India, China and Brazil needs continuous improvement and adaptation to proactively embrace and refine their data governance models, regulatory capacities and AI infrastructures to better position themselves at the forefront of patient care, innovation and operational excellence. The countries of Global South have to prepare their digital healthcare systems ready to adapt comprehensive data governance strategies to foster a culture of trust and transparency to maintain ethical, efficient, and patient-centric healthcare delivery while safeguarding patient rights.

References

1. ^*Conduah AK, Ofoe S, Siaw-Marfo D (2025). "Data Privacy in Healthcare: Global Challenges and Solutions." Digital Health. **11**. doi:10.1177/20552076251343959.*
2. a, b*Oktaviana RS, Handayani PW, Hidayanto AN (2024). "Health Organization Challenges in Health Data Governance Implementation: A Systematic Review." J Infrastruct Policy Dev. **8**(6):3892. doi:10.24294/jipd.v8i6.3892.*
3. ^*Mayor A, Hamainza B, Roca-Feltrer A (2026). "Collective Action for Responsible Global Health Data Sharing and Use." BMJ Glob Health. **11**:e022013. doi:10.1136/bmjgh-2025-022013.*
4. ^*Li L, Back E, Lee S, Shipley R, Mapitse N, Elbe S, Smallman M, Wilson J, Yasin I, Rees G, Gordon B, Murray V, Roberts SL, Cupani A, Kostkova P (2025). "Balancing Risks and Opportunities: Data-Empowered-Health Ecosystems." J Med Internet Res. **27**:e57237. doi:10.2196/57237. PMID 40132190.*
5. a, b*Ahmed A, Shahzad A, Naseem A, Ali S, Ahmad I (2025). "Evaluating the Effectiveness of Data Governance Frameworks in Ensuring Security and Privacy of Healthcare Data: A Quantitative Analysis of ISO Standards, GDPR, and HIPAA in Blockchain Technology." PLoS One. **20**(5):e0324285. doi:10.1371/journal.pone.0324285.*

6. ^Cervera de la Cruz P, Lalova-Spinks T, Shabani M (2026). "The European Health Data Space: An Opportunity to Strengthen Citizen Rights and Engage Citizens in Health Data Governance." Front Med. **12**:1699941. doi:10.3389/fmed.2025.1699941.
7. ^Deghati S (2024). "Impact of Data Governance on Data Quality in Healthcare Institutions." Am J Data Inf Knowl Manag. **5**(1):39–48. doi:10.47672/ajdikm.2351.
8. ^OECD, World Health Organization (2024). "Health at a Glance: Asia/Pacific 2024." OECD Publishing. doi:10.1787/51fed7e9-en.
9. a, bGalvin M, Heverin M, Mac Domhnaill É, Mcfarlane R, Meldrum D, Murray D, Bolger A, Connelly J, Flynn K, Fox E, Gibbons F, Hederman L, Impey S, O'Keefe I, O'Meara C, McKibben D, Nicholson M, Stephens G, Van Dijk J, Van Den Berg L, Hardiman O (2025). "Challenges and Solutions to Complex Data Governance Issues in Cross-National, Cross-Sectoral, Multidisciplinary Real World Health Research: A Descriptive Overview." Amyotroph Lateral Scler Frontotemporal Degener. **26**(sup1):1–7. doi:10.1080/21678421.2024.2428927.
10. ^Van Scharen A, Cruyt K, Colon J (2026). "Unlocking Health Data for Research, Legal, Technical and Organizational Lessons from a Belgian Interdisciplinary Case Study." J Healthc Inform Res. **10**:179–208. doi:10.1007/s41666-025-00220-w.

Declarations

Funding: No specific funding was received for this work.

Potential competing interests: No potential competing interests to declare.