Data Governance and Cybersecurity in Digital Healthcare: A Comparative Literature Review of Global Frameworks and India's Regulatory Ecosystem

A Dissertation as a prerequisite for the award of

PGDM

[Hospital and Health Management]

By

Dr. Pearl Jaggi

(PG/23/078)

At

International Institute of Health Management Research [IIHMR], Delhi

Under the guidance of

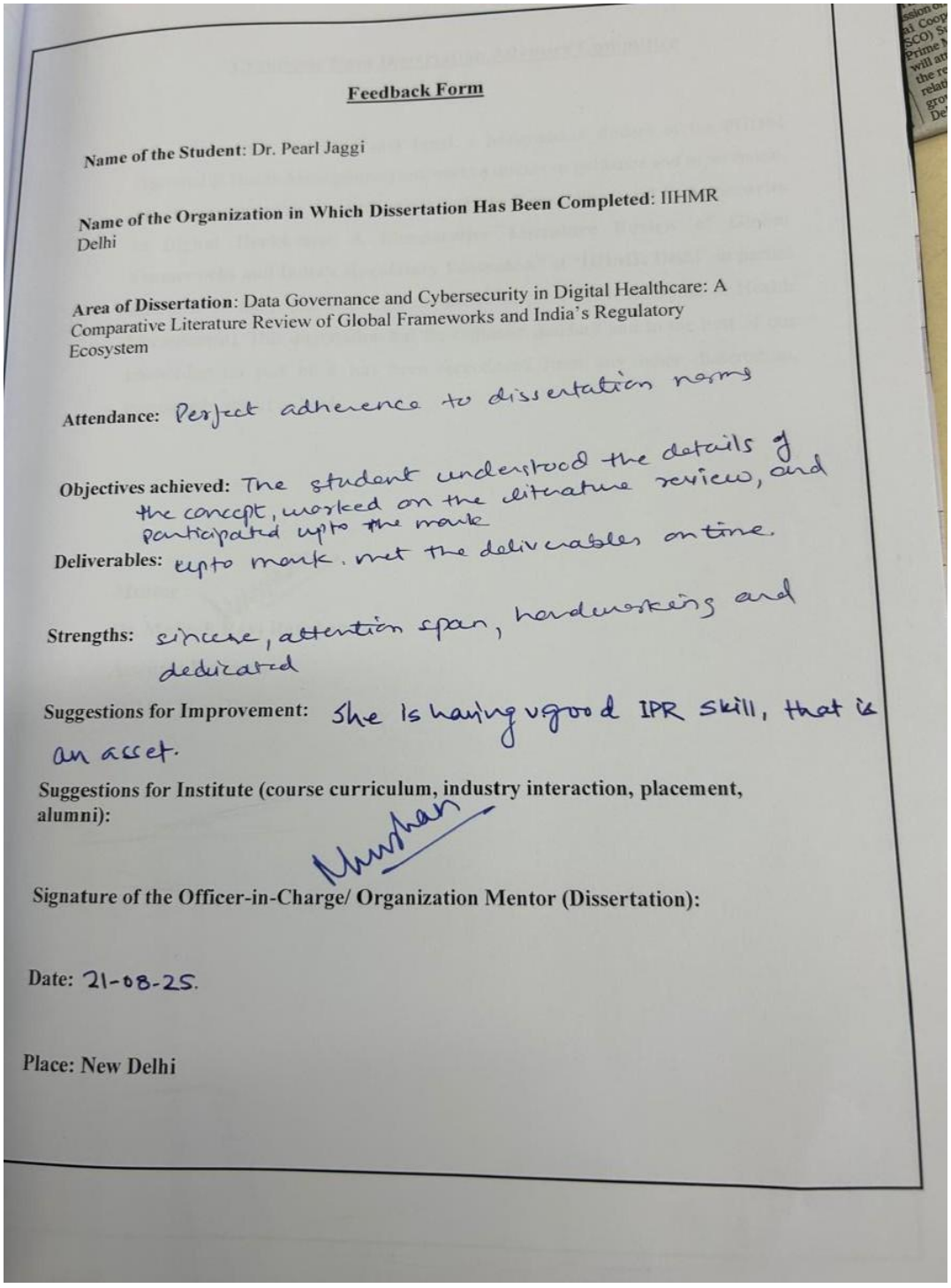
Dr. Mukesh Ravi Raushan

Assistant Professor, IIHMR, New Delhi

International Institute of Health Management Research, New Delhi

2025

Feedback Form



Feedback Form

Name of the Student: Dr. Pearl Jaggi

Name of the Organization in Which Dissertation Has Been Completed: IIHMR Delhi

Area of Dissertation: Data Governance and Cybersecurity in Digital Healthcare: A Comparative Literature Review of Global Frameworks and India's Regulatory Ecosystem

Attendance: Perfect adherence to dissertation norms

Objectives achieved: The student understood the details of the concept, worked on the literature review, and participated upto the mark

Deliverables: upto mark. met the deliverables on time.

Strengths: sincere, attention span, hardworking and dedicated

Suggestions for Improvement: She is having v good IPR skill, that is an asset.

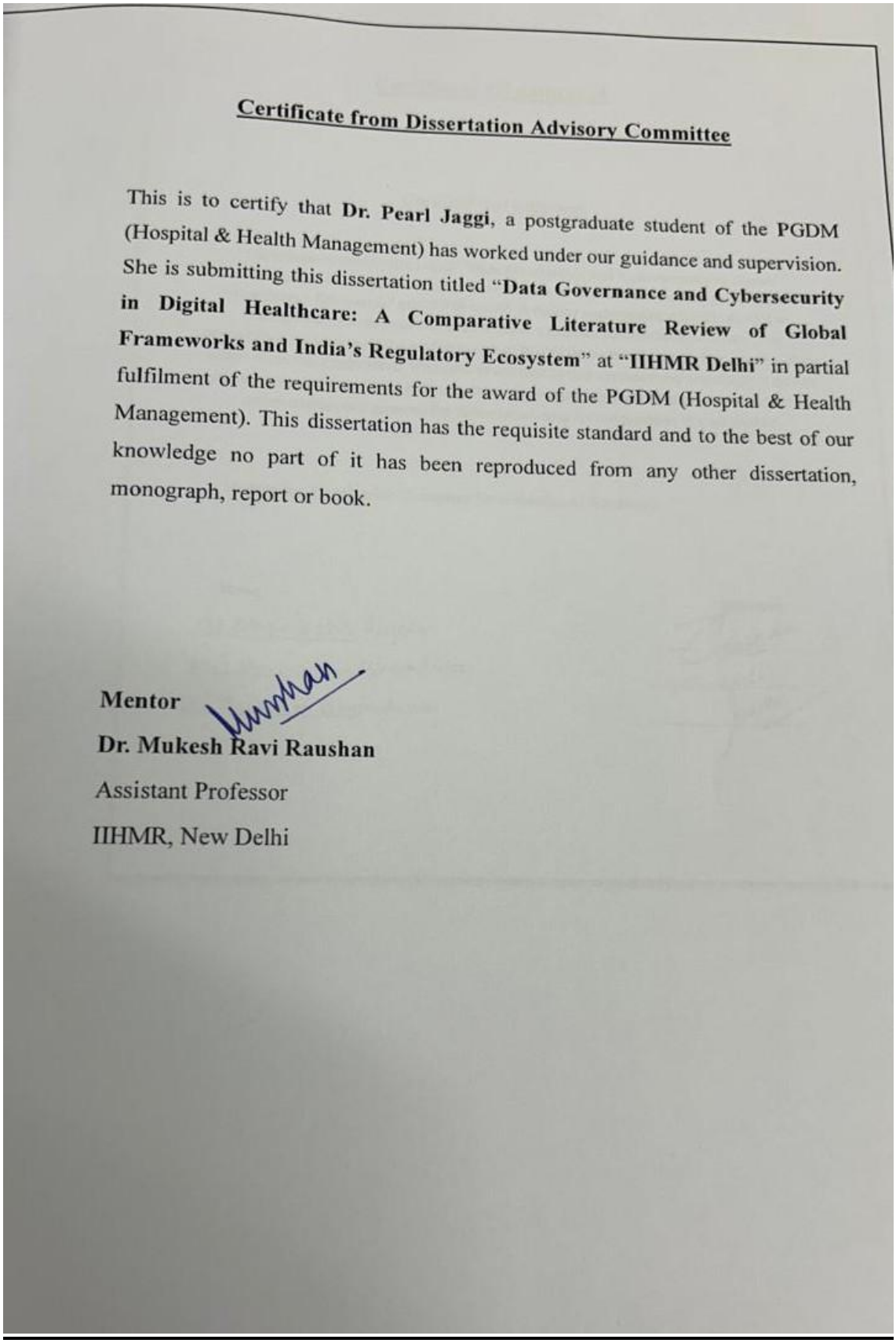
Suggestions for Institute (course curriculum, industry interaction, placement, alumni):

Signature of the Officer-in-Charge/ Organization Mentor (Dissertation):

Date: 21-08-25.

Place: New Delhi

Certificate from Dissertation Advisory Committee



Certificate from Dissertation Advisory Committee

This is to certify that **Dr. Pearl Jaggi**, a postgraduate student of the PGDM (Hospital & Health Management) has worked under our guidance and supervision. She is submitting this dissertation titled "**Data Governance and Cybersecurity in Digital Healthcare: A Comparative Literature Review of Global Frameworks and India's Regulatory Ecosystem**" at "**IIHMR Delhi**" in partial fulfilment of the requirements for the award of the PGDM (Hospital & Health Management). This dissertation has the requisite standard and to the best of our knowledge no part of it has been reproduced from any other dissertation, monograph, report or book.

Mentor

Dr. Mukesh Ravi Raushan

Assistant Professor

IIHMR, New Delhi

Certificate Of Approval

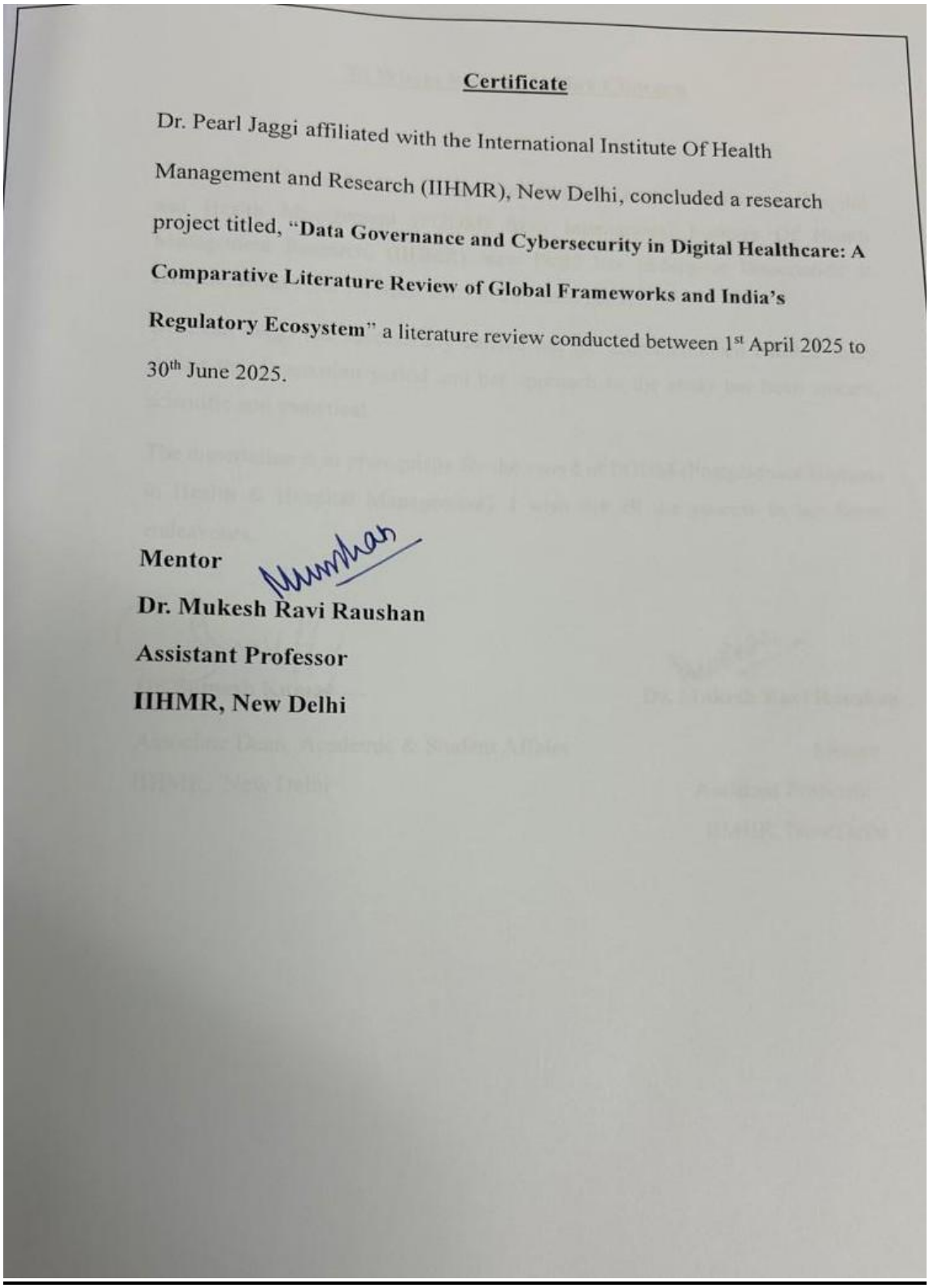
Certificate of Approval

The following dissertation titled **"Data Governance and Cybersecurity in Digital Healthcare: A Comparative Literature Review of Global Frameworks and India's Regulatory Ecosystem"** at **"IIHMR Delhi"** is hereby approved as a certified study in management carried out and presented in a manner satisfactorily to warrant its acceptance as a prerequisite for the award of **PGDM (Hospital & Health Management)** for which it has been submitted. It is understood that by this approval the undersigned do not necessarily endorse or approve any statement made, opinion expressed, or conclusion drawn therein but approve the dissertation only for the purpose it is submitted.

Dissertation Examination Committee for evaluation of dissertation.

Name	Signature
Ms. Akanksha Rajeev	
Ms. Anuradha Bhardwaj	
Dr Sukesh Bhardwaj	

Certificate



Certificate

Dr. Pearl Jaggi affiliated with the International Institute Of Health Management and Research (IIHMR), New Delhi, concluded a research project titled, "**Data Governance and Cybersecurity in Digital Healthcare: A Comparative Literature Review of Global Frameworks and India's Regulatory Ecosystem**" a literature review conducted between 1st April 2025 to 30th June 2025.

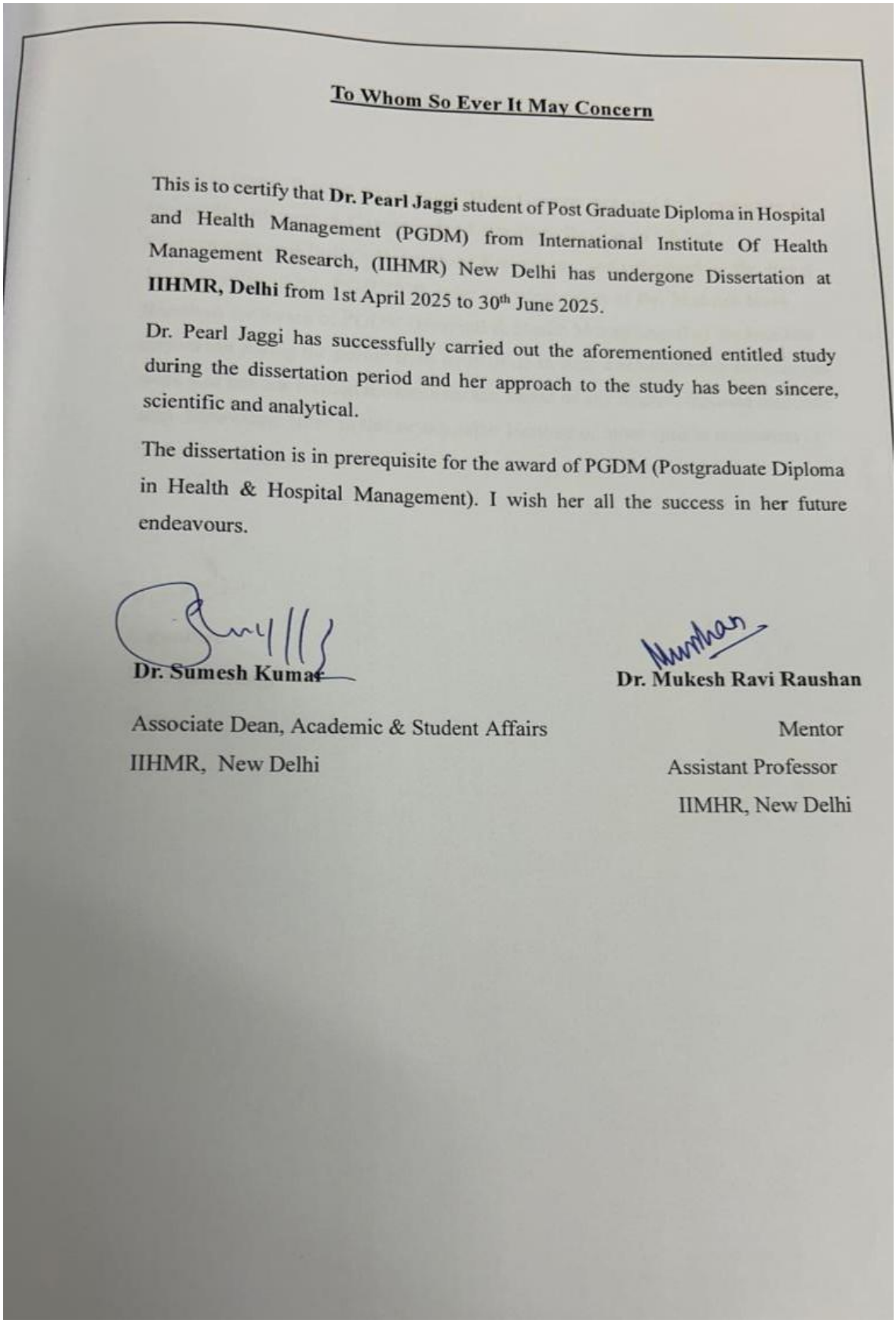
Mentor

Dr. Mukesh Ravi Raushan

Assistant Professor

IIHMR, New Delhi

To Whom So Ever It May Concern



To Whom So Ever It May Concern

This is to certify that **Dr. Pearl Jaggi** student of Post Graduate Diploma in Hospital and Health Management (PGDM) from International Institute Of Health Management Research, (IIHMR) New Delhi has undergone Dissertation at **IIHMR, Delhi** from 1st April 2025 to 30th June 2025.

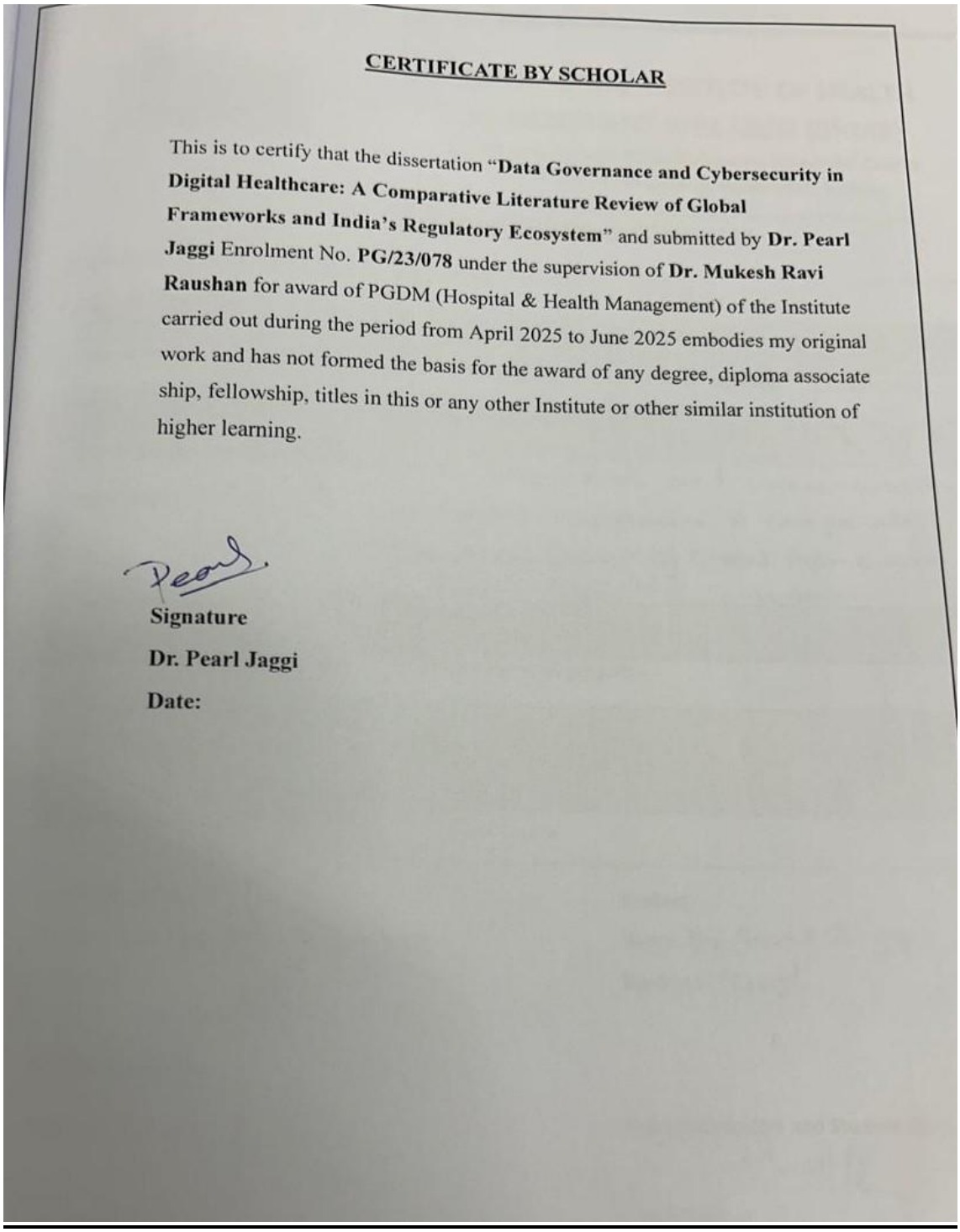
Dr. Pearl Jaggi has successfully carried out the aforementioned entitled study during the dissertation period and her approach to the study has been sincere, scientific and analytical.

The dissertation is in prerequisite for the award of PGDM (Postgraduate Diploma in Health & Hospital Management). I wish her all the success in her future endeavours.

Dr. Sumesh Kumar
Associate Dean, Academic & Student Affairs
IIHMR, New Delhi

Dr. Mukesh Ravi Raushan
Mentor
Assistant Professor
IIMHR, New Delhi

CERTIFICATE BY SCHOLAR



CERTIFICATE BY SCHOLAR

This is to certify that the dissertation "**Data Governance and Cybersecurity in Digital Healthcare: A Comparative Literature Review of Global Frameworks and India's Regulatory Ecosystem**" and submitted by **Dr. Pearl Jaggi** Enrolment No. **PG/23/078** under the supervision of **Dr. Mukesh Ravi Raushan** for award of PGDM (Hospital & Health Management) of the Institute carried out during the period from April 2025 to June 2025 embodies my original work and has not formed the basis for the award of any degree, diploma associate ship, fellowship, titles in this or any other Institute or other similar institution of higher learning.

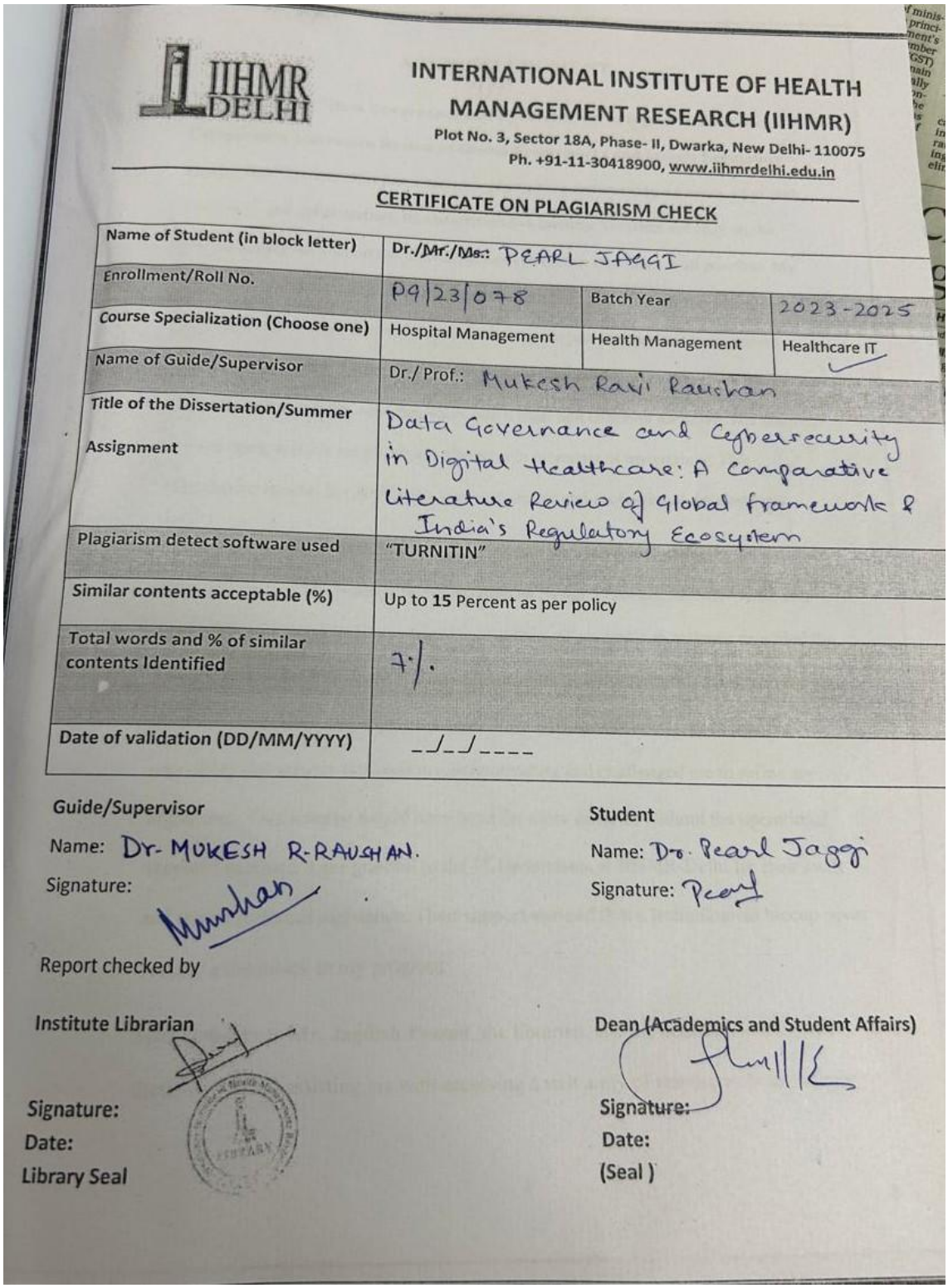
Pearl

Signature

Dr. Pearl Jaggi

Date:

CERTIFICATE ON PLAGIARISM CHECK



IIHMR DELHI

INTERNATIONAL INSTITUTE OF HEALTH MANAGEMENT RESEARCH (IIHMR)

Plot No. 3, Sector 18A, Phase- II, Dwarka, New Delhi- 110075
Ph. +91-11-30418900, www.iihmrdelhi.edu.in

CERTIFICATE ON PLAGIARISM CHECK

Name of Student (in block letter)	Dr./Mr./Ms.: PEARL JAGGI		
Enrollment/Roll No.	P9|23|078	Batch Year	2023-2025
Course Specialization (Choose one)	Hospital Management	Health Management	Healthcare IT ✓
Name of Guide/Supervisor	Dr./ Prof.: Mukesh Ravi Raushan		
Title of the Dissertation/Summer Assignment	Data Governance and Cybersecurity in Digital Healthcare: A Comparative Literature Review of Global Frameworks & India's Regulatory Ecosystem		
Plagiarism detect software used	"TURNITIN"		
Similar contents acceptable (%)	Up to 15 Percent as per policy		
Total words and % of similar contents Identified	7%		
Date of validation (DD/MM/YYYY)	__/__/____		

Guide/Supervisor
Name: Dr. MUKESH R. RAUSHAN.
Signature: Mukesh

Student
Name: Dr. Pearl Jaggi
Signature: Pearl

Report checked by

Institute Librarian
Signature:
Date:
Library Seal

Dean (Academics and Student Affairs)
Signature:
Date:
(Seal)

ACKNOWLEDGMENT

This dissertation, **"Data Governance and Cybersecurity in Digital Healthcare: A Comparative Literature Review of Global Frameworks and India's Regulatory Ecosystem,"** is more than just a research paper; it's a testament to a journey of growth, discovery, and collaboration. Its completion is a moment to reflect not only on the subject matter but also on the incredible support system that made it all possible. My most profound gratitude goes to my mentor and guide, **Dr. Mukesh Ravi Raushan**. His influence on this work is immeasurable. He was not just a supervisor but a patient teacher and a steadfast source of encouragement. He challenged me to think more critically and transform complex ideas into a clear and coherent narrative. His door was always open, and his insights were a beacon in moments of uncertainty. This dissertation reflects his dedication to my academic and professional development.

I also want to acknowledge the environment that allowed this research to flourish. My sincere thanks to **Dr. Sutapa Bandhopadhyay Neogi**, Director, IIHMR-Delhi. Her leadership and commitment to fostering a culture of academic excellence provided the ideal backdrop for this study. To the entire faculty of IIHMR-Delhi, thank you for your diverse perspectives and support always. Your willingness to engage in thought-provoking discussions enriched my understanding and challenged me to refine my arguments. This journey would have been far more difficult without the operational support I received. I am grateful to the IT Department at IIHMR-Delhi for their swift and expert technical assistance. Their support ensured that a technological hiccup never became a roadblock to my progress.

Special thanks to **Mr. Jagdish Prasad**, the librarian, and his dedicated staff. Their tireless efforts in assisting me with accessing a vast array of resources, from obscure

journals to essential frameworks, laid the groundwork for the literature review. Their guidance was a lifeline in the sea of available information.

I am deeply grateful for the inputs of my colleagues. The conversations we shared, the advice we exchanged, and the feedback we gave each other were a crucial part of this process. Their willingness to share their experiences and expertise helped me navigate my own challenges and provided invaluable clarity.

Finally, I'm incredibly grateful to my family and friends for their unwavering support. My deepest appreciation goes to my husband, whose guidance helped me find the right path for my work. His unwavering belief in me was a constant source of strength and motivation. And to my two-year-old son, thank you for being an unexpected source of inspiration and a joyful reminder of the future I am working to build. This dissertation is as much a tribute to their support as it is to my own hard work. Their love, patience, and understanding provided a much-needed sanctuary from the rigors of research.

And to anyone else who contributed in their own small way, perhaps with a kind word or a moment of encouragement, I thank you. This accomplishment is a testament to a collective effort, and I am humbled and grateful to everyone who was a part of it.

Above all, I extend my deepest thanks to The Divine providing me with the strength and positivity to see this through.

LIST OF ABBREVIATIONS

S.No	Symbol	Abbreviations
1.	ABDM	Ayushman Bharat Digital Mission
	ABHA	Ayushman Bharat Health Account
	DISHA	Digital Information Security in Healthcare Act
	DPB	Data Protection Board (of India)
	DPDP Act	Digital Personal Data Protection Act, 2023
	DPO	Data Protection Officer
	DSP Toolkit	Data Security and Protection Toolkit
	EHR	Electronic Health Record
	GDPR	General Data Protection Regulation
	HDMP	Health Data Management Policy
	HIPAA	Health Insurance Portability and Accountability Act
	HITECH	Health Information Technology for Economic and Clinical Health Act
	IT Act	Information Technology Act, 2000
	MoHFW	Ministry of Health and Family Welfare
	NCIIPC	National Critical Information Infrastructure Protection Centre
	NDHM	National Digital Health Mission
	NHA	National Health Authority
	NHS	National Health Service
	PHI	Protected Health Information
	PM-JAY	Pradhan Mantri Jan Arogya Yojana

Abstract

Background: Digital healthcare is expanding globally, raising crucial concerns about patient data privacy and cybersecurity. Mature regulatory frameworks such as the United States' HIPAA (Health Insurance Portability and Accountability Act) and HITECH Act, the European Union's GDPR (General Data Protection Regulation), and the United Kingdom's NHS Data Security and Protection Toolkit provide robust standards for data governance in healthcare. India, meanwhile, is advancing its own regulatory ecosystem—including the Digital Personal Data Protection (DPDP) Act 2023, the Ayushman Bharat Digital Mission (ABDM), and legacy provisions under the IT Act—yet questions remain on how these measures stack up against global best practices. The main research question guiding this study is: What are the gaps and challenges of India's data governance and cybersecurity policies in digital healthcare when compared with global standards?

Objectives: This comparative literature review aims to:

(1) understand global frameworks related to data governance and cybersecurity in healthcare; (2) examine India's current digital health regulations (including the DPDP Act 2023, ABDM, and IT Act); and

(3) identify gaps and challenges by comparing India's approach with global frameworks.

Methods: A systematic literature review of policy documents, legal frameworks, and scholarly analyses was conducted. Key international frameworks (HIPAA, HITECH,

GDPR, NHS Toolkit) and Indian regulations were reviewed. No primary data were collected; instead, a qualitative comparative analysis was done focusing on areas such as regulatory scope, privacy provisions, security standards, enforcement mechanisms, and infrastructure readiness. Sources included academic journals, government publications, and industry reports. The Vancouver style has been used for citations.

Results: Global frameworks have well-defined standards for protecting healthcare data. HIPAA (augmented by HITECH) in the US mandates strict privacy controls for personal health information, including prohibitions on disclosure without patient consent (except for treatment, payment, or healthcare operations) , and requires covered entities to implement administrative, physical, and technical safeguards. HITECH broadened HIPAA's scope by directly regulating business associates and imposing breach notification requirements.

The GDPR in the EU treats health data as "special category" sensitive data, requiring explicit consent or other stringent legal bases for processing, and mandates Data Protection Impact Assessments for high-risk processing including health data . GDPR also empowers individuals with strong data rights and imposes severe penalties for violations (up to 4% of global turnover).

The UK's NHS Data Security and Protection Toolkit operationalizes these principles within healthcare organizations through annual self-assessments against ten security standards (covering areas like staff training, access control, incident response, and up-to-date cybersecurity practices). Compliance with the NHS toolkit is mandatory for organizations handling NHS patient data, aligning with GDPR and building a culture of data security and accountability .

In comparison, India's regulatory ecosystem is in a formative stage. The DPDP Act 2023 is India's first comprehensive data protection law, recognizing privacy as a fundamental right and establishing obligations for data fiduciaries. It provides a framework for consent-based processing and enforcement via a Data Protection Board, with penalties up to ₹250 crore for data breaches. However, unlike GDPR, the DPDP Act does not explicitly categorize health data as sensitive nor require additional safeguards for it.

India's Ayushman Bharat Digital Mission (ABDM) has introduced a Health Data Management Policy that espouses "privacy by design" and a consent-driven model for sharing health records . ABDM's federated architecture allows patients to control access to their digital health records via consent managers, ensuring data is shared only with explicit patient consent and employing encryption and anonymization techniques.

The Information Technology Act 2000 and its 2011 "Reasonable Security Practices and Sensitive Personal Data" Rules previously served as an interim regime: they defined medical records as sensitive personal data and required organizations to implement security safeguards (with liability for negligence under Section 43A).

However, these provisions lacked sector-specific guidance and enforcement rigor, and they are now largely superseded by the DPDP Act. A proposed law specific to health data, the Digital Information Security in Healthcare Act (DISHA), was drafted to establish dedicated health data authorities and stricter consent requirements, akin to HIPAA , but it has not been enacted. This leaves India with a general data protection law (DPDP) and various policies, but no singular health-sector law.

Conclusions: The comparative analysis reveals significant gaps and challenges for India. Global frameworks illustrate the importance of tailored healthcare data regulations, strict breach notification duties, and well- resourced enforcement. India's

DPDP Act is a milestone, yet gaps include the absence of special protections for health data, unclear guidelines for health data exchange in clinical practice, limited obligations for proactive security measures, and broad exemptions (e.g., potential government agency carve-outs) . In practice, Indian healthcare institutions often lag in cybersecurity preparedness, as evidenced by high-profile incidents like the 2022 ransomware attack on AIIMS Delhi that compromised millions of patient records and exposed lapses in basic security hygiene. This study underscores the need for India to address these gaps by learning from global standards: adopting stricter health data regulations (or sectoral rules under the DPDP framework), mandating robust cybersecurity protocols and breach reporting in healthcare, investing in infrastructure and training, and strengthening enforcement through dedicated bodies. By doing so, India can better protect patient privacy and build trust in its digital health initiatives. The dissertation offers recommendations for policy enhancement and suggests areas for further research, including evaluating the effectiveness of these measures over time. Overall, while India's digital health ecosystem is advancing, aligning more closely with international best practices is crucial to ensure that the benefits of digital health do not come at the cost of patient privacy or safety.

CHAPTER 1 INTRODUCTION

1.1 Background

Healthcare is in the midst of a digital transformation globally. Electronic Health Records (EHRs), telemedicine, health information exchanges, and AI-driven health analytics are becoming commonplace. This digital health revolution promises improved

patient outcomes, operational efficiencies, and data-driven public health interventions. The World Health Organization's Global Strategy on Digital Health 2020–2025 emphasizes maximizing these benefits while ensuring that patient data privacy, confidentiality, and security are robustly protected. Health data is considered highly sensitive personal information; its mishandling can lead to identity theft, discrimination, or harm to patient welfare. Consequently, data governance and cybersecurity have emerged as critical components of digital health systems worldwide.

In response, countries have developed regulatory frameworks to govern how healthcare data is collected, used, shared, and protected. For instance, the United States enacted the Health Insurance Portability and Accountability Act (HIPAA) in 1996, establishing nationwide standards for healthcare data privacy and security. The HIPAA Privacy Rule (2000) and Security Rule (2003) set strict limits on the use and disclosure of Protected Health Information (PHI) and require healthcare providers to implement safeguards for electronic health data. The subsequent HITECH Act of 2009 strengthened these provisions, promoting EHR adoption and tightening enforcement of privacy/security rules. Across the Atlantic, the European Union's General Data Protection Regulation (GDPR), implemented in 2018, is a comprehensive data protection law that has significantly influenced health data governance in EU member states and beyond. GDPR classifies health-related data as "special category" personal data subject to heightened protections, and it enforces principles like consent, data minimization, and accountability on any entity processing personal data, with rigorous penalties for non-compliance. Even sector-specific tools exist; for example, the United Kingdom's National Health Service (NHS) employs the Data Security and Protection Toolkit as an annual self- audit mechanism to ensure that healthcare organizations meet defined cybersecurity and information governance standards.

India, with its vast population and rapidly growing digital infrastructure, stands at a crossroads in shaping its data governance policies for healthcare. Initiatives such as the Ayushman Bharat Digital Mission (ABDM) aim to create an integrated digital health ecosystem, including unique health IDs, interoperable health record systems, and digital health services nationwide. This push towards digital health has highlighted the need for robust data protection measures. Historically, India lacked a dedicated data protection law; instead, privacy protections were scattered across various statutes and IT regulations. In 2017, India's Supreme Court affirmed the fundamental right to privacy, setting the stage for legislative action. After several draft iterations, the Digital Personal

Data Protection Act (DPDPA) 2023 was enacted, signalling a new era in data governance. The health sector is expected to be significantly impacted by this Act, alongside specific guidelines under ABDM and existing IT laws.

However, critical questions arise: How well do India's emerging frameworks protect health data compared to mature systems like HIPAA or GDPR? What gaps remain in terms of legal provisions, implementation capacity, and enforcement in the Indian context? And what challenges do healthcare organizations face on the ground in complying with these standards? High-profile incidents, such as the November 2022 cyberattack on the All India Institute of Medical Sciences (AIIMS) in New Delhi, have exposed vulnerabilities – the attack crippled hospital IT systems for weeks, compromised roughly 4 million patient records (including those of high-profile individuals), and underscored deficiencies in cybersecurity preparedness. Such events highlight that policy frameworks, no matter how well-crafted, must be effectively implemented and supported by infrastructure and awareness.

In this backdrop, the present study undertakes a comparative analysis of global data governance frameworks in comparison to India's regulatory ecosystem for digital health. It operates as a literature-based inquiry, given that India's approach is still evolving and no primary data is collected. By examining global best practices and India's current trajectory, the study seeks to identify gaps and recommend pathways to strengthen data governance and cybersecurity in Indian healthcare.

This literature review is organized into three main parts. Section 7.1 examines global frameworks that set the benchmark for healthcare data governance and cybersecurity (focusing on the US, EU, and UK contexts).

Section 7.2 then reviews India's regulatory ecosystem for digital health data governance, including recently enacted laws and ongoing initiatives. Section 7.3 synthesizes insights from the literature, highlighting key themes such as common principles, and surfacing gaps or debates relevant to the comparative analysis.

1.2 Review of Literature

Global Frameworks for Data Governance in Healthcare

1.2.1 United States: HIPAA and HITECH

HIPAA – Privacy and Security of Health Information: The Health Insurance Portability and Accountability Act (HIPAA) is a landmark US law enacted in 1996, primarily known for its provisions on health data privacy and security. Under the HIPAA Privacy Rule, healthcare providers, insurers, and clearinghouses (collectively termed "covered entities") must protect "Protected Health Information" (PHI) and are generally prohibited from disclosing it without patient consent, except for core purposes of treatment, payment, or health care operations. PHI encompasses individually identifiable health information such as medical histories, test results, insurance information, and other data that relates to a person's health status or healthcare services. HIPAA established a federal floor of privacy protections – meaning states could enact stricter rules but not more lenient ones.

In addition to privacy, HIPAA's Security Rule (effective 2005) specifically addresses electronic PHI (ePHI). It requires covered entities and their business associates (partners who handle PHI on their behalf, like cloud service providers or billing companies) to implement administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI. Examples include access controls (unique user IDs, emergency access procedures), encryption of data, audit controls (tracking system activity), facility security, workforce training, and incident response plans. The Security Rule is designed to be scalable – recognizing that a small clinic's security measures may differ from a large hospital's, but both must perform a risk analysis and apply appropriate safeguards for their size and complexity.

HITECH Act – Strengthening Enforcement and Promoting IT: The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 (part of the ARRA stimulus package) significantly bolstered HIPAA's provisions in two ways. First, it incentivized the adoption of Electronic Health Records through the "Meaningful Use" program, which indirectly improved data governance by encouraging standardization and security in health IT systems. Second, HITECH enhanced privacy and security enforcement: it extended HIPAA compliance directly to business associates (not just through contracts, but by law) and introduced a breach notification rule. Under HITECH's breach notification requirements, healthcare entities must notify affected individuals of any breach of "unsecured" PHI. If a breach affects 500 or more individuals, the entity must also notify the U.S. Department of Health and Human Services (HHS) and in many cases the media . This transparency requirement aimed to

ensure organizations promptly address breaches and that patients are made aware of potential exposure of their data.

Enforcement of HIPAA/HITECH is overseen by the HHS Office for Civil Rights (OCR). Penalties for non- compliance can be substantial – ranging from fines of a few hundred dollars for minor violations (if corrected) to as high as $1.5 million per year for each type of violation, even higher in aggregated cases. The HITECH Act also empowered state attorneys general to bring civil actions for HIPAA violations, further increasing enforcement avenues. Over the years, OCR enforcement actions (including settlements and fines) have reinforced the importance of risk assessments, employee training, and prompt breach reporting in U.S. healthcare organizations.

Key Principles and Practices: From literature and official summaries, several core principles of the U.S. framework can be identified: - Minimum Necessary Use: Only the minimum necessary information should be used or disclosed for a given purpose (this is a HIPAA Privacy Rule standard). - Patient Rights: Patients have rights to access their health records, request corrections, and be informed of how their data is used. These rights empower individuals to be involved in governance of their data. - Security Safeguards: A comprehensive approach to security is mandated, covering administrative policies (like appointing a privacy and security officer, workforce training), physical controls (secure locations for servers, controlled facility access), and technical controls (authentication, encryption, etc.). - Breach Accountability: There is an emphasis on accountability for breaches – requiring notification and subjecting entities to penalties, which creates an incentive to avoid incidents and improve security posture.

Overall, HIPAA and HITECH have created a robust, if complex, framework that has been in place for over two decades. They specifically target the healthcare sector, making the U.S. approach sectoral (as opposed to GDPR's cross-sectoral nature). One limitation often noted in literature is that HIPAA's scope is limited to "covered entities" and their formal business associates. It may not automatically cover emerging digital health tools that patients use directly (like health apps or wearables) unless those tools interface with covered entities. This has led to discussions in the U.S. about extending protections (for example, the proposed U.S. "Health Data Use and Privacy Commission Act" or reliance on the FTC Act for non-HIPAA health data). Nonetheless, HIPAA remains a cornerstone, and its concepts of privacy and security by design in healthcare have influenced laws internationally (including India's thinking in DISHA and the Personal Data Protection Bill drafts as they relate to health information).

1.2.2 European Union: GDPR and Healthcare Data Protection

GDPR – Comprehensive Data Protection with Special Attention to Health: The General Data Protection Regulation (GDPR), effective May 2018, revolutionized data protection law in the EU and has become a global reference point. It is an omnibus law applying to all sectors and types of personal data, but it delineates certain "special categories" of personal data that merit higher protection. These special categories include data concerning health, genetic data, biometric data (when used for identification), among others (like racial or ethnic origin, political opinions, sexual orientation, etc.). Health data under GDPR refers to any data about a person's physical or mental health, including the provision of health services, which reveal information about their health status.

Under GDPR, processing of health data is generally prohibited unless a specific condition is met (Article 9). Conditions that allow processing include: the explicit consent of the data subject, necessity for preventive or occupational medicine or treatment, public health interests (such as protecting against serious cross-border health threats), health research (with appropriate safeguards), etc. Even when allowed, controllers must ensure appropriate safeguards like pseudonymization where possible. This baseline rule – "no processing of health data unless…" – is a stark difference from HIPAA, which permits use within the health system relatively freely for treatment/payment once consent to treat is given. GDPR's approach is more restrictive at face value but provides flexibility through the mentioned exceptions.

Individual Rights and Control: GDPR endows individuals (called "data subjects") with strong rights over their data. These include the right to access their data, correct inaccuracies, and even erase data ("right to be forgotten") in certain conditions. For health data, a patient in the EU could, for example, request a hospital to provide a copy of all their records in a portable format (GDPR's data portability right) – an empowerment tool that also links to health initiatives like MyHealth@EU where patients can use e- prescriptions across member states. GDPR requires that processing be transparent – patients should know what is happening with their data, hence privacy notices must be clear and comprehensive.

Data Security and Breach Notification: GDPR mandates that organizations implement "appropriate technical and organizational measures" to ensure a level of security appropriate to the risk (Article 32). This includes measures such as encryption, ensuring

ongoing confidentiality/integrity/availability, and regular testing of security measures. A concept of "data protection by design and by default" means privacy and security considerations should be embedded in systems from the start, not as an afterthought. Importantly, GDPR introduced a universal breach notification requirement: any personal data breach must be reported to the national Data Protection Authority (DPA) within 72 hours of discovery, unless the breach is unlikely to pose a risk to individuals' rights. If the breach poses a high risk (e.g., sensitive health data leaked), the affected individuals must also be informed without undue delay. This is similar in spirit to HITECH's rules but applies to all sectors and has a very tight reporting timeline.

Enforcement and Penalties: GDPR enforcement is overseen by independent Data Protection Authorities in each EU country, coordinated by a European Data Protection Board. Penalties under GDPR are famously stringent: for serious infringements, fines can go up to €20 million or 4% of the company's worldwide annual turnover, whichever is higher . Notably, by August 2024, cumulative GDPR fines reached ~€4.6 billion, with the healthcare sector accounting for €17 million of that , illustrating active enforcement in health as well. Enforcement can also include orders to stop processing data or mandates to improve practices. GDPR also allows individuals to seek compensation for material or non-material damage resulting from violations, and data subjects can lodge complaints with DPAs.

Comparison within EU (e.g., UK's adaptation): The UK, although no longer in the EU, has incorporated GDPR into its laws (as the UK GDPR and the Data Protection Act 2018). In the healthcare context, the UK's National Health Service has additional tools (like the aforementioned DSP Toolkit) to implement GDPR's requirements in practice, ensuring every NHS-connected entity annually reviews their compliance across key domains (governance, training, technical security, etc.) . The DSP Toolkit's alignment with GDPR means that meeting the toolkit standards inherently moves an organization toward GDPR compliance (for example, Standard 6 and 7 of the toolkit require robust cyber-attack resistance and continuity planning, which complement GDPR's Article 32 security requirements) .

Global Influence: GDPR has influenced privacy laws worldwide (often termed "GDPR-inspired"). Many countries (Brazil's LGPD, Thailand's PDPA, South Africa's POPIA, etc.) have provisions akin to GDPR. Even in India, earlier drafts of the Personal Data Protection Bill had categorized health data as sensitive personal data with explicit consent requirements, reflecting GDPR-like thinking . The DPDP Act 2023 in its final

form took a different approach (dropping special categories), which is a notable divergence that this study will explore. Nonetheless, GDPR's principles – especially user consent, rights, and accountability – serve as a benchmark when assessing any data protection regime, including India's.

1.2.3 United Kingdom: NHS Data Security and Protection Toolkit

While the UK's overarching law for data protection is essentially GDPR-based, the health sector has implemented an additional layer of governance through the NHS Data Security and Protection (DSP)

Toolkit. This is a practical instrument worth examining as a global best practice in sector-specific compliance framework.

What is the NHS DSP Toolkit? It is an online self-assessment tool mandated for all organizations that handle NHS patient data or systems. Each year, organizations (including hospitals, general practices, IT service providers to NHS, etc.) must submit their compliance status against a set of data security standards. The toolkit was born out of recommendations from the National Data Guardian's review and lessons learned from incidents (e.g., the WannaCry cyberattack in 2017 that affected NHS services). It clusters requirements under three broad "Leadership Obligations" – People, Process, and Technology – and enumerates ten Data Security Standards within these categories.

Briefly, the ten standards include: - People (Leadership Obligation 1):

1. Personal confidential data is handled securely and lawfully.

2. All staff understand their responsibilities for data security (with emphasis on following the Caldicott Principles, which are UK's guiding principles on patient information confidentiality).

3. All staff receive annual data security training and pass a mandatory test - Process (Leadership Obligation 2):

4. Access Control: Only authorized staff have access to data they need, and access is removed promptly when no longer needed.

5. Process Review: Organizations annually review their processes, especially after any breaches or near-misses, to improve weak points.

6. Responding to Threats: Defenses against cyber-attacks are in place and updated (including acting on threat advisories), and incidents trigger immediate, appropriate

responses. Notably, serious incidents must be reported to senior management within 12 hours of detection.

7. Continuity Planning: Business continuity plans exist for data and cyber incidents, tested annually, to ensure care can continue in a crisis- Technology (Leadership Obligation 3):

8. No unsupported software or hardware is used – systems must be kept up-to-date (addresses known vulnerabilities by avoiding outdated tech).

9. A strategy (based on recognized cybersecurity frameworks, like Cyber Essentials) is in place to protect IT systems, reviewed annually.

10. IT suppliers (vendors) are held accountable via contracts for protecting data and meeting these standards.

Organizations completing the toolkit answer detailed questions and provide evidence for each requirement. Their submissions yield an overall compliance score, and importantly, it is not just a paperwork exercise – failing to complete the toolkit or address its requirements can result in loss of NHS contracts or other interventions. In essence, the toolkit operationalizes GDPR an broader best practice into concrete checks for healthcare entities.

Benefits and Impact: Literature and NHS guidance highlight that the DSP Toolkit has multiple benefits:

- It ensures Protecting Patient Data in practice by verifying that security controls are not just planned but active

- It aligns with Legal Compliance (GDPR, UK Data Protection Act) so that healthcare providers meet their statutory obligations

- It builds trust among patients and partners – an organization that is DSPT-compliant signals its commitment to data security.

- It improves Information Governance Practices by making organizations regularly review data handling, sharing, and disposal practices.

- It enhances Cyber Resilience and Incident Response, as orgs must show they can detect and respond to incidents (Standards 6 and 7).

From a comparative standpoint, the NHS DSP Toolkit illustrates an approach where a national health system takes ownership of data governance by setting sector-specific expectations on top of general law. This may be a useful model for India, where compliance culture around data protection in health is nascent. For example, India could consider a similar checklist or accreditation for hospitals regarding data security

(perhaps via the National Health Authority or Ministry of Health), especially for participants in ABDM, to ensure consistent adherence to privacy and security norms.

Moreover, the toolkit's existence acknowledges that compliance is not just one-time – it must be continuous and evolving. The NHS updates the toolkit requirements as threats evolve (e.g., adding new questions about cloud security or multi-factor authentication when those become pertinent). This dynamic aspect ensures that the governance framework can adapt to emerging cybersecurity challenges, an aspect crucial for any country's approach.

In summary, the global landscape shows a range of mechanisms: - Laws/Regulations (HIPAA, GDPR) that set enforceable rules and rights. - Incentive and Enforcement Programs (HITECH Meaningful Use, Breach fines) to drive compliance. - Sector Toolkits/Standards (NHS DSP Toolkit, and even international standards like ISO 27799 for health information security) that provide detailed guidance. These components together create a robust data governance ecosystem. The next section turns to India's environment to describe what tools are in place and how they function.

1.2.4 India's Digital Health Regulatory Ecosystem

India's approach to data governance in healthcare is presently a patchwork of general data protection law, sectoral policies, and older IT Act provisions. This section outlines the main elements of this ecosystem, noting recent changes and current status.

1.2.4.1 Digital Personal Data Protection Act, 2023 (DPDPA 2023)

The Digital Personal Data Protection Act, 2023 (DPDP Act) is the centerpiece of India's new data protection regime. Passed by Parliament in August 2023, it represents India's first comprehensive law dedicated to personal data protection. Given that it is a horizontal law (applying to all sectors and types of personal data), it forms the backdrop for health data governance as well. Key features of the DPDP Act include:

• Consent-Oriented Framework: The Act requires that personal data be processed only for lawful purposes and primarily on the basis of an individual's consent (with some

"deemed consent" exceptions). Consent must be "free, specific, informed, unconditional and unambiguous" . For healthcare, this means that, in general, hospitals, apps, or researchers should obtain clear consent from individuals before using their health data, unless an exception applies.

• Legitimate Uses (Deemed Consent): Section 7 of the Act outlines scenarios where data can be processed without explicit consent, which are relevant to healthcare. Two notable clauses are: processing for "responding to a medical emergency involving a threat to the life or immediate health" of a person, and processing for "undertaking measures to provide medical treatment or health services during an epidemic, outbreak of disease or any threat to public health".

These effectively allow sharing/use of personal health data in emergencies and public health situations, aligning with common-sense needs (similar to how HIPAA allows disclosure for treatment emergencies). However, outside of these, routine healthcare operations in non-emergency contexts are not explicitly carved out in the Act, meaning consent would typically be required for most uses of health data in normal care (raising questions on how hospitals will handle consent for standard treatment disclosures, perhaps treating the consent to treatment as also consent to data use – something that might need clarification).

• No Special Category/Sensitive Data Definition: Unlike GDPR (and even unlike India's earlier drafts of data protection bills), the 2023 Act does not classify any personal data as "sensitive" or provide extra safeguards for health data. As the CCG analysis notes, health, genetic, biometric data are treated the same as a person's email or address under the law. This is a significant design choice – it simplifies the law but arguably at the cost of not acknowledging that certain data types (like health) need stronger protection. The Act thus does not mandate, for instance, explicit consent for health data or localization of health data (older drafts had localization for sensitive data). However, the Act does empower the government to notify "significant data fiduciaries" based on factors including volume and sensitivity of data. Hospitals or large digital health platforms might be designated as significant data fiduciaries in the future, which would bring additional obligations like appointing a Data Protection Officer and conducting periodic data protection impact assessments. Those rules are yet to be fleshed out via notification.

• Data Principal Rights: Individuals (data principals) have rights such as the right to access information about personal data processed, and the right to correction and erasure of their data (with some limits). These are relatively basic rights compared to GDPR (which also has data portability and objection rights), but they do offer some control. A specific challenge in health could be how, for example, the right to erasure applies to medical records – generally, medical ethics and other laws require retaining records for a period; the Act does allow refusal of erasure if needed for legal purposes or if the data must be retained by law.

• Data Protection Board and Enforcement: The Act establishes a Data Protection Board of India (DPB) to enforce provisions and adjudicate non-compliance. If a breach or violation occurs, the DPB can impose monetary penalties. Penalties can go up to ₹250 crore (~USD 30 million) for certain major violations . However, notably, any penalties are to be paid into the government's Consolidated Fund, not as compensation to affected individuals . Individuals do not have a direct right to seek compensation under the Act (unlike GDPR's allowance for private lawsuits); they effectively rely on the DPB to take action. Also, the DPB is an administrative body under the central government, raising discussions about its independence.

• Scope and Exemptions: The DPDP Act applies to digital personal data (including data that was initially non-digital but digitized later) . It has broad territorial scope – covering processing within India and processing abroad if it's related to offering goods/services to people in India. Government agencies can be exempted by the central government for certain purposes (national security, law enforcement, etc.). There is concern that health data held by government hospitals or programs could be exempted from some provisions by such powers, though it remains to be seen how the government uses this exemption clause.

Implications for Healthcare: The Act provides a long-awaited legal foundation for privacy, but leaves much to be clarified for healthcare:

- Hospitals and clinics will likely need to institute processes for obtaining and managing patient consent for data usage beyond immediate treatment. They also need to gear up for potential breach notifications (the Act does not explicitly spell out breach reporting obligations to individuals or a timeline, which is a gap.

– Though sectoral regulators like CERT-In have some rules on breach reporting within 6 hours for any organization).

- Health tech companies (telemedicine apps, wearables manufacturers processing health data, etc.) are clearly under the Act's purview. They must implement privacy by design and have mechanisms for users to exercise their rights.

- The lack of a special category means, legally, a data fiduciary might not be obliged to treat health data differently. But prudent practice and other domain-specific norms (like doctor-patient confidentiality under the National Medical Commission guidelines) would compel careful handling. For instance, doctors in India are bound by professional ethics to maintain confidentiality of "every communication" with a patient, though as a paper in Nature (Sood et al. 2025) points out, it's ambiguous how this translates when patients share data via informal channels like WhatsApp. The DPDP Act doesn't directly address these nuances, which leads to uncertainty among practitioners about legal liability for such data sharing necessary for care.

In summary, the DPDP Act is a broad framework setting general principles of consent, use limitation, and penalties. It is a positive development, yet by itself it may not be sufficient to handle the intricacies of health data governance. This is where health-specific policies like ABDM's guidelines come in, which we discuss next.

1.2.4.2 Ayushman Bharat Digital Mission (ABDM) and Health Data Management Policy

The Ayushman Bharat Digital Mission (ABDM), launched nationally in 2021 (after a pilot as National Digital Health Mission, NDHM, in 2020), is the Indian government's flagship program to build a unified digital health infrastructure. It aims to provide every citizen with a unique Health ID (now Ayushman Bharat Health Account – ABHA), enable exchange of health records with consent, and facilitate seamless healthcare delivery through digital means. Recognizing that such an ecosystem must be underpinned by strong data governance, ABDM put forth a Health Data Management Policy (HDMP) as its guiding framework for data privacy and security.

Health Data Management Policy (2020, revised 2022): This policy acts as the sector-specific privacy policy for the ABDM ecosystem. It lays down principles and minimum standards for data privacy that all participants in ABDM (hospitals, labs, health tech services connecting to the network) should adhere to. Key aspects of the policy include:
- Consent-Based Data Sharing: ABDM architecture is built such that personal health information is shared only upon the explicit consent of the individual (data principal). The system uses electronic consent artifacts, which digitally capture the individual's

consent parameters (what data, shared with who, for what purpose, for how long). Users can use a Personal Health Record (PHR) app to manage these consents, and they have the ability to revoke consent at any time 11.

- Privacy by Design: The policy explicitly adopts ‘security and privacy by design’ as a guiding principle 68 . ABDM is architected as a federated system – instead of centralizing all health records in one government database, the data remains at the point of care (e.g., a hospital’s local system) and is shared via network only when needed and authorized . This decentralization reduces the risk of a single catastrophic breach. It also aligns with the idea that those generating the data (hospitals, clinics) continue to be responsible for its security. - Encryption and Security Standards: Data flowing through ABDM (like when a record is transmitted from a hospital to a patient’s PHR) is encrypted end-to-end. The policy sets baseline security requirements for any software systems joining the network (e.g., compliance with certain standards, certification, secure coding, etc.)

- Data Anonymization and Use for Public Good: The policy acknowledges that aggregated, anonymized health data can be extremely valuable for research and public health (like epidemiological trends). It provides for an “anonymizer” service/module that can take personal data and anonymize it, such that individual identities are protected, enabling use of data for analytics without privacy loss. This is crucial for realizing the population health benefits of digitization while respecting individual privacy.

- Alignment with Global Standards: It is noted that ABDM’s data management policy aligns with global norms like GDPR. For example, it incorporates concepts of data principal rights, data fiduciary responsibilities, and lawful processing bases which mirror GDPR’s ethos. In fact, the policy was crafted when India’s Personal Data Protection Bill was still under consideration, and it anticipated those requirements (since the PDP Bill 2019 did categorize health as sensitive data requiring explicit consent, the ABDM policy enforced explicit consent). - Data Retention and Ownership: The policy clarifies that citizens have ownership of their health data. It also likely outlines retention guidelines (e.g., health records should not be kept indefinitely without reason, and must be deleted or de-identified after a period unless needed for care or legal reasons – though specifics would depend on allied regulations and clinical record-keeping norms).

The implementation status of ABDM: As of early 2025, ABDM has been rolling out. As per Business India (March 2025), over 500 million health records were linked to ABDM and 80,000+ healthcare facilities were participating. The scale is large, which underscores the importance of its data governance mechanisms. The same article notes that ABDM's success depends on wide adoption and contributions from private sector and NGOs, which in turn requires trust that data is secure. Thus, ABDM's privacy and security provisions are not just ethical niceties but fundamental to user uptake.

DISHA – A potential dedicated health data law: Alongside ABDM, there has been discussion of the Digital Information Security in Healthcare Act (DISHA). This was a draft bill (circa 2018) intended to create a legal framework for health data protection. DISHA would have established a National Electronic Health Authority (NeHA) and similar state authorities to regulate health data exchanges, require patient consent for any sharing, and impose penalties for violations. It was called out as an Indian analogue of HIPAA. However, DISHA did not progress to enactment, possibly because the government waited for an omnibus data law first (the PDP Bill, now DPDP Act) and decided that one broad law might suffice. The Business India piece suggests DISHA is still "expected" and would reinforce patient consent requirements, but with DPDP Act in place, it's unclear if DISHA will be revived or if health-specific rules will be issued under the DPDP Act's framework instead.

Other Guidelines: The Ministry of Health and Family Welfare (MoHFW) also introduced Electronic Health Record (EHR) Standards in 2016 (updated 2017). These are technical standards for interoperability and record structure, indirectly related to data governance because standardization helps in better control and audit of data. There are also telemedicine practice guidelines (2020) which touch on maintaining patient data confidentiality in remote consultations.

1.2.4.3 Information Technology Act, 2000 and IT Rules (Legacy Framework)

Prior to the DPDP Act, India's only privacy-related statute applicable to health data was the Information Technology Act 2000, particularly: - Section 43A of IT Act (added in 2008 amendment): This section made companies (or any legal body) handling sensitive personal data liable to compensate individuals if they were negligent in implementing "reasonable security practices" and such negligence caused wrongful loss or gain. It was effectively India's early data protection rule, albeit narrow. To operationalize Section 43A, the government notified the IT (Reasonable Security Practices and Sensitive

Personal Data or Information) Rules, 2011. These rules defined “Sensitive Personal Data or Information (SPDI)” which included health information (medical records and history) and biometric data. The rules mandated that organizations must publish privacy policies, collect consent for disclosure of SPDI, use it only for purpose, and implement security measures (with a safe-harbor if they followed an approved standard like ISO 27001). They also gave individuals the right to correction and withdrawal of consent (subject to conditions), quite ahead of their time for Indian law. However, enforcement of Section 43A was minimal; only a handful of cases ever cited it. Still, it set the precedent that health data is sensitive and needs protection. Now that DPDP Act is here, Section 43A is effectively overridden for personal data matters.

- Section 72A of IT Act: This criminalizes disclosure of personal information by someone who has obtained it under a contract (like an employee or service provider) without consent, intending or knowing it will cause harm. A doctor or clinic employee improperly sharing patient data could theoretically be prosecuted under this, though again cases have been rare.

- CERT-In Rules 2022: Under the IT Act, CERT-In (India’s Computer Emergency Response Team) has authority to mandate breach/incident reporting. In 2022, CERT-In issued directions requiring all organizations (across sectors) to report certain cyber incidents within 6 hours of noticing. Healthcare entities are included in its scope. So, if a hospital faces a ransomware attack, it should inform CERT-In quickly. This runs parallel to any obligations under DPDP Act or sectoral expectations, and helps the government coordinate responses to cyber threats.

Despite these provisions, the ground reality has been that many health establishments in India have had low awareness or compliance with these IT rules. The healthcare industry wasn’t a primary focus of IT Act enforcement. As a result, data governance maturity in many Indian hospitals is low – privacy policies may not be robust, cybersecurity investments have been insufficient, and data sharing practices often rely on convenience (e.g., doctors using WhatsApp to discuss a case with a specialist, or patients emailing records) rather than secure platforms. These practices, while well-intended for patient care efficiency, pose challenges for data protection because consumer apps may not meet healthcare-grade security, and it blurs lines of responsibility under the law.

1.2.4.4 Other Initiatives and Standards

To complete the picture, it's worth noting: - The National Health Authority (NHA), which implements ABDM, has also set up a data policy for the government's flagship insurance scheme PM-JAY. They have experience handling big health data and ensuring privacy (e.g., anonymized claims data for fraud analytics).

- Data Security Council of India (DSCI), an industry body, released a privacy best practice guide for healthcare in 2020. It offers a checklist (7 points as listed: accurate data collection, patient consent, secure storage, etc.) for healthcare providers to align with privacy principles. Although not law, it's a resource that forward-looking organizations might adopt to prepare for eventual stricter regulations.

- National Digital Health Blueprint (2019): This policy document laid out the design for NDHM/ABDM including the creation of a unified health interface, registries for professionals and facilities, and the guiding principle of privacy/security. It provides the conceptual rationale behind ABDM's structure.

- Standards for EHR Interoperability: MoHFW's EHR standards (based on international standards like HL7 FHIR) are relevant because good data governance also implies data quality and consistency, which these standards promote.

Summary of India's Ecosystem: As of 2025, India has:

- A brand new, general data protection law (DPDP Act) that applies to health data but doesn't specially tailor for it. - A national mission (ABDM) with its own policy filling some gaps by requiring consent and tech safeguards in that ecosystem.

- Legacy IT Act provisions which set the stage but will likely be subsumed by the DPDP Act once fully operational. - Professional ethics and guidelines that impose confidentiality duties on healthcare providers (e.g., the National Medical Commission's code mentions patient confidentiality).

- Early efforts at standard setting and best practices through government and industry (EHR standards, DSCI guidelines).

- However, no single dedicated regulator or regulation purely for health data (like a "health data authority" as envisioned in DISHA).

The effectiveness of this framework is still to be tested. The DPDP Act rules are being formulated, ABDM is being scaled, and stakeholders are adjusting to new compliance requirements. The next section (7.3) will identify themes from literature – particularly

where scholars, policymakers, or industry observers have identified gaps or challenges in India's approach, which will segue into the comparative analysis in the Results and Discussion chapters.

1.2.5 Key Themes from Literature: Gaps and Challenges

Analysing the literature across global and Indian sources reveals several recurring themes and points of comparison:

1. Regulatory Scope and Coverage: One striking difference is sector-specific vs general legislation. Global practice shows that having health-specific regulations (HIPAA, or even GDPR's special provisions for health) helps address the unique needs of healthcare. India currently lacks a specific health data law; instead it has a general law (DPDP Act) that leaves nuance to be figured out by the health industry. Literature suggests this could be problematic; for example, McDonald (2023) argues that absence of a clear categorization for health data and the possibility of government exemptions in DPDP Act could leave public healthcare institutions less accountable. The comparative insight is that India might need either supplementary rules or very clear guidelines to ensure health data gets due protection despite not being tagged as sensitive by law.
2. Consent and Data Sharing in Care: In healthcare, an overly rigid consent requirement can impede routine care coordination (doctors consulting each other, referrals, etc.), while too lax a regime risks privacy. HIPAA navigates this by allowing data sharing for treatment without separate patient authorization. GDPR allows processing of health data by hospitals under the "medical purposes" exception and legitimate interest with safeguards. Indian law's stance is less explicit, creating a grey area for day-to-day practices like doctors using messaging apps to share reports for a second opinion. Sood et al. (2025) highlight this dilemma – frontline medical professionals fear that the new law could penalize even well-intentioned data sharing unless it's clearly exempted. The recommendation emerging is for India to carve out clear allowances for health data use in direct patient care and research, possibly by amending the DPDP Act or through sectoral guidelines (e.g., exempt health practitioners from certain consent requirements when data is used for patient benefit, as long as confidentiality is maintained).
3. Data Security and Breach Response: There is a consensus that Indian healthcare institutions need to significantly improve cybersecurity measures. Global

frameworks not only mandate security (HIPAA Security Rule, GDPR Article 32) but also have strict breach reporting and response norms. India has patchy breach notification rules. The DPDP Act leaves it to the DPB to order notifications in some cases, and CERT- In rules impose fast reporting to the government but not necessarily to affected persons. The literature (e.g., Sood et al. 2025 Recommendation 2) suggests mandatory reporting of health data breaches to both authorities (like CERT-In) and the individuals affected. This would align with global practice and ensure transparency. Without mandatory disclosure, there is a risk that breaches are swept under the rug, denying patients the chance to protect themselves (like changing passwords or monitoring misuse if their data leaked). The AIIMS incident exemplified how damaging a breach can be and how little recourse patients had in absence of a data law at that time.

4. Enforcement and Liability: Under DPDP Act, only the data fiduciary (the entity deciding purpose) is held liable for violations; data processors (e.g., a cloud vendor or an IT company managing hospital records) are not directly penalized by the Act, except possibly through contractual flow-down. GDPR, on the other hand, can hold processors directly responsible and fine them if they infringe their obligations . This difference might mean weaker incentives for some third-party service providers in India to maintain best practices, unless contracts or future rules address it. The literature (as in Sood et al.) recommends that liability should be shared, especially in complex cases like AI in healthcare where both a hospital (data fiduciary) and an AI vendor (processor) are handling sensitive data. Without joint accountability, processors might not invest enough in security, potentially leaving a blind spot. Additionally, enforcement capacity is an issue. The DPB is new and will have to handle all sectors. Contrast that with HHS OCR which focuses on health or DPAs in EU that often have health-specialist staff. India might consider empowering sectoral bodies (like perhaps NHA) to assist with enforcement or compliance in health.
5. Infrastructure and Organizational Culture: Many sources point out that laws alone don't secure data; hospitals need resources and training. The NLIU blog on AIIMS cyber-attack revealed basic failings: outdated software, unpatched systems, lack of employee training, no regular audits . This is an infrastructural and cultural gap. By comparison, NHS's mandatory training (DSP Toolkit Standard 3) and yearly audits push a culture of security. Indian healthcare would benefit from similar regular audits (perhaps NABH accreditation standards could

include IT security criteria, or ABDM participation could require annual compliance checklists). Sood et al. (2025) Recommendation 5 and 6 also emphasize awareness training for medical staff and budgetary commitment to cybersecurity (e.g., yearly vulnerability assessments, hiring security teams). These recommendations align with global best practice (GDPR requires regular testing of security measures). The challenge is ensuring Indian healthcare providers, especially smaller clinics or government hospitals with tight budgets, can implement these. It might need government funding or public-private partnerships to improve health IT security infrastructure nationwide.

6. Patient Rights and Empowerment: Under global standards, patients often have robust rights (like accessing their records, knowing who accessed their data, etc.). In India, patient awareness of privacy rights is low. The DPDP Act's rights (access, correction) need to be operationalized in healthcare – e.g., hospitals might need a portal for patients to view and request corrections to their records. ABDM partially addresses this by giving patients a health locker to store and see their records and consents. The literature encourages empowering patients because an informed patient can act as a watchdog for their data. For instance, if a patient sees unauthorized access to their ABDM records (assuming audit trails are visible), they could raise a complaint.
7. Harmonization and Policy Coherence: One gap identified in older commentary was conflict between proposed laws. For example, as Express Healthcare noted, the 2019 PDP Bill allowed processing health data with consent, whereas DISHA would have outright banned commercial use of health data. Divergent rules can confuse healthcare providers. Going forward, it will be important that any new health-specific guidelines under DPDP Act, or any revival of DISHA, complements rather than contradicts the DPDP Act. Ideally, one clear framework should emerge.

In conclusion, the literature points to a transitional phase: India has the intent and now some tools (law, ABDM policy), but execution will be key. Global frameworks offer valuable lessons – such as the need for explicit health data rules, the importance of enforcement heft, and continuous improvement cycles like NHS has. These themes set the stage for the Results chapter, where the findings of this comparative analysis are presented systematically, and the Discussion which will delve deeper into how India can address the identified gaps.

CHAPTER 2 METHODOLOGY

2.1 Introduction

As India digitizes its healthcare sector, ensuring the privacy and security of personal health data has become a pressing concern. While global frameworks (e.g., HIPAA, GDPR) provide models for safeguarding health information, India's regulations are relatively nascent. There is uncertainty about whether India's existing laws and policies adequately address the unique challenges of digital health data, and how they compare with international standards. The problem is compounded by incidents of data breaches and cyber-attacks on healthcare institutions, indicating potential weaknesses in both policy and practice.

2.2 Data Sources and Search Strategy

Sources of Information: The sources reviewed can be categorized as follows: - Legal and Policy Documents: e.g., the text of HIPAA and the HITECH Act (via official HHS summaries), GDPR (via EU GDPR portal and secondary summaries), NHS DSP Toolkit guidelines (from NHS Digital resources), the full text of India's DPDP Act 2023, and policy documents from ABDM (like the Health Data Management Policy). - Academic Journals and Conference Proceedings: Peer-reviewed articles analyzing data protection in healthcare, both globally and in India. Examples include journal papers in Health Policy, Journal of Medical Ethics, and Health Informatics dealing with privacy and digital health. Notably, the study referenced an open- access article by Sood et al. (2025) in Nature portfolio (which was available via PubMed Central) for specific insights on DPDP Act challenges, and another by Ahmed et al. (2025) in PLOS ONE regarding data governance frameworks.

- Government and Institutional Reports: For instance, WHO and UN reports on global digital health strategies, and any whitepapers by Indian committees (like the 2018 Srikrishna Committee report on data protection which influenced early drafts).

- Industry Publications and News Articles: These include analysis by law firms, think tanks (like the Center for Internet and Society, or NASSCOM-DSCI reports), healthcare IT news (e.g., Express Healthcare articles), and credible tech media (like Medianama, which often covers data policy). They provide context on implementation and ground reality, such as details of cyber incidents and opinions from stakeholders.

- Blogs and Opinion Pieces by Experts: For current developments (like the DPDP Act's impact on health), blogs by legal experts (for example, the CCG NLU Delhi blog on health data and DPDP) and LinkedIn articles by practitioners were considered. While not peer-reviewed, these often contain up-to-date commentary and are cited accordingly for their informative value.

Search Strategy: Searches were conducted using academic databases (PubMed, Scopus for relevant keywords like "health data privacy India", "HIPAA vs GDPR health"), legal databases (for statutes and regulations text), and general search engines for grey literature. Keywords and phrases used included:

- "Data governance healthcare comparative"

- "India health data DPDP Act vs GDPR"

- "HIPAA HITECH summary healthcare data"

- "NHS Data Security Toolkit requirements"

- "India digital health cybersecurity challenges"

- "Ayushman Bharat Digital Mission privacy policy"

- "Health data breach India hospitals"

- "GDPR health data research exemptions" etc.

Additionally, backward and forward reference tracing was used on key articles – meaning, looking at the references of a useful paper to find earlier foundational works, and searching which later works cited it to find more recent discussions.

All sources used were in English, which was not a limitation here since the laws and policies of interest (US, EU, UK, India) are available in English. The search spanned literature from roughly 2010 (when HITECH and global e-health discussions ramped up) to 2025, with a focus on the last 5 years given the recency of GDPR and the DPDP Act. This ensured capturing the latest developments and commentaries.

Inclusion Criteria: Sources were included if they offered substantive information about:

- The content of relevant regulations or frameworks.

- Analysis or critique of those regulations in practice.

- Comparative perspectives (either comparing across countries or analyzing India's readiness).

- Case studies demonstrating regulatory impact (like a data breach incident analysis).

Peer-reviewed sources were prioritized for credibility, but due to the very recent nature of Indian developments (DPDP Act 2023), some high-quality blog analyses and news reports were included for the most up-to-date insights.

Exclusion Criteria: Sources were excluded or given less weight if:

- They were very outdated (pre-2010 discussions of privacy might not account for GDPR or current tech).

- They did not specifically address healthcare (general data protection articles that didn't touch on health context were less relevant).

- They lacked authoritative backing or evidence (random opinions not backed by data or not from subject matter experts were avoided).

- Non-English sources (if any relevant existed) due to language barrier.

2.3 Research Design – Comparative Literature Review

This study employs a comparative literature review as its research design. Given the nature of the research question – which asks to compare frameworks and identify gaps – a literature-based analysis is appropriate and feasible, especially since no primary empirical data (surveys, interviews, etc.) were required or collected. The goal was to synthesize existing knowledge from laws, policy documents, academic analyses, and expert commentaries to draw conclusions about India's position relative to global standards.

The design is qualitative and descriptive-analytical. Instead of quantitative metrics, it focuses on qualitative aspects of policies (such as presence or absence of certain provisions, strength of enforcement, etc.) and narrative evidence (such as case studies of breaches, expert opinions on challenges). This approach aligns with a traditional thesis in the domain of health policy, where understanding regulatory text and context is crucial.

The comparative element involved examining multiple units (global frameworks vs. Indian frameworks) across common dimensions (e.g., consent requirements, data subject rights, security measures, enforcement mechanisms). By structuring the review

to cover each framework and then thematically analyzing differences, the study maintains clarity in comparison.

2.4 Research Question

To assess the gaps and challenges of India's data governance and cybersecurity policies in digital healthcare when compared with global standards.

This overarching question can be broken down into sub-questions:

- How do leading international frameworks (such as HIPAA/HITECH, GDPR, NHS Data Security Toolkit) approach data governance and cybersecurity in healthcare?

- What are the key components of India's current regulatory ecosystem for digital health data (e.g., DPDP Act, ABDM, IT Act)?

- In what areas does India's approach align with or diverge from global best practices?

- What gaps (legal, technical, or operational) exist in India's framework, and what challenges might impede effective data governance and cybersecurity in the health sector?

- What strategies or policy measures could bridge these gaps to strengthen India's digital healthcare data governance?

2.5 Objectives of the Study

- To understand the global frameworks related to data governance and cybersecurity in healthcare
- To study current digital health regulations, including the DPDP Act and ABDM in context of India.
- To understand the comparative approaches identifying the gaps and challenges in context of India and global

2.6 Analytical Framework for Comparison

To systematically compare the frameworks, a set of criteria or themes was established (in alignment with the research objectives and literature themes identified):

- Legal Nature: (Sector-specific law vs general law; mandatory or voluntary standards).

- Definitions and Scope: (How is health data defined? Who is regulated – e.g., covered entities, data fiduciaries, processors, etc.).

- Consent and Lawful Bases: (Requirements for obtaining consent for health data, exceptions for medical use, emergency provisions).

- Individual Rights: (What rights do patients/data subjects have regarding their data – access, correction, deletion, data portability, etc.).

- Data Security Requirements: (Are there specific security measures mandated? e.g., encryption, access control, audit logs).

- Breach Notification: (Obligations to report breaches to authorities and individuals, timeline, threshold).

- Enforcement Mechanisms: (Regulatory bodies, penalties/fines, liability distribution, compliance audits).

- Guidance and Compliance Support: (Are there tools or standards provided to help compliance, like NHS toolkit or guidelines in India).

- Challenges noted in Implementation: (From literature: e.g., cost of compliance, lack of awareness, complexity in given jurisdiction).

- Outcomes/Evidence: (Any evidence of effectiveness or failure – e.g., number of fines issued, known compliance rates, breach stats).

Each framework (HIPAA/HITECH, GDPR, NHS Toolkit, DPDP Act/India) was analyzed against these criteria. A table (as referenced in List of Tables) was drafted during note-taking to juxtapose key points (for instance, HIPAA vs GDPR on breach notification vs DPDP Act's stance, etc.), which later informed the narrative in Results.

Using this analytical framework ensured that the comparison wasn't arbitrary but focused on relevant aspects of data governance and cybersecurity.

2.7 Significance of the Study

This study is significant for several reasons:

• Policy Relevance: It comes at a time when India is implementing the new DPDP Act and scaling up the ABDM. Policymakers can benefit from a consolidated analysis that benchmarks India's efforts against tried-and-tested global models. Identifying gaps early could inform amendments, subordinate legislation (rules, standards), or targeted guidelines for the health sector. For example, understanding GDPR's handling of health

data or HIPAA's enforcement experience can guide the Data Protection Board of India and the National Health Authority in refining regulations or compliance requirements.

• Healthcare Institutional Perspective: Hospitals, clinics, and digital health startups in India are directly affected by these regulations. A clear understanding of global best practices versus Indian requirements can help these stakeholders in compliance planning and in advocating for necessary support. For instance, if global frameworks require certain cybersecurity measures (encryption, access controls, breach notification protocols), Indian healthcare providers can proactively adopt similar measures, anticipating that Indian regulations may move in that direction. The research can also highlight the need for capacity building–e.g, training healthcare staff in data security as mandated in NHS toolkit standard 3.

• Academic Contribution: This dissertation adds to the growing body of knowledge on health informatics and governance. It compiles scattered information on laws and practices into a comparative format, which can be a reference for future research. By focusing on India's scenario in comparison to global frameworks, it fills a gap in the literature – most existing studies examine either global laws in isolation or India's law in isolation, but few juxtapose them comprehensively in the context of healthcare.

•Protecting Patient Interests: At the heart of this issue are patients whose personal health data must be protected to maintain trust in digital health services. By identifying weaknesses in data protection, this study indirectly serves patient interests. If its recommendations are heeded (for example, strengthening breach reporting or improving consent practices in India), the outcome would be a safer environment for patient data and, consequently, greater public confidence in digital health innovations.

In summary, the study's comparative approach not only sheds light on where India stands today, but also provides a roadmap for how India's digital healthcare data governance can evolve. Ensuring strong data governance and cybersecurity is foundational for the success of digital health initiatives – without it, technological advances may falter due to privacy breaches or cyber threats. Therefore, this study is both timely and essential for aligning India's health data policies with global standards while addressing local challenges.

2.8 Limitations of the Study

While the methodology is thorough in reviewing literature, certain limitations must be acknowledged:

- Evolving Nature of Regulations: The DPDP Act 2023 is very new and still in the early stages of implementation (rules and guidelines are forthcoming). Therefore, literature on its impact, especially specific to healthcare, is limited and mostly speculative or anticipatory. The study had to rely on analysis of the law's text and initial expert opinions. Actual on-ground outcomes might differ as the law is operationalized. - Scope of Global Frameworks: The study selected key frameworks (US, EU, UK) as representative global standards. However, there are other notable frameworks (e.g., Canada's Personal Health Information Protection Act in Ontario, Australia's My Health Record system with its own legislation, etc.) which were not covered due to scope. The chosen ones were deemed most influential for comparison.

- Lack of Primary Data: The research does not include interviews with hospital administrators or surveys of compliance in Indian hospitals, which could have provided empirical backing to some identified challenges (like how many hospitals have cybersecurity budgets, or awareness of DPDP Act among healthcare providers). It relies on reported information and case studies instead. As a result, some assertions (e.g., "many Indian hospitals lack regular security audits") are drawn from secondary reports and may not reflect a quantified measure. - Potential Bias in Sources: There is a mix of source types. While peer- reviewed articles provide rigor, blogs or news pieces may have author bias or incomplete information. The study mitigated this by cross-verifying facts across multiple sources (for example, using multiple sources to confirm details of the AIIMS breach and response). - Interpretation and Generalization: Laws like GDPR or HIPAA are complex; this study focused on key points relevant to the research question. There is a risk of oversimplification. Also, the situation in India is heterogeneous – top corporate hospitals vs small clinics might have very different states of data governance. The study's broad strokes might not capture every nuance. - Vancouver Citation and Source Constraints: The dissertation guidelines emphasized using Vancouver style and preserving citations in a specific format. Ensuring that all statements are well- supported by citations from the available sources sometimes constrained how information could be presented (had to find a citable source for each significant point).

Despite these limitations, the methodology's triangulation of legal text, expert commentary, and real incident analysis provides a robust foundation to address the research question. The comparative framework, though qualitative, allows reasoned identification of gaps. Future research could build on this by incorporating interviews or compliance data as the DPDP Act matures.

2.9 Ethical Considerations

Since this study did not involve human subjects or sensitive personal data collection, there were no direct ethical approvals required from an institutional review board. However, the topic itself deals with privacy and personal data, so the research was conducted with an ethos of respect for confidentiality. When discussing case studies (like the AIIMS breach), information was limited to what is publicly reported; no personal patient data was accessed or disclosed by the researcher.

All sources are properly cited to credit original authors. Care was taken to present laws and policies accurately to avoid any misrepresentation that could mislead on compliance matters. With the methodology outlined, the dissertation now proceeds to the Results chapter, where the comparative findings are presented succinctly, followed by the Discussion interpreting those findings and making recommendations.

CHAPTER 3 RESULTS

This chapter presents the key findings of the comparative analysis, organized according to the study objectives and major thematic areas. It is essentially the outcome of the literature synthesis, highlighting how global frameworks operate, how India's framework operates, and where the significant differences or gaps lie.

For clarity, the results are segmented into three sections corresponding to the objectives:

3.1 Overview of Global Best Practices in Healthcare Data Governance

Legal Foundation & Scope: Global best practices show that comprehensive legal frameworks underpin data governance in healthcare. In the US, HIPAA (with HITECH amendments) specifically targets health data held by healthcare providers, insurers, and their partners. It has stood the test of time and adaptation, illustrating the importance of a sector-specific law for health data. In the EU, GDPR provides a universal data

protection law with particular clauses for health data, showing that general privacy laws can work if they include sector-sensitive provisions (like requiring higher justification for health data use). The UK's DSP Toolkit is an example of translating high-level law into concrete practice for a sector via mandated self- assessment.

A cross-comparison reveals:

- All these frameworks clearly define health data and recognize its sensitivity (HIPAA calls it PHI and tightly controls it; GDPR calls it special category data and restricts processing; the NHS standards treat patient data as "confidential" by default).

- All have broad scope in coverage of entities: HIPAA covers all major health entities and, after HITECH, their contractors. GDPR can cover any entity (public or private, big or small) processing health data of EU residents. The NHS toolkit applies to any org interfacing with NHS data, including private subcontractors. This universality ensures no major care scenario falls through regulatory cracks.

Consent and Data Use Norms: In global frameworks, patient consent is a cornerstone but with pragmatic exceptions:

- Under HIPAA, patient authorization is not required for sharing PHI among providers for treatment, enabling integrated care, but any non-routine use (like marketing) needs consent. This strikes a balance between privacy and practical healthcare needs.

- GDPR typically needs explicit consent for health data, but healthcare providers often rely on the "medical diagnosis and treatment" legal basis (Art 9(2)(h)) or "vital interests" in emergencies, thus not impeding medical care. Consent is more crucial for secondary uses (research, etc.), where GDPR often requires either consent or a specific legal provision and ethics safeguards.

- The NHS toolkit indirectly ensures consent practice by referencing Caldicott Principles (one of which is that the duty to share information can be as important as the duty to protect confidentiality for patient benefit – implying that when sharing is in patient's interest, it's permitted, but patient's expectations must be considered).

Security Measures and Certifications: One of the strongest points of global frameworks is the emphasis on concrete security controls:

- The HIPAA Security Rule effectively established an industry baseline for healthcare IT security in the US. Many hospitals implement frameworks (like NIST's cybersecurity framework) to comply. Regular risk assessments are required.

- GDPR's requirement is outcomes-based (ensure appropriate security), which in practice has led to widespread adoption of standards like ISO 27001 in health organizations and use of techniques like pseudonymization for health research data . Many EU hospitals conduct Data Protection Impact Assessments (DPIAs) for new tech deployments involving patient data , which is a proactive risk mitigation step.

- The NHS's approach, with its 10 standards (including annual penetration tests, rapid response to incidents, no outdated software) , represents a best practice checklist. Compliance rates have improved year-on-year as organizations close gaps identified in prior toolkit submissions, indicating a cycle of continuous improvement.

Breach Handling: Global frameworks enforce transparency in breach handling: - HIPAA/HITECH: If >500 individuals are affected by a breach, not only are patients notified, but HHS and sometimes media are informed, effectively naming-and-shaming organizations (HHS's "Wall of Shame" website lists breaches). This has incentivized better cybersecurity. - GDPR: The 72-hour rule for reporting to authorities is strict; failure to notify can itself incur fines. Many EU healthcare breaches have led to regulatory investigations and fines when organizations were found lacking adequate protection. Patients have been informed in multiple incidents (e.g., hospital system hacks) due to GDPR's mandates. - NHS Toolkit Standard 6: It requires that action is taken immediately after a breach and reported to management in 12 hours . Additionally, separate UK laws (Data Protection Act 2018) and NHS policies require notifying the ICO (UK's DPA) and affected individuals if a breach has risk. The synergy of internal NHS rules and GDPR means UK patients generally get informed of serious breaches.

Enforcement and Accountability: A summary of global enforcement:

- HIPAA: Enforcement actions (penalties) have ranged from a few thousand dollars for small clinics to multi-million-dollar settlements for large breaches or egregious violations. The presence of audits (OCR's periodic audits of healthcare entities) keeps pressure on compliance.

- GDPR: We see consistent enforcement. For example, in 2020, a hospital in Portugal was fined €400,000 for improper staff access controls (too many people had access to patient records, violating need-to-know) – a direct enforcement of the principle mirrored in NHS standard 4. Such cases send a message and lead others to tighten access governance.

- The NHS toolkit itself is not an enforcement mechanism per se, but it's tied to contracts; an organization must comply or risk losing the ability to do business with NHS. This indirect enforcement is powerful in a publicly funded health system.

These best practices demonstrate that robust data governance in healthcare is multi-faceted: clear rules, emphasis on consent but not to the detriment of care, strong security requirements, breach accountability, and active enforcement. They also demonstrate ongoing evolution (HIPAA is being updated even now for better patient access via apps, GDPR developments like the proposed European Health Data Space build on GDPR to facilitate health data sharing with privacy, etc.).

3.2 Current State of Data Governance and Cybersecurity in Indian Healthcare

3.2.1 Legal and Policy Status (as of 2025): India's scenario can be described as "in transition": - The DPDP Act 2023 has been passed but is in early implementation stages (rules are expected to specify more details, Data Protection Board is being set up). So, many healthcare organizations are still trying to understand what changes are needed. Awareness is growing among large hospitals and health-tech companies, especially those that previously prepared for the older draft bills. However, medium and small providers may not yet be fully cognizant of the law's requirements.

- IT Act/Rules Legacy: Up until 2023, compliance with IT Act's privacy rules was inconsistent. Larger hospital chains had IT security policies and followed some ISO standards. But many others, especially in the public sector, were not fully following the 2011 Rules (for instance, explicit consent in writing for sharing medical data was rarely practiced; often implicit consent was assumed when patients registered).

- ABDM participation: Thousands of government and private facilities have joined ABDM, issuing digital health IDs and sharing e-prescriptions, etc. As part of onboarding, they are supposed to adhere to the ABDM Health Data Management Policy. In practice, the National Health Authority has obtained commitment letters from participants to abide by privacy principles. ABDM also introduced consent managers

(like NDHM's own app, and some private PHR apps) that operationalize consent. So, in ABDM-linked services, one could say a baseline data governance framework exists (e.g., a doctor must request the patient's consent via the system to pull their past records).

- Areas outside ABDM: A lot of health data processing still happens outside the ABDM network (e.g., hospitals maintaining their own patient databases, diagnostic companies with online reports, telehealth apps). In these areas, practices vary. Some health-tech apps have detailed privacy policies and allow users to download or delete data, aligning with global norms. Others may be less transparent. The DPDP Act will push all these to standardize privacy notices and consent flows.

3.2.2 Challenges Observed:

- Gaps in Law for Health Context: As noted, no differentiation of health vs regular data by law. This means, for example, there's no legal mandate for hospitals to perform Privacy Impact Assessments for a new health IT system, whereas GDPR would require a DPIA for large-scale health data processing. Unless future rules say so, this might be overlooked.

- Data Sharing for Care vs Privacy Dilemma: Indian doctors commonly share patient data for referrals or expert opinion using convenient channels (WhatsApp, etc.). Under a strict reading of DPDP Act, this might be seen as processing without explicit consent (outside an emergency), and thus a violation. There is real worry in the medical fraternity about being penalized for such practice, which they view as in patient interest. The results show ambiguity here is a challenge. In absence of official clarification, many providers are unsure if they need to obtain written consent every time they forward a lab report to a colleague. This could lead to one of two scenarios: either they ignore the law (and risk penalties), or they become over-cautious (which could impede collaborative care). Both outcomes are undesirable.

- Cybersecurity Posture: Evidence suggests many Indian healthcare entities are under-prepared for cyber threats:

- The AIIMS Delhi breach (Nov 2022) revealed systemic issues: outdated systems, poor network segmentation, weak incident response. It took ~15 days to fully restore systems. If India had GDPR-like fines, an incident compromising millions of records would have triggered enormous fines; however, currently, there's no report of any

penalty on AIIMS under IT Act (since DPDP Act wasn't in force and AIIMS is a government entity likely to be exempt from older rules).

- A report by CloudSEK (a cybersecurity firm) in 2022 indicated that India's healthcare sector faced the second highest number of cyber attacks globally (after the US). It also noted a 95% increase in attacks compared to the previous year. This indicates a trend – as healthcare goes digital, attackers are targeting it, but the defenses haven't ramped up proportionately.

- Many hospitals do not have a dedicated Chief Information Security Officer (CISO) or Data Protection Officer yet. Only some large chains do. The concept of regular VAPT (vulnerability assessment and penetration testing) is not yet routine in health sector except perhaps in those accredited by JCI or catering to medical tourism (where international patients ask about data security).

- Enforcement and Culture: Historically, enforcement of data protection in India has been weak. There were hardly any fines under Section 43A on hospitals or others for data leaks. Thus, a culture of proactive compliance did not develop. This is gradually shifting – for instance, after the AIIMS incident, the government directed all major hospitals to audit their IT security. The Ministry of Health also reportedly planned to declare health as "critical information infrastructure" which would bring NCIIPC (National Critical Information Infra Protection Centre) into play for healthcare (though unclear if that designation is formal yet).

3.2.3 Strengths/Opportunities:

It's not all grim; there are some positive aspects in the current state:

- ABDM's consent framework is quite modern and if fully adopted, gives patients granular control – something even many Western systems struggle with implementing.

- The DPDP Act's penalty provisions, once active, put big financial and reputational stakes on the line, which should prompt healthcare management to take notice and invest in compliance.

- India's IT talent pool means that solutions like anonymization, blockchain for health records (as research suggests), etc., can be implemented domestically. There are startups working on privacy-preserving data sharing for health research, indicating an ecosystem readiness if properly incentivized.

- Public awareness post high-profile breaches is increasing. Patients are starting to ask questions about how their data is used (especially more educated urban populations). This can drive healthcare providers to pay attention to privacy as part of customer service.

In sum, the current state is one of partial readiness: frameworks exist on paper (laws, policies) but translation into practice is uneven. Key gap areas identified include explicit guidelines for health data sharing, robust cybersecurity measures across the board, and setting up enforcement mechanisms that keep health sector nuances in mind. These results set the foundation for the comparative gaps analysis in the next section.

3.3 Comparative Analysis: Gaps and Challenges Identified

Bringing the above findings together, this section explicitly compares and identifies gaps – i.e., where India's approach diverges from global standards in ways that could be problematic, and challenges – i.e., practical issues that could hinder implementation of good data governance in India's digital health space.

Gap 1: Absence of Health-specific Data Protection Provisions in Law – Unlike GDPR (special category data) and HIPAA (dedicated law), India's DPDP Act does not single out health data for special treatment. This is a legal gap. The consequence is that heightened safeguards like requiring explicit consent for health data, mandatory risk assessments for health projects, or stricter penalties for misuse of health data are not codified. The global perspective suggests health data needs extra care due to its sensitivity. The gap can be filled by either amending the law to introduce a health data category or by sectoral rules under the Act (the Act allows central government to make additional provisions for certain sectors – this could be used).

Gap 2: Inadequate Clarity on Permissible Health Data Sharing for Care – Global frameworks clearly allow sharing for treatment (HIPAA's TPO exception, GDPR's Art 9(2)(h) for healthcare purposes). India's law doesn't explicitly mention "treatment" as a basis (aside from emergency/public health threats)

. This gap could lead to hesitation or inconsistent practices. An Indian hospital might wonder: can we send patient data to a specialist via email without violating DPDP Act? The law doesn't say "yes" or "no" clearly. As a result, each entity might interpret differently, possibly until jurisprudence or regulations clarify. This gap needs to be

addressed by official guidance or amendments – perhaps an exemption or deemed consent category for standard healthcare operations, as recommended by experts (Sood et al. recommended that "DPDPA should consider extenuating circumstances related to patient care and provide exemptions to health care workers").

Gap 3: Breach Notification to Individuals – Currently, Indian law or policy does not mandate that patients be informed if their health data is breached (unless one interprets that DPB may order it or if some consumer court takes it up). This is behind global practice where patient notification is standard. The absence of a clear breach notification rule means patients may remain in the dark about breaches affecting them, as was the case historically. This gap undercuts patient autonomy and the ability to mitigate harm (e.g., they can't watch for identity theft if they never knew their data leaked). It's a gap to fill in either DPDP rules or by sectoral guidelines (e.g., NHA could mandate that if a participant of ABDM has a breach, they must inform affected individuals and NHA within X time).

Gap 4: Shared Liability for Data Processors – DPDP Act's stance of holding only data fiduciaries liable contrasts with GDPR where processors also carry responsibility. In modern healthcare, third-party IT providers play huge roles (cloud hosts, SaaS EHR systems, AI analytics firms). If they have no direct obligation under law, the deterrence is weaker. The gap is that India lacks direct oversight over such actors beyond contract. This might be resolved if "significant data fiduciaries" rules force audits that include processors, or if future amendments bring processors under some direct purview. Or possibly sector- specific licensing – e.g., if an IT company wants to offer software for health data processing, it must get certified or approved for security compliance (something akin to how RBI regulates banking software providers). But currently, this gap exists.

Gap 5: Operational Infrastructure for Compliance – One practical challenge (though not a "gap" in law, it's a gap in capacity) is that Indian healthcare institutions lack the compliance infrastructure that many Western counterparts have developed. For example, GDPR requires a Data Protection Officer (DPO) for big data handlers – many EU hospitals have one. In India, even though DPDP Act might designate some as "significant" requiring a DPO, this concept is new. There's a shortage of professionals trained in both healthcare and data privacy. Similarly, processes like annual security audits are not institutionalized in health sector. This challenge means even if rules exist, implementation will lag until capacity is built. It's a gap that calls for training programs,

perhaps government-led capacity building (Recommendation 5 from Sood et al. was to hold multiple workshops to sensitize the medical fraternity, which is exactly to address this).

Gap 6: Public Sector vs Private Sector Disparity – Global regulations apply across both, but enforcement sometimes differs. In India, a potential challenge is that government hospitals or programs (which serve a huge portion of the population) might be exempted from certain DPDP Act provisions using the government's exemption powers. This would create a two-tier system: private hospitals strictly regulated, public ones not as much. That gap would be harmful to citizens (since many sensitive records are with government facilities like AIIMS, large state hospitals). Ethically and logically, government should hold itself to equal if not higher standards. Bridging this gap means resisting over-broad exemptions and ensuring public sector complies similarly.

Gap 7: Patient Rights Execution – While DPDP grants rights, there is a gap in user-friendly mechanisms to exercise them in healthcare. For instance, GDPR induced hospitals to set up patient portals for data requests. In India, few hospitals have such systems yet. Without accessible channels, rights exist on paper but not in reality. ABDM's infrastructure might help (a patient could potentially use their health locker to see and manage data, which covers the access right somewhat). But for withdrawal of consent or deletion, processes are unclear – can a patient demand a hospital delete their record? Under DPDP Act they can request erasure, but medical laws require some retention. Such conflicts need reconciliation. Thus, a challenge is aligning DPDP rights with medical record-keeping norms and creating clear guidelines on how to honour rights without compromising continuity of care. This hasn't been fully addressed yet.

3.4 Challenge:

Ensuring Cybersecurity Investment

– Indian healthcare spending on IT security is generally low (<5% of IT budget often). Convincing management to invest is a challenge unless driven by either regulation or painful incidents. The results suggest that after big attacks, there is wake-up action (the Health Ministry did order audits after AIIMS attack). But a sustained program (like NHS had a one-time £60m investment post-WannaCry to boost hospital cybersecurity) may be needed. Without plugging this, India's digital health could face repeated disruptions and loss of trust. In the comparative context, this is not a "gap" in regulatory

text but a gap in system readiness relative to what is necessary in light of global threat environment.

To summarize the comparative outcome: India has taken important steps but falls short of global frameworks in specific legal provisions (special protection for health data, breach notifications) and in maturity of implementation (security practices, compliance culture). The identified gaps and challenges are critical areas for improvement. These findings will inform the Discussion in the next chapter, which will interpret their implications and suggest recommendations for bridging these gaps, ultimately answering the research question of how to elevate India's data governance and cybersecurity in digital health to meet global standards.

CHAPTER 4 DISCUSSION

In this chapter, the implications of the findings are examined, and the main research question is addressed: What are the gaps and challenges of India's data governance and cybersecurity policies in digital healthcare when compared with global standards? The discussion is organized around key findings, interpreting their significance in the broader context, and leads into concrete recommendations and policy implications.

4.1 Interpretation of Key Findings

The comparative results illustrate that India is at an early but promising stage in establishing a robust data governance framework for digital health. The passage of the DPDP Act 2023 and launch of ABDM mark a paradigm shift from a previously fragmented approach to a more unified vision of protecting personal data, including health data. However, when benchmarked against global exemplars like HIPAA, GDPR, and NHS's practices, several shortcomings become evident.

A central interpretation is that India's regulatory framework is currently more generalized and less prescriptive for healthcare, which could result in both under-protection of patient data and uncertainty among healthcare providers. Global frameworks by contrast either tailor the rules to healthcare (as HIPAA does) or explicitly recognize the heightened sensitivity of health data (as GDPR does). India's choice not to have a special category for health data in the DPDP Act signals a reliance on one- size-fits-all data protection. This might simplify compliance on paper, but in

practice, it does not account for the unique ethical and practical considerations of healthcare data handling (for example, the necessity to share data quickly in patient interest vs. the obligation to maintain confidentiality).

Another interpretation is that enforcement and accountability mechanisms in India are still largely untested and potentially weak in the health context. Enforcement historically has been reactive rather than proactive – the AIIMS breach outcome, for instance, involved post-incident scrambling rather than preventive oversight. Global standards show that having teeth in enforcement (like heavy fines and audit requirements) changes organizational behaviour. India's DPDP Act provides for fines, but the actual enforcement will depend on the capacity and will of the Data Protection Board. If enforcement remains lax (due to capacity issues or political hesitation to penalize especially government-run entities), the law's deterrent effect will diminish. Essentially, the law's presence alone is not enough; implementation will make or break its success.

The findings also highlight a tension between innovation/utilization of health data and privacy/ security. For India, with massive health datasets potential, there is a huge opportunity to leverage data for public health (predicting outbreaks, planning resources) and AI-driven solutions. The ABDM framework encourages sharing data for such beneficial uses in anonymized form. Global frameworks too allow research use (GDPR has provisions for research exemptions with safeguards). The challenge is ensuring that this does not become a loophole for misuse. The DPDP Act currently doesn't elaborate on research uses or secondary use of health data. If left ambiguous, it might either stifle legitimate research (if organizations err on side of caution) or expose data to misuse (if they too liberally assume deemed consent). Therefore, interpreting the gap, there's a need for clearer rules around when and how health data can be used beyond direct care, without compromising privacy. This is exactly what HIPAA's Privacy Rule does by defining permitted uses and requiring authorizations for others, and what GDPR does by requiring either consent or strong anonymization for secondary use.

In sum, the key findings suggest that while India has the skeletal framework now, it lacks the fleshed-out musculature and reflexes that global systems have developed over years: - The "musculature" being specific provisions and guidelines for handling health data; - The "reflexes" being well-practiced incident response, user-rights facilitation, and continuous compliance improvement.

Addressing these will be crucial for India to truly safeguard digital health data.

4.2 Regulatory Gaps in India with Global Standards

From the gaps identified, some deserve further discussion for policy consideration:

Special Protection for Health Data: The decision not to categorize any data as sensitive in DPDP Act has drawn criticism from privacy advocates . Global experience shows health data is often targeted (medical identity theft, insurance fraud, etc.) and breaches can be deeply personal. By treating all personal data alike, the Indian law misses an opportunity to mandate stronger protection where it's due. For example, under the older regime, health data required explicit consent (2011 Rules) , whereas now a hospital might argue implied consent is enough for a lot of processing since the Act doesn't say otherwise. This is a step backwards in privacy stringency. The rationale given by drafters was likely to simplify the law and avoid ambiguity of categorization. But in doing so, they've placed the onus on data fiduciaries to decide sensitivity case-by-case. It would be prudent for the government or Data Protection Board to issue guidance that health data be accorded higher protection as a matter of best practice, even if not mandated. Alternatively, the government could use rule-making power to introduce a subclass of significant fiduciaries specifically for those handling health data, thereby indirectly acknowledging sensitivity and imposing extra duties (like annual audits, appointing a DPO, etc.)

Emergency and Care Exemptions: The results made clear that one of the trickiest gaps is the lack of a "routine care" exemption. The DPDP Act's exemption for medical emergency or epidemic is useful but too narrow. It doesn't cover, say, a doctor referring a case to a specialist in normal (non-emergency) circumstances. Should each such referral has to go through a formal consent? Globally, that's not expected; the patient's general consent to treatment covers it. In India, perhaps an argument can be made that when a patient signs a hospital admission form, they can be informed that their data will be used/ disclosed to other treating providers as needed – and that constitutes consent under the Act. However, the Act's consent requirements are strict and may not be met by a one-time hospital form unless carefully worded. This regulatory gap could hamper integrated care if interpreted strictly. The National Medical Commission or MoHFW might need to step in to provide ethical guidelines that align with data law – e.g., a guideline that says "obtaining consent for sharing with other providers is part of

informed consent for treatment, and should be documented in the patient's initial consent form." Such clarity would harmonize medical practice with legal expectations.

Breach Notification and Transparency: The gap here is stark. After the AIIMS breach, for example, patients whose data might have been stolen were not individually alerted. Contrast with how, in the US, large breaches result in hospitals sending letters to patients advising them of the breach and offering credit monitoring. Not informing patients not only is unfair to them but also misses a chance to make institutions accountable (if patients knew, they could demand answers, sue, or pressure for improvements). The DPDP Act in current form seems to center around penalizing organizations (penalties to Consolidated Fund), but not explicitly around remedying individual harm. That perspective should shift – data protection is ultimately about protecting individuals, not just punishing companies. Embracing a GDPR-like breach notification rule would align with global standards and likely drive better security (since organizations dread the reputational damage of notifying customers). While including such a rule in the Act would have been ideal, it can still be introduced via rules or sectoral guidelines. CERT-In's 6-hour reporting rule is there, but it is more for government awareness and doesn't ensure user notification. Perhaps the Data Protection Board, once established, could make it a practice to require fiduciaries to notify users when a significant breach is reported to them.

Liability and Compliance of Third Parties: As discussed, not holding processors directly liable might be workable if the primary fiduciary is big enough to enforce contracts (e.g., a big hospital can demand its IT vendor comply or face contract breach). But in situations where the data fiduciary is small or unaware (imagine a small clinic using a third-party app for appointments that stores patient info – the clinic might not have legal know-how to ensure contracts cover everything), patient data could slip through cracks. Global standards bring those processors into regulatory reach; India might need to consider either an expansion of DPDP Act in future amendments to cover processors (somewhat like GDPR does) or specific sectoral licensing. For instance, perhaps the upcoming Digital Health Authority (if reintroduced from DISHA plans) could certify health data processors and hold them to standards.

Public vs Private Sector Accountability: The discussion should also acknowledge the political economy: imposing large fines on a public hospital like AIIMS effectively means government paying itself and less budget for the hospital, which is counterproductive to public health. That may be one reason governments are hesitant to

punish their own institutions. But an alternative accountability mechanism must exist. Perhaps a system of publicly available audit reports for public hospitals (instead of fines) could drive change – if AIIMS had to publish an annual data protection audit and it showed gaps, Parliament and the public could hold it accountable. The UK sort of does that through NHS Digital oversight. In India, bringing health under critical infrastructure and requiring NCIIPC audits might help for key hospitals. So, bridging that gap might require creative thinking beyond just copying GDPR fines.

In conclusion, the regulatory gaps identified are significant but not insurmountable. A combination of legal amendments, detailed rule-making, and inter-sectoral coordination (between data protection authority and health authority) can address many of them. The sooner these gaps are filled, the more confidence stakeholders will have in the system.

4.3 Infrastructural and Enforcement Challenges

Beyond written rules, the real test is implementation on the ground. India faces several challenges here:

1.Healthcare IT Infrastructure Variability: Indian healthcare facilities range from state-of-the-art hospitals with integrated EHR systems to small clinics still on paper records. Imposing uniform data protection requirements is challenging because the capacity to comply differs vastly. Many government hospitals are only now moving towards digitization (some propelled by ABDM). These nascent systems might not have mature security controls. The risk is that as we digitize rapidly (to reap benefits of e-health), we might be creating vulnerable points for breaches if security is not concurrently upgraded.

The challenge is to ensure that infrastructure upgrades are holistic: not just digitize for convenience but also secure those digital systems. Budget constraints are real – public sector allocations for IT in health are limited. Private sector might invest more, especially those eyeing medical tourism or accreditation. One suggestion is to integrate cybersecurity requirements into health project funding, e.g., if a state is funding hospital IT modernization, 10% of that budget must go to security measures and training. International aid or public-private partnerships could also focus on this (“cyber health capacity building” programs, akin to training hospital staff on new IT).

2. Human Resource and Awareness: A recurring theme is that healthcare workers are not sufficiently aware of data protection principles. A doctor’s primary focus is patient care,

understandably. But in the digital age, they also need to be mindful of how they handle patient data. The concept of a Data Protection Officer or an Information Security Officer is new in many hospitals. Training programs specific to healthcare (maybe short courses certified by bodies like DSCI or medical associations) could empower individuals to take on these roles.

Enforcement here also means internal enforcement – hospital management enforcing policies on their staff. The NHS toolkit's requirement of annual training and tests for all staff is something Indian hospitals could emulate voluntarily or as required by NHA/NABH accreditation. One practical step: incorporate data privacy and security into medical and nursing curricula. If new doctors and nurses learn about confidentiality in the digital context (not just the traditional sense), they will carry that mindset.

3. Multiplicity of Regulators and Coordination: Digital health in India sits at the intersection of health ministry, IT ministry (which handles data laws), and even agencies like NHA, CERT-In, NCIIPC. Coordination is crucial. A challenge is to avoid regulatory silos or conflicting directives. For example, CERT-In might tell a hospital to do X in response to a cyber threat, while DPB might have another requirement for reporting. Coordination, maybe via a joint task force on health data protection comprising officials from MoHFW, MeitY, NHA, CERT-In, would help streamline efforts. Without it, hospitals might be confused about whom to report to or what standard to follow.

4. Enforcement Approach: How the Data Protection Board approaches the health sector will set the tone. If it comes down heavy with penalties for minor breaches or uses a punitive approach without guidance, there might be pushback or even chilling effects on digital adoption (e.g., small clinics deciding not to digitalize records for fear of legal trouble). On the other hand, too lenient an approach (just warnings, no fines even for serious negligence) will fail to create change. A balanced enforcement strategy is needed: initial period of educating and issuing warnings, followed by stricter action for willful or repeated failures. The DPB could issue sector-specific codes of practice – maybe work with NHA to create one for healthcare – and use those as a basis to judge compliance.

5. Dealing with Legacy Systems and Data: Many hospitals have legacy software that may not meet modern security standards, but replacing them is costly and time-consuming (especially if patient data migration is involved). This is a challenge in achieving compliance. For instance, an old pathology lab system might store passwords

in plain text or not encrypt data at rest – fixing that might require a new system. Hospitals will have to prioritize risks; perhaps an incentive (tax breaks for health IT improvements or government funding) could accelerate upgrades. The analog in the West was when HITECH gave incentives for EHR adoption – perhaps India could have incentives for "secure EHR adoption or ABDM adoption" where part of funding can be used for security measures.

In summary, enforcement and infrastructure challenges are about building the ecosystem capacity: - Technical (better systems, networks, backup solutions to mitigate ransomware effects – e.g., the 3-2-1 backup strategy as suggested). - Organizational (policies, roles like DPO, routine drills, audits). - Cultural (every healthcare worker understanding that protecting patient data is part of their duty of care).

Addressing these is not a quick fix; it will be a process. But acknowledging them is the first step, and the recommendations will suggest ways to start tackling these challenges systematically.

4.4 Recommendations for Strengthening Data Governance and Security in India's Digital Health Ecosystem

Based on the comparative insights and identified gaps, several recommendations can be made:

1. Issue Health Sector Rules or Guidelines under the DPDP Act: The central government, possibly in consultation with the proposed Data Protection Board and Ministry of Health, should promulgate rules or at least official guidelines specifically addressing health data. These should: - Clarify that sharing of personal health data among treating healthcare providers for the purpose of patient care is considered a "reasonable purpose" or falls under deemed consent, to remove ambiguity and fear among providers (essentially codifying what Sood et al. recommended as an exemption for patient care).

- Mandate that any significant breach of health data (above a threshold of records compromised) must be notified to the impacted individuals and to a central authority (Data Protection Board or CERT-In). This could be modeled on HITECH/GDPR breach notification standards.

- Encourage or require pseudonymization or anonymization when using patient data for secondary purposes like research, and require Institutional Ethics Committee approval

for using identifiable data in research if consent is not being taken (aligning with Sood et al.'s Recommendation 3).

- Emphasize duties of data processors (IT service providers) in handling health data, even if the Act doesn't directly penalize them – perhaps by requiring that health sector contracts include specific data protection clauses and making the health institution responsible to ensure its vendors comply.

- Possibly set a timeline for legacy compliance – e.g., within 2 years, all health facilities processing digital personal data should implement XYZ minimum security measures (this could align with NDHM's policy which sets minimum standards).

2. Empower a Sectoral Agency (like NHA or a revived NeHA) to Oversee Digital Health Data Protection: Having a dedicated body that understands healthcare operations can help translate data protection principles on the ground. This body can:

- Develop standard operating procedures (SOPs) and toolkits for hospitals/clinics to implement DPDP Act requirements – for instance, templates for consent forms, privacy policy templates tailored for hospitals, breach response plan templates, etc.

- Conduct periodic audits or require self-assessments akin to the NHS DSP Toolkit. For example, NHA could require hospitals enrolled in ABDM to annually submit a compliance checklist covering training done, security updates applied, number of breaches, etc. This nudges institutions to review themselves regularly.

- Coordinate with CERT-In for sector-specific threat intelligence sharing. The healthcare sector could have a special Information Sharing and Analysis Center (ISAC) where hospitals get updates on latest cyber threats and vulnerabilities.

- Work with insurance companies to possibly include cyber liability coverage for hospitals – this can indirectly enforce good behavior as insurers might require certain security posture for coverage.

3. Invest in Capacity Building and Training: A multi-tier approach is needed: - Healthcare Leadership Training: Hospital executives and administrators need to grasp the importance of data governance. Bootcamps or executive courses (maybe in collaboration with bodies like IIHMR or IIMs) focusing on healthcare cybersecurity and privacy management can be offered.

- Clinician Awareness: Incorporate data privacy and cybersecurity modules in Continuous Medical Education (CME) and nursing education. Even simple guidelines like “Don’t share patient data on social media or insecure apps without consent” can go a long way. The medical community should treat patient data confidentiality in electronic form with the same seriousness as they treat traditional ethical confidentiality.

- Technical Staff Upskilling: Many hospitals have IT departments but need specialization in cybersecurity. Government could subsidize certifications for hospital IT staff (such as Certified Cybersecurity Technician, or healthcare-specific security courses).

- Workshops and Conferences: As recommended in literature , hold workshops – possibly NHA and MeitY jointly – across regions to explain the DPDP Act to healthcare entities, share best practices (maybe have experts from EU/US share experiences). These should be done sooner rather than later, to prepare stakeholders before enforcement of penalties begins in earnest.

4. Strengthen Technical Infrastructure and Standards: Recommendations here include: - Adopt Standards: Encourage or require healthcare organizations to follow recognized security standards (ISO 27001 for information security, or the healthcare-specific ISO 27799, or even basic frameworks like Cyber Essentials as in UK). The government could create a voluntary certification for “Health Data Secure” for hospitals that meet a set of standards, which might over time become an industry mark that patients trust. - Secure IT Procurement: Every new IT system in healthcare (like HMS, LIS, telemedicine platform) should be vetted for security (perhaps require developers to comply with NDHM’s Security Standards and get certification). NHA could maintain an approved list of applications that meet security criteria for use in healthcare, to guide smaller providers who may not know how to choose secure software.

- Incident Response Mechanism: Establish a clear incident response channel for healthcare. For example, a dedicated healthcare-CERT or a helpline that hospitals can call when under attack, to get expert guidance. The quicker the response, the less the damage (the AIIMS case taught that delays in response/expertise prolonged the outage).

- Data Minimization and Retention: Hospitals should be guided to not hoard data unnecessarily. Many hospitals in India keep patient data indefinitely due to lack of policy, increasing breach impact. Setting retention schedules (e.g., delete or archive with higher security any data older than X years unless needed for active care) and deletion

protocols in line with legal requirements can reduce the amount of data at risk. GDPR strongly advocates data minimization; Indian practice would benefit from adopting that mindset.

5. Improve Public Awareness and Patient Engagement: When patients start valuing privacy, they will demand it from providers, creating bottom-up pressure for better practices. To that end:

- ABDM could include patient-facing notifications: e.g., whenever someone views their health record via the network, they get an alert (some parts of ABDM do this, like when you share an OTP to link records). Extending such transparency builds trust and awareness.

- Run public service campaigns or incorporate in health insurance policies some information about data privacy rights. For instance, insurers could inform policyholders that their health data is protected and they have rights under DPDP Act (this both educates and assures them).

- Patient advocacy groups (or consumer rights orgs) should be encouraged/supported to include digital privacy in their agenda. If they test and publish report cards, say on how different hospital chains handle data (which have good privacy notices, which respond to data requests, etc.), it can spur competition on privacy as a quality parameter.

6. Address Public Sector Issues: Specifically for government hospitals and programs:

- They should lead by example. MoHFW can direct all its institutions to implement the recommendations above and perhaps undergo third-party security assessments yearly. The results might not be public immediately, but at least the process will start.

- Allocate dedicated budget lines for cybersecurity in public health sector (the suggestion in Sood et al.'s Recommendation 6 was to include provisions for cybersecurity in annual health expenditure). This ensures it's not optional or ad-hoc.

- Update the government hospital management manuals to include data protection accountability.

– for example, make the Medical Superintendent responsible for data protection compliance in addition to clinical services.

7. Continual Policy Review and Alignment: Technology and threats evolve. The government should periodically review and update the data protection approach for health:

- If something like DISHA is revived, ensure it complements DPDP Act and perhaps gives more operational detail rather than creating conflicting requirements.

- Keep an eye on global developments, like the proposed EU Health Data Space, which aims to standardize electronic health record exchange while maintaining privacy. India's ABDM can take cues to ensure interoperability doesn't compromise privacy (like how EU is building in consent and audit trails into the Health Data Space).

- Engage with international forums on digital health (e.g., Global Digital Health Partnership) to learn best practices and showcase what India is doing, fostering cross-pollination of ideas.

In making these recommendations, it's understood that resource and capacity constraints are real. Therefore, a risk-based approach is prudent: focus first on high-impact areas (large hospitals, big data processors, national programs) for stringent measures, while gradually bringing smaller entities up to speed with support.

4.5 Implications for Policy and Future Research

Policy Implications: The recommendations, if implemented, would significantly tighten India's data governance regime in healthcare. Policymakers should realize that data protection in health is not merely a compliance issue but also a public health issue: a major data breach can erode trust in health systems, leading patients to withhold information or avoid digital services, ultimately impacting care delivery. Conversely, strong data governance can be an enabler – patients and providers will be more willing to use digital tools if they trust them. India's vision of a digital health ecosystem (ABDM) hinges on that trust.

A specific implication is that India may need to amend its new law or supplement it. That is always a political and bureaucratic undertaking. However, given that DPDP Act is brand new, it might be wise to see how it plays out and use the flexibility in rules to address sector needs in short term. If down the line it's seen that health (and maybe finance, etc.) would benefit from extra legal provisions, an amendment or a separate health data law like DISHA could be reconsidered. The comparative review might support the argument that a dedicated legal instrument for health data (like HIPAA,

albeit tuned to India's context) could still be valuable to pursue in the future, if the general law approach proves insufficient.

Implementation Timeline: The DPDP Act is expected to roll out over 2024 (with full enforcement perhaps by end 2024). ABDM is ongoing. It's a ripe moment to integrate privacy and security into these initiatives rather than retrofitting later. The policy implication is urgent action required: government should not wait for a big scandal to make changes, they have the information now (some from their own commissioned studies, as well as what has been discussed here).

Resource Allocation: These improvements will need funding – whether it's training thousands of personnel or upgrading systems. Government budgets and private healthcare budgets need to account for this. Perhaps a public-private fund could be established to support cybersecurity in healthcare (with contributions from big tech firms as part of CSR, since they also benefit from safe digital ecosystems). It's a policy idea worth exploring.

Legal Liability and Redress: The discussion also implies that patient redress mechanisms should be strengthened. If a patient's data is misused, currently their remedy is to complain to DPB or maybe sue under tort (which is cumbersome). Global practice allows class actions or regulator-facilitated compensation. India might consider introducing easier redress (maybe health ombudsman roles that include data complaints, or enabling consumer courts to take up such issues swiftly). The benefit is twofold: justice for affected individuals and pressure on institutions to avoid negligence.

Future Research Needs: While this dissertation provides a broad review, further research could deepen understanding in specific areas: - Empirical studies on compliance readiness: Survey hospitals to gauge their current data protection measures. This would provide baseline metrics to measure improvement over time. - Impact of breaches on patient behavior: Research how data breaches (like AIIMS) affect patient trust and engagement with digital health. Quantifying that impact could motivate stronger policies. - Cost- benefit analysis of implementing data security in healthcare: To convince decision-makers, research showing the return on investment (ROI) of cybersecurity spending in hospitals (perhaps by comparing breach costs vs. prevention costs) could be influential.

- Comparative case studies of enforcement: Study a few breach cases in EU/US vs similar incidents in India to highlight differences. This could yield practical lessons for Indian regulators on what strategies work in enforcement and breach management.

- Technological solutions research: Explore emerging tech such as blockchain for health records (some literature alludes to it improving security and patient control) in the Indian context – pilot projects could be studied to see if they indeed bolster data governance.

Ethical and Social Considerations: As India strengthens data governance, it must consider ethics, especially because health data often involves issues of consent (like for minors, or for people who might not fully understand digital processes). There's a social dimension: many Indians are not digitally literate, so expecting them to manage consents via an app might exclude or confuse them. Policies should ensure inclusion – e.g., allow offline consent or have patient counselors to help with ABDM processes. These fine- grained issues would benefit from socio-legal research and user experience studies.

In closing this discussion: India stands to gain enormously from digital health, but that won't happen without winning patient trust. Strong data governance and cybersecurity are the guardians of that trust. Learning from global frameworks, India can leapfrog by not repeating mistakes and adopting best practices swiftly. The gaps identified are not indictments but opportunities for improvement. The challenges are significant, yet with concerted effort from regulators, healthcare institutions, and technology partners, they can be overcome. Doing so will safeguard patients' fundamental right to privacy while enabling the digital health revolution to improve healthcare outcomes nationwide.

CHAPTER 5 CONCLUSION

Digital healthcare in India is at a pivotal juncture. The nation is embracing technologies that promise accessible, efficient, and personalized care for over a billion people. However, as this dissertation has explored, the backbone of a successful digital health ecosystem is robust data governance and cybersecurity. Without these, the digital promise could be undermined by data breaches, loss of public trust, and harm to patients.

This thesis set out to compare global frameworks for health data governance with India's emerging regulatory ecosystem, in order to identify gaps and challenges. Through a comprehensive literature review and analysis, several conclusions can be drawn:

• Global frameworks provide valuable blueprints: The experience of HIPAA and HITECH in the US demonstrates the benefit of sector-specific rules that clearly delineate how health information can be used and protected. GDPR in Europe exemplifies the power of comprehensive data rights and strong enforcement to induce a culture of privacy in all sectors, including health. The NHS's DSP Toolkit underscores the importance of operationalizing principles into everyday practices and audits. These frameworks, though varied, converge on common principles of patient consent, confidentiality, security safeguards, and accountability for misuse.

• India has made important strides, but critical gaps remain: The introduction of the Digital Personal Data Protection Act, 2023 and initiatives like ABDM show India's commitment to data protection. However, the DPDP Act in its current form lacks health-specific provisions (for instance, it does not give special status to health data), and there is ambiguity in how traditional healthcare practices fit into the new consent requirements. The comparison highlighted that India does not yet mandate breach notifications to individuals, has not directly imposed obligations on health IT vendors, and is still developing a compliance enforcement regime. Additionally, infrastructural challenges – such as outdated systems and insufficient cybersecurity measures in many hospitals – pose serious risks as seen in incidents like the AIIMS ransomware attack.

• The gaps identified could weaken patient privacy and safety if not addressed: Key areas of concern include the need for clearer guidelines on data sharing for patient care

(so that doctors can collaborate without legal fear, yet patients' privacy is respected), stronger breach response requirements to ensure transparency and remediation after incidents, and measures to improve cybersecurity posture across the health sector (through standards, audits, and training). If these gaps persist, India may face a dual problem: on one hand, potential misuse or breaches of health data affecting individuals' privacy and, on the other, hesitation among healthcare providers to fully utilize digital tools due to unclear or onerous regulations.

• Bridging these gaps is feasible and urgent: The dissertation's recommendations outline a path forward, including introducing health-specific rules under the DPDP Act, possibly drawing from the DISHA draft to resurrect useful elements like dedicated health data authorities or consent requirements. Investing in capacity building – essentially creating a privacy and security-aware workforce in healthcare – is a high priority, echoing the global best practice that people are the first line of defense as well as potential points of failure . There is also a strong case for leveraging India's strength in IT to develop or adopt technological solutions (for example, secure health information exchange platforms, encryption tools, anonymization techniques) that can embed privacy by design into digital health infrastructure.

• Ultimately, data governance is an enabler, not an impediment, of digital health: A key insight from the literature is that good data governance and cybersecurity practices not only protect patients, but also enable trust which is foundational for the uptake of digital health services. Countries that have high trust in their health systems' data handling see greater use of electronic health records, health apps, and data-driven innovations. India's regulatory ecosystem should thus aim to enhance trust by being transparent, fair, and effective in protecting health data. This involves not just creating rules but also ensuring they are followed and that violators are held accountable, which in turn will deter negligence and malicious behaviour.

In conclusion, the research question can be answered as follows: India's data governance and cybersecurity policies in digital healthcare are developing rapidly, but compared to global standards, they currently exhibit significant gaps in legal provisions, implementation capacity, and enforcement rigor. These gaps manifest as unclear guidelines for data use and sharing, insufficient emphasis on breach accountability, and underinvestment in security measures. The challenges to closing these gaps include raising awareness, building technical and organizational capacity, and ensuring cohesive

oversight. However, by learning from international frameworks and adapting their strengths to the Indian context, India can address these shortcomings.

The dissertation underscores that addressing these issues is not merely a compliance exercise, but a necessary step to protect patient rights and to ensure the long-term success of digital health initiatives. It calls upon policymakers, healthcare institutions, and technology partners to collaborate in fortifying the foundations of data governance in healthcare. As India moves forward, the comparative lens provided by this study should serve as a guide: highlighting what to emulate, what to avoid, and what innovative solutions might be crafted to suit India's unique context. With timely and decisive action on the recommendations, India can aspire to not only meet global standards but potentially set new ones in the realm of digital health data protection, thereby safeguarding the health and privacy of its citizens in equal measure.

BIBLIOGRAPHY

1. Sood A, Mishra S, Chavan NA, et al. Challenges and recommendations for enhancing digital data protection in Indian Medical Research and Healthcare Sector. NPJ Digital Medicine. 2025;8(1): Article 123.
2. Burde H. THE HITECH ACT: An Overview. AMA Journal of Ethics. 2011;13(3):172-175.
3. European Union. Regulation (EU) 2016/679 (General Data Protection Regulation). 2016. Articles 5, 9, 32, 33.
4. NHS Digital (UK). Data Security and Protection Toolkit (DSP Toolkit) Guidelines. 2021.
5. Health Insurance Portability and Accountability Act (HIPAA), Pub.L. 104–191. Privacy Rule (45 CFR §164.502) and Security Rule (45 CFR §§164.306-316).
6. Office for Civil Rights, HHS (USA). Summary of the HIPAA Privacy Rule and Summary of the HIPAA Security Rule. 2013.
7. Ministry of Electronics & IT (India). The Digital Personal Data Protection Act, 2023. Gazette of India, Aug 2023. Sections 4, 7, 8, 33.
8. National Health Authority (India). Ayushman Bharat Digital Mission: Health Data Management Policy (version 2022).
9. Express Healthcare News. Data privacy in healthcare (Chigateri C). Express Healthcare. Jan 21, 2022.
10. NLIU Cell for IPR (McDonald S). The AIIMS Cyber-Attack and India's Dilapidated Cyber-security Infrastructure. Blog post. Jan 26, 2023.

11. Internet Freedom Foundation (India). Analysis of the DPDP Act in context of health data (CCG Blog). Feb 13, 2024.

12. VitalHub (Abesamis N). What is the NHS Data Security and Protection Toolkit? Blog post. Mar 24, 2024.

13. CERT-In (India). Directions under sub-section (6) of section 70B of the IT Act, 2000 (regarding cyber incident reporting). April 28, 2022.

14. Data Security Council of India (DSCI). Privacy and Security Guidelines for Healthcare Sector. 2020.

15. Moneycontrol News. Indian healthcare sector at high risk of cyber attacks (report excerpt). 2022.

16. Hindustan Times. AIIMS server attack originated from abroad, exposes 4 crore records. Nov 2022.

17. The Hindu. 1.3 TB of data encrypted in AIIMS cyberattack: officials. Dec 2022.

18. Information Technology Act, 2000 (India). Section 43A (Inserted 2008) & IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

19. National Medical Commission (India). Registered Medical Practitioner (Professional Conduct) Regulations, 2023 – Clause on Patient Privacy.

20. Ahmed A, Shahzad A, et al. Evaluating the effectiveness of data governance frameworks in healthcare data security (ISO, GDPR, HIPAA) using blockchain. PLOS ONE. 2025;20(5).

Pearl Jaggi D report

ORIGINALITY REPORT

7%	5%	5%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to NALSAR University of Law Hyderabad Student Paper	<1%
2	fastercapital.com Internet Source	<1%
3	"International Transfers of Health Data", Springer Science and Business Media LLC, 2024 Publication	<1%
4	Chukwuka Elendu, Eunice K. Omeludike, Praise O. Oloyede, Babajide T. Obidigbo, Janet C. Omeludike. "Legal implications for clinicians in cybersecurity incidents: A review", Medicine, 2024 Publication	<1%
5	pmc.ncbi.nlm.nih.gov Internet Source	<1%
6	www.coursehero.com Internet Source	<1%
	cis-india.org	

7	Internet Source	<1%
8	www.slideshare.net Internet Source	<1%
9	Submitted to University of Northumbria at Newcastle Student Paper	<1%
10	www.orfonline.org Internet Source	<1%
11	www.accountablehq.com Internet Source	<1%
12	Submitted to B.V. B College of Engineering and Technology, Hubli Student Paper	<1%
13	Sonali Dhananjay Patil, Rajesh Ingle, Amar Buchade, Vidy Potdar. "Decentralized Healing – Transforming Healthcare with Federated Learning and Blockchain Technologies", CRC Press, 2025 Publication	<1%
14	Submitted to The University of Law Ltd Student Paper	<1%
15	Vasudha Khanna, Atul Kotwal. "Examining the significance of the digital personal data protection act, 2023 in the context of the	<1%

	healthcare industry: a comprehensive analysis", Discover Public Health, 2025 Publication	
16	www.indcareer.com Internet Source	<1%
17	www.india.gov.in Internet Source	<1%
18	Submitted to Uttaranchal University, Dehradun Student Paper	<1%
19	Submitted to Concordia University Student Paper	<1%
20	hipaasolutions.net Internet Source	<1%
21	Submitted to National School of Healthcare Science Student Paper	<1%
22	systematicreviewsjournal.biomedcentral.com Internet Source	<1%
23	alumni-portal.sasin.edu Internet Source	<1%
24	elibrary.tucl.edu.np Internet Source	<1%
25	en.wikipedia.org Internet Source	<1%

26	Minal R. Narkhede, Nilesh I. Wankhede, Akanksha M. Kamble. "Enhancing patient autonomy in data ownership: privacy models and consent frameworks for healthcare", Journal of Digital Health, 2025 Publication	<1 %
27	theses.gla.ac.uk Internet Source	<1 %
28	www.healthit.gov Internet Source	<1 %
29	www.kiteworks.com Internet Source	<1 %
30	Submitted to King's College Student Paper	<1 %
31	eucyberdirect.eu Internet Source	<1 %
32	pdf.secdatabase.com Internet Source	<1 %
33	"Autonomous Vehicles and the Law", Walter de Gruyter GmbH, 2025 Publication	<1 %
34	Ariel Evans. "Enterprise Cybersecurity in Digital Business – Building a Cyber Resilient Organization", Routledge, 2022 Publication	<1 %

35	www.mdpi.com Internet Source	<1 %
36	Submitted to American InterContinental University Student Paper	<1 %
37	Submitted to Fakir Mohan University Student Paper	<1 %
38	Jon Rueda, Sebastian Porsdam Mann, Janet Delgado, Brian D. Earp et al. "Data governance must consider the interests of the global community", Nature Medicine, 2025 Publication	<1 %
39	Maria Tzanou. "Health Data Privacy under the GDPR – Big Data Challenges and Regulatory Responses", Routledge, 2020 Publication	<1 %
40	Submitted to Southern New Hampshire University – Continuing Education Student Paper	<1 %
41	btlj.org Internet Source	<1 %
42	digital.nhs.uk Internet Source	<1 %
43	Submitted to Capella University Student Paper	<1 %

44	Submitted to Colorado Technical University Online Student Paper	<1%
45	Michaela Th. Mayrhofer, Santa Slokenberga, Signe Mežinska. "Artificial Intelligence in Biobanking – Ethical, Legal and Societal Challenges", Routledge, 2025 Publication	<1%
46	Submitted to Swiss School of Business and Management – SSBM Student Paper	<1%
47	Submitted to The WB National University of Juridical Sciences Student Paper	<1%
48	Submitted to UCL Student Paper	<1%
49	Submitted to University of College Cork Student Paper	<1%
50	etda.libraries.psu.edu Internet Source	<1%
51	podtail.com Internet Source	<1%
52	Submitted to Indiana University Student Paper	<1%
53	quarterlytics.com Internet Source	

		<1%
54	www.bdo.global Internet Source	<1%
55	www.davidsonmorris.com Internet Source	<1%
56	www.dlapiperdataprotection.com Internet Source	<1%
57	www.ijser.in Internet Source	<1%
58	www.lexology.com Internet Source	<1%
59	Ashwaghosha Parthasarathi, Tina George, Muruga Bharathy Kalimuth, Sudhindra Jayasimha et al. "Exploring the potential of telemedicine for improved primary healthcare in India: a comprehensive review", The Lancet Regional Health – Southeast Asia, 2024 Publication	<1%
60	Submitted to Middlesex University Student Paper	<1%
61	cookie-script.com Internet Source	<1%
62	eprints.usm.my Internet Source	<1%

63	newincmagazine.com Internet Source	<1%
64	sundayguardianlive.com Internet Source	<1%
65	Giovanna De Minico, Oreste Pollicino. "Virtual Freedoms, Terrorism and the Law", Routledge, 2021 Publication	<1%
66	Submitted to Indian School of Business Student Paper	<1%
67	Mathilde Léon, Marion Korwin-Zmijowski, Alejandrina Cristia. "Regulation relevant to (long-form) audio recordings gathered in India", Open Science Framework, 2023 Publication	<1%
68	Pushan Kumar Dutta, Martin Ricciuti, Ismail Bogrekci, Sumeet Suseelan. "Airline Customer Experience – Digitalization in Passenger Services", Routledge, 2025 Publication	<1%
69	bmchealthservres.biomedcentral.com Internet Source	<1%
70	brightideas.houstontx.gov Internet Source	<1%
71	comms.southsudanngoforum.org Internet Source	<1%

72	enhelion.com Internet Source	<1%
73	the420.in Internet Source	<1%
74	www.euroconsult-ec.com Internet Source	<1%
75	Amit Gupta, Harpreet Singh, Riddhi Sancheti, Saurabh Jha, Krithika Rangarajan. "Legalities, Ethics and Frameworks for Healthcare AI in India", Academic Radiology, 2025 Publication	<1%
76	Andrew Denley, Mark Foulsham, Brian Hitchen. "GDPR – How to Achieve and Maintain Compliance", Routledge, 2019 Publication	<1%
77	Eriona Çela, Narasimha Rao Vajjhala, Behrouz Aslani. "Artificial Intelligence in Legal Systems – Bridging Law and Technology through AI", CRC Press, 2025 Publication	<1%
78	John J. Trinckes. "The Definitive Guide to Complying with the HIPAA/HITECH Privacy and Security Rules", CRC Press, 2012 Publication	<1%
79	K. P. Jaheer Mukthar, Rosario Mercedes Huerta-Soto, Vishal Jain, Edwin Hernan	<1%

	Ramirez-Asis. "AI and Fintech – Improving the Financial Landscape", CRC Press, 2025 Publication	
80	Submitted to University of Delhi Student Paper	<1%
81	authors.go2articles.com Internet Source	<1%
82	cust.edu.pk Internet Source	<1%
83	essay.utwente.nl Internet Source	<1%
84	ijlr.iledu.in Internet Source	<1%
85	www.cpomagazine.com Internet Source	<1%
86	www.frontiersin.org Internet Source	<1%
87	www.gdpr-advisor.com Internet Source	<1%
88	www.gibsondunn.com Internet Source	<1%
89	www.sattrix.com Internet Source	<1%

90	Ísis de Siqueira Silva, Cícera Renata Diniz Vieira Silva, Claudia Santos Martiniano, Aguinaldo José de Araújo et al. "Digital health and quality of care in Primary Health Care: an evaluation model", Frontiers in Public Health, 2024 Publication	<1 %
91	Josh Cowls. "Chapter 9 Privacy Risks and Responses in the Digital Age", Springer Science and Business Media LLC, 2019 Publication	<1 %
92	Tümtürk, Asli Alkis. "A Comparative Study of the Online Privacy and Data Protection of Children in the European Union and the United States.", Szeged University (Hungary), 2024 Publication	<1 %
93	zuniclaw.com Internet Source	<1 %
94	Shemphang Wann Lyngdoh, Sunil, Mangal Chhering. "chapter 10 Cybersecurity Threats and Legal Responsibilities in E-Business", IGI Global, 2024 Publication	<1 %