Strengthening Health Governance and Data Protection Through the Digital Data Protection Act, 2023 in India's Digital Health Ecosystem

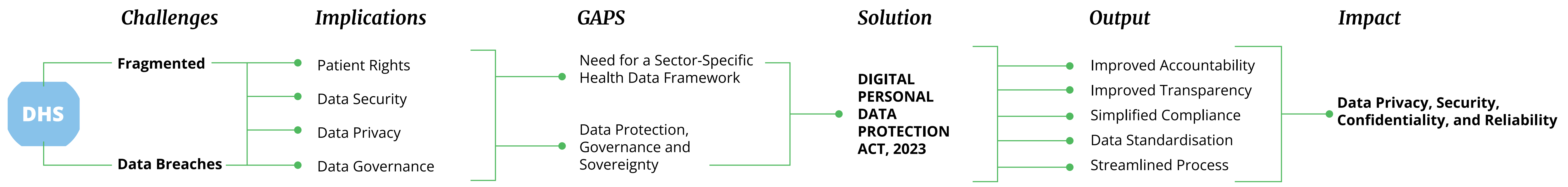
1). Background/Introduction

The digital transformation of healthcare has revolutionized service delivery, patient outcomes, and resource optimization. In India, the government's push for digital health through the Ayushman Bharat Digital Health Mission (ABDM) highlights its commitment to modernizing healthcare. However, the country's health data ecosystem is fragmented, with a complex regulatory framework. This research aims to explore key components for establishing a robust regulatory environment and effective health data governance in India, in alignment with the Digital Personal Data Protection Act (DPDPA), 2023.

2). Objectives:

The study aims to provide a comprehensive roadmap for strengthening health governance and data protection in India's digital health ecosystem. The major objectives of the research study are:

- Examine the current state of India's health data protection frameworks and regulations
- Identify gaps, challenges, and grey areas in India's health data governance ecosystem; and their impact on patient rights and privacy.
- Identify and analyze successful international models of health data governance that could be adapted or replicated in the Indian context.
- Develop policy recommendations for strengthening health data governance in India


Challenges | *Implications* | *GAPS* | *Solution* | *Output* | *Impact*

DHS

Fragmented

Data Breaches

Patient Rights

Data Security

Data Privacy

Data Governance

Need for a Sector-Specific Health Data Framework

Data Protection, Governance and Sovereignty

DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Improved Accountability

Improved Transparency

Simplified Compliance

Data Standardisation

Streamlined Process

Data Privacy, Security, Confidentiality, and Reliability

3). Methodology

3.1 Study Design

This study adopted a mixed-methods approach, combining quantitative and qualitative research techniques to comprehensively analyze the governance and data protection challenges in India's digital health ecosystem. The methodology was divided into four interconnected phases, as given in the figure :

Phase 1: Systematic Literature Review (SLR)

Database selection (e.g., PubMed, JSTOR, Google Scholar).

Inclusion criteria: Peer-reviewed articles, policy briefs, and reports from 2015–2024.

Screening: Titles and abstracts reviewed, followed by full-text analysis.

Data Extraction: Keywords used to elicit details on governance frameworks, security, privacy, and interoperability.

Synthesis: Thematic analysis of common findings (privacy, security, stakeholder roles, interoperability).

Phase 2: Policy Analysis

Frameworks Analyzed: DPDPA, National Digital Health Blueprint (NDHB), Ayushman Bharat Digital Health Mission (ABDM), IT Act, 2000.

Dimensions:
- Scope and objectives of health data governance.
- Stakeholder roles and responsibilities.
- Alignment with global standards (e.g., GDPR, HIPAA).
- Implementation and enforcement strategies.

Comparative Analysis: India's policies compared with global frameworks, identifying strengths and gaps.

Phase 3: Semi-Structured Stakeholder Interviews

Participants: Policymakers, legal experts, healthcare providers, technology developers, civil society organizations.

Sampling: Purposive sampling of 20–30 experts across sectors.

Interview Protocol: Semi-structured interviews exploring challenges in DPDPA implementation, interoperability, data security, and stakeholder roles.

Data Analysis: Qualitative analysis using NVivo, identifying themes and patterns.

Phase 4: Validation Workshop

Participants: Experts from academia, government, industry, and stakeholders from Phase 3.

Structure:
- Presentation of preliminary findings.
- Feedback session for accuracy and gap identification.
- Consensus-building moderated discussion for actionable solutions.

Outcome:
- Integration of stakeholder feedback into final analysis.
- Validation of policy recommendations for practical applicability.

4). Major Results/Findings

4.1 Landscape of India's Digital Health Ecosystem: Key Components

4.1.1 Government Initiatives

a

ABDM Elements:
- ABHA ID (Ayushman Bharat Health Account ID)
- Healthcare Professional Registry (HPR)
- Healthcare Facility Registry (HFR)
- National Health Claims Exchange (HCX)

b

e-Sanjeevani Telemedicine Platform

4.1.2 Private Sector

a. **Telemedicine and virtual care platforms** like Practo, Meddo, Portea, CallHealth, etc.
b. **Health and Wellness Apps** like HealthifyMe, Blyss, Fittr, Livlong
c. **Virtual Pharmacies** like 1mg, Netmeds, and PharmEasy
d. **Digital Health Records & Health Information Systems** with companies like CureMetrix and HealthPlix
e. **Artificial Intelligence (AI) & Machine Learning (ML)** platforms such as Qure.ai and Niramai.
f. **Insurtech companies** like Bajaj Allianz, HDFC ERGO, Religare Health Insurance
g. **Digital Health Wallets and Payment Solutions** with companies like Paytm and PhonePe

4.2 India's Digital Health Ecosystem: Barriers and Challenges

India's digital health ecosystem has witnessed significant progress in the last decade, driven by government initiatives. However, despite these advancements, several challenges continue to hinder the full realization of a robust and equitable digital health ecosystem.

- Fragmentation of regulations, leading to inconsistencies in their application.
- Lack of sector-specific legislation
- Lack of interoperability to enable seamless data exchange across healthcare platforms, systems, and stakeholders
- Scalability issues due to accommodate diverse needs of populations.
- Accessibility issues: connectivity, technological illiteracy, digital infrastructure gaps.
- Data quality and standardization issues, affecting data accuracy & reliability in decision making
- Hesitance and mistrust around digital health platforms
- Issues around data sovereignty and cross-border data flows
- Cybersecurity threats and risks
- Ethical implications of AI and machine learning

4.3 The Digital Personal Data Protection Act, 2023: Strengths and Gaps

The Digital Personal Data Protection Act (DPDPA), 2023, is a critical milestone in India's efforts to safeguard personal data and ensure robust data governance across sectors, including healthcare. However, certain gaps persist, particularly in the context of healthcare.

Key Provisions of the DPDPA	Strengths of the DPDPA	Limitations of the DPDPA
Clear roles and responsibilities for data fiduciaries and data principals	Enhanced Transparency	Absence of Sector-Specific Provisions
Consent-Based Framework before data collection or processing	Accountability Mechanisms	Ambiguities in Implementation
Right to Data Portability, enhancing consumer autonomy and promoting competition	Simplified Compliance	Overlapping Regulations
Data Localization for sensitive personal data	Consumer Centric Framework	Inadequate Focus on Emerging Technologies

4.4 Global Benchmarks for Health Data Governance: Lessons for India

As India navigates the evolving landscape of digital health and data governance, global benchmarks provide valuable insights and lessons that can inform the development of India's own framework.

United States: Health Insurance Portability and Accountability Act (HIPAA)
- India can benefit from a sector-specific healthcare data protection law like HIPAA to address health data challenges, ensuring data is treated with the required sensitivity while promoting interoperability and security.

Australia's My Health Record System
- India can learn from the centralized nature of My Health Record, developing a national centralized health data repository similar to My Health Record to facilitate integrated healthcare.

European Union: General Data Protection Regulation (GDPR)
- GDPR's principles of data minimization and purpose limitation can guide India's approach to health data collection, processing, and retention; along with its strong enforcement mechanisms and data subject rights.

International Standards: ISO 27799
- Adopting ISO 27799 standards can ensure high-security benchmarks, interoperability, and establish a framework for managing the massive amounts of sensitive health data generated across India's digital health infrastructure.

5). Policy Recommendations

Consolidating Health Data Governance
- Merge Existing Policies into a Unified Framework under the DPDPA
- Introduce a Sector-Specific Health Data Protection Act

Strengthening Privacy and Security Measures
- Mandate Encryption and Anonymization Techniques for Sensitive Health Data through end-to-end encryption
- Introduce Stringent Penalties for Breaches to Deter Negligence

Regulating Emerging Technologies
- Establish Guidelines for Wearable Devices, Health Apps, and Telemedicine Platforms
- Promote Innovation Through Regulatory Sandboxes

Creating a Data Protection Certification Program for Healthcare Providers
- Establish a Data Protection Certification Program for Healthcare Providers
- Provide incentives (e.g., tax breaks, funding for technology upgrades) for healthcare providers that obtain certification

Addressing Cybersecurity Challenges for Health Data Systems
- Create cybersecurity best practices for the healthcare sector through advanced encryption technologies, secure data transfer protocols, and multi-factor authentication systems
- Require organizations to perform annual security audits and penetration testing

Enhancing Interoperability
- Develop Open Standards for Data Exchange Across Platforms
- Learn from the Unified Payments Interface (UPI) to Design Scalable and Interoperable Systems

Strengthening Data Sovereignty and Localization
- Mandate Local Storage of Critical Health Data
- Provide clear guidelines for cross-border data transfers

Bridging the Digital Divide
- Invest in Digital Literacy Programs for Marginalized Populations
- Ensure Affordable Access to Digital Health Services

Authors: Oshia Garg, Maulik Chokshi, Tushar Mokashi
ACCESS Health International, New Delhi, India
Presenting Author: Oshia Garg
oshia.garg@accessh.org