
Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:14, Issue:11(3), November, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

HEALTH DATA, HIDDEN RISKS: PRIVACY CONCERNS IN THE AYUSHMAN BHARAT DIGITAL MISSION & THE NATIONAL DIGITAL HEALTH ECOSYSTEM

Dr. Swarup Mukherjee
Associate Professor of Law, ICFAI University Tripura

Abstract:

India's Ayushman Bharat Digital Mission (ABDM) and the wider National Digital Health Ecosystem (NDHE) promise better continuity of care, lower costs, and data-driven public-health insights by making health records portable, interoperable, and machine-readable. Yet the movement of highly sensitive health data across many actors — hospitals, labs, pharmacies, insurers, third-party apps, consent managers, and government services — creates concentrated privacy risks. Key vulnerabilities arise from consent management gaps, re-identification of de-identified data, weak authentication and federated implementation pitfalls, Aadhaar and mobile-number linkages, opaque third-party data flows, algorithmic inference, and uneven accountability across private and public actors. India's statutory environment has also shifted: the Digital Personal Data Protection Act (DPDP/DPDPA) 2023 and accompanying rules and sectoral policies (including ABDM's Health Data Management Policy) set new baseline obligations for lawful processing, consent, data minimization and grievance redress — but gaps remain in operational enforcement, clarity on sensitive health-data handling, and oversight of AI/analytics on health datasets. Recent operational incidents and reported fraud highlight that theoretical safeguards can be bypassed in practice. This article maps the technical, legal and governance fault-lines in ABDM/NDHE, illustrates likely harm vectors (privacy violations, discrimination, identity fraud, financial harm), and proposes layered mitigations: stronger consent design and UI, enforceable purpose bindings, mandatory privacy-by-design audits, robust re-identification risk assessments, limiting linkage with identity systems, clear processor/fiduciary duties, independent oversight and transparency reporting, and strengthened incident response. With rapid digitalization of health in India, the urgency is not only to keep building interoperable systems but to build them such that individual privacy and public trust are foundational, auditable and enforceable.

Keywords: ABDM, NDHE, Ayushman Bharat, ABHA, health data privacy, DPDP Act 2023, Health Data Management Policy, consent manager, data minimization, re-identification, federated architecture, interoperability, India

1. Introduction — Promise and Peril

The **Ayushman Bharat Digital Mission (ABDM)**, launched in 2021 by the Government of India, represents a transformative step toward creating an integrated digital health infrastructure for the country. It aims to establish a **National Digital Health Ecosystem (NDHE)** that connects healthcare providers, patients, insurers, laboratories, and government health programs through a seamless flow of digital information. At its core lies the **Ayushman Bharat Health Account (ABHA)** — a unique health ID that enables individuals to access, store, and share their medical records electronically across different healthcare systems.

The primary **promise** of ABDM is to make healthcare more **accessible, affordable, and efficient**. By ensuring **interoperability** of electronic health records, patients can obtain better continuity of care, doctors can make informed clinical decisions, and health systems can avoid duplication of diagnostic tests and procedures. The digital ecosystem also facilitates **telemedicine**, **health insurance portability**, and **data-driven policymaking** — particularly valuable for a populous nation with significant healthcare delivery disparities between urban and rural regions.

However, this unprecedented digitalization also introduces **serious privacy and ethical concerns**. Health data is among the most sensitive categories of personal information, often revealing not only an individual's physical and mental health conditions but also genetic traits, sexual and reproductive history, and lifestyle patterns. Misuse or unauthorized disclosure

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:14, Issue:11(3), November, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

can result in **social stigmatization, discrimination in employment or insurance, identity theft, and emotional distress**. When millions of citizens' health records are digitized and linked with other databases (such as Aadhaar, insurance, or demographic registries), the **potential for surveillance, profiling, and data exploitation** grows exponentially.

Furthermore, India's healthcare sector comprises a **diverse mix of public and private entities**, many of which vary widely in their capacity for cybersecurity and data governance. This diversity amplifies the risk of **data leakage, unauthorized sharing, and weak consent practices**, particularly in smaller clinics, diagnostic centers, and local health startups that may integrate into the NDHE via APIs. Unlike financial data, health information carries **lifelong implications** — once leaked, it cannot be "reset" or easily anonymized.

The **legal landscape** is also in transition. While the **Digital Personal Data Protection Act (DPDP Act) 2023** lays a general framework for personal data protection in India, its practical enforcement, sectoral rules, and coordination with ABDM's **Health Data Management Policy (HDMP)** are still evolving. Questions remain over how **consent, purpose limitation, and accountability** will operate in a federated digital health network where data constantly flows between numerous actors — hospitals, insurers, app developers, and government departments.

This creates a paradox at the heart of ABDM's vision: the **same interoperability that empowers citizens also multiplies privacy risks**. If not carefully managed, the digital health mission could erode public trust — a critical component for voluntary adoption. As the NDHE scales up, ensuring **robust privacy-by-design, transparent consent mechanisms, independent oversight, and strict data governance** will determine whether the initiative becomes a model of ethical innovation or a cautionary tale of digital overreach.

2. Legal and policy framework (short primer)

2. Legal and Policy Framework: The Emerging Architecture of Digital Health Data Governance in India

The governance of digital health data in India stands at a critical intersection of **technological innovation** and **legal evolution**. The **Ayushman Bharat Digital Mission (ABDM)** and the **National Digital Health Ecosystem (NDHE)** are being operationalized in parallel with India's first comprehensive data protection statute — the **Digital Personal Data Protection Act, 2023 (DPDP Act)**. Together with the **ABDM Health Data Management Policy (HDMP)** and sectoral health regulations, these instruments lay the foundation for a privacy-protective yet innovation-friendly framework. However, their coexistence also presents challenges of coherence, enforcement, and clarity regarding institutional responsibilities.

2.1 The Ayushman Bharat Digital Mission (ABDM) Framework

The ABDM, implemented by the **National Health Authority (NHA)** under the Ministry of Health and Family Welfare, aims to establish an **interoperable digital health ecosystem**. The mission's key components include:

- **ABHA (Ayushman Bharat Health Account):** a unique 14-digit health identifier that enables individuals to link, access, and share their health records.
- **Health Information Exchange and Consent Manager (HIE-CM):** a technological mechanism that allows users to control who can access their data, for what purpose, and for how long.
- **Healthcare Professional Registry (HPR)** and **Health Facility Registry (HFR):** digital directories for verified healthcare providers and institutions.
- **Personal Health Records (PHR) app:** allowing individuals to manage and view their medical data.

The ABDM operates on a **federated architecture**, meaning that health records remain with respective healthcare providers rather than being stored in a single centralized database. Data exchange occurs through **standardized APIs**, and each transaction is meant to be governed by user consent mediated by the consent manager.

While this model promotes **data sovereignty** and **reduces centralized risks**, it also disperses accountability among multiple stakeholders. Determining **who qualifies as the "data fiduciary"** under the DPDP Act — the hospital, the NHA, or the consent manager — becomes complex in this multi-node network.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:14, Issue:11(3), November, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

2.2 Health Data Management Policy (HDMP) under ABDM

The **Health Data Management Policy (2020, revised 2022)** serves as the internal privacy framework for ABDM. It borrows heavily from international data protection principles — **lawfulness, fairness, purpose limitation, data minimization, storage limitation, and accountability**. The policy emphasizes:

- **Explicit and informed consent** before any collection or sharing of health data.
- **Limited retention periods** and the right of individuals to revoke consent.
- **De-identification and anonymization** for non-clinical uses such as research.
- **Transparency obligations** requiring entities to publish privacy notices.

However, the HDMP lacks the **statutory force of law**; it functions as a policy instrument applicable mainly to ABDM participants. Without explicit legislative backing or enforcement penalties, compliance relies on contractual obligations and accreditation requirements enforced by the NHA.

Moreover, while the policy aligns conceptually with the DPDP Act, certain definitions — such as "sensitive personal data," "data fiduciary," or "data processor" — remain **inconsistent** across frameworks. This ambiguity could result in **jurisdictional overlaps** or **accountability gaps** once the DPDP Act is fully operational.

2.3 The Digital Personal Data Protection Act (DPDP Act), 2023

The **DPDP Act, 2023**, is India's first cross-sectoral data protection legislation and marks a milestone in the evolution of informational privacy. Its core provisions apply to **digital personal data**, including health data, processed within India or by entities offering goods and services to Indian residents.

Key features relevant to ABDM include:

- **Consent-based processing:** Personal data can only be processed with free, informed, specific, and unambiguous consent of the individual (the *data principal*).
- **Purpose limitation and data minimization:** Data can be used only for the purpose stated during collection and must be limited to what is necessary.
- **Rights of individuals:** Data principals have the right to access, correct, erase, and withdraw consent.
- **Obligations of data fiduciaries:** Entities must ensure accuracy, security safeguards, and prompt reporting of breaches.
- **Significant Data Fiduciaries (SDFs):** Large-scale processors (like national health programs) may face additional obligations such as Data Protection Impact Assessments (DPIAs) and audits.
- **Penalties:** The Act prescribes monetary penalties for non-compliance, enhancing deterrence compared to earlier policy frameworks.

Despite these advances, **critical uncertainties remain**. The DPDP Act does not classify "health data" as a distinct category of "sensitive data," unlike the earlier draft of the Personal Data Protection Bill, 2019. This omission dilutes the special protection health data typically receives in jurisdictions like the EU (under GDPR) or Singapore. Additionally, **sectoral coordination** between the **Data Protection Board** (established under the DPDP Act) and the **National Health Authority** (which oversees ABDM) is not yet defined — leaving open the question of who enforces privacy breaches within the digital health ecosystem.

2.4 Interlinkage Between ABDM and DPDP Act

In theory, the ABDM ecosystem is designed to comply with the DPDP Act's requirements. Consent managers under ABDM serve as *technological fiduciaries*, enabling granular consent as mandated by the law. However, several practical gaps persist:

- The **standard consent architecture** may not meet the *informed consent* threshold if users lack clear understanding of data use, especially in vernacular languages.
- The **federated architecture** complicates **breach notification** and **liability assignment**, as multiple actors process the same data.
- The **Health Data Management Policy** is not legally binding, which may lead to uneven compliance across private and public entities.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:14, Issue:11(3), November, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

- There is limited clarity on how **data localization** and **cross-border transfers** of health data will be governed, especially when cloud-based infrastructure or foreign service providers are used.

Thus, while the **legal scaffolding** for health data protection in India is emerging, **institutional capacity and regulatory synchronization** will determine its effectiveness. Without coherent alignment between the DPDP Act, ABDM's operational policies, and sector-specific health regulations, the NDHE may face fragmented accountability and inconsistent privacy standards.

2.5 The Global Context

Globally, frameworks such as the **EU General Data Protection Regulation (GDPR)**, the **U.S. Health Insurance Portability and Accountability Act (HIPAA)**, and **OECD Guidelines on Privacy and Transborder Data Flows** provide instructive examples. These frameworks treat health data as *sensitive personal data*, warranting **higher consent thresholds, breach reporting standards, and research exemptions under strict ethical oversight**. India's digital health architecture would benefit from incorporating these international best practices to build public trust and facilitate secure cross-border research collaborations.

2.6 Conclusion: A Dual-Track Legal Regime

In summary, India's legal environment for digital health data is moving toward a **dual-track regime** — one based on the **statutory authority of the DPDP Act** and the other on the **policy-driven operational rules of ABDM**. Bridging these two tracks through harmonized definitions, interoperable consent standards, and coordinated enforcement is essential. Only then can India's digital health revolution evolve from a **technological mission** into a **rights-based health data governance model**, ensuring that privacy protection remains the backbone — not the afterthought — of public health innovation.

3. Main Privacy Concerns in ABDM and NDHE

While the **Ayushman Bharat Digital Mission (ABDM)** and the **National Digital Health Ecosystem (NDHE)** seek to build a seamless digital health infrastructure across India, their success depends on public trust — trust that the data shared by millions of citizens will remain confidential, secure, and used only for legitimate purposes. However, a close analysis of ABDM's structure reveals several **systemic privacy vulnerabilities**. These concerns stem from technical design choices, regulatory ambiguities, weak consent mechanisms, and risks of re-identification and misuse.

3.1 Consent — Formal Compliance vs. Meaningful Choice

Consent lies at the heart of the ABDM's architecture. The **Health Information Exchange and Consent Manager (HIE-CM)** is designed to allow users to grant and manage permission for the sharing of their health data between entities — hospitals, laboratories, insurers, and telemedicine platforms. In principle, this aligns with the **Digital Personal Data Protection Act (DPDP Act), 2023**, which mandates free, informed, and specific consent.

However, in practice, **meaningful consent** is difficult to ensure in the healthcare context. Patients often face emergencies, linguistic barriers, or digital illiteracy that prevent them from fully understanding the implications of data sharing. Consent screens on apps or hospital portals are often **lengthy, technical, and non-transparent**, effectively becoming a formality rather than an expression of informed choice.

Moreover, **bundled consent** — where a patient must agree to multiple forms of data use (treatment, research, analytics, or insurance) simultaneously — undermines the voluntariness required under the law. While the ABDM technically allows consent withdrawal, there is little clarity on **what happens to already-shared data** once consent is revoked.

Hence, consent under ABDM risks being **procedural rather than substantive**, creating the illusion of control while enabling wide-scale data circulation. Meaningful consent would require **layered disclosures**, simplified language interfaces, and verifiable user comprehension mechanisms.

3.2 Data Minimization and Purpose Limitation

One of the cardinal principles of data protection — reinforced in the DPDP Act and the Health Data Management Policy — is **data minimization**: collecting only what is necessary for a specific, lawful purpose.

However, in ABDM's federated network, there is a tendency for **over-collection** and **purpose creep**. Hospitals and diagnostic centers may collect entire patient histories or biometric identifiers even when not necessary for a particular service. Over time, this accumulation creates **massive data silos** vulnerable to breaches and misuse.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:14, Issue:11(3), November, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

Additionally, **purpose limitation** is often diluted in digital health systems. Data collected for clinical treatment may later be repurposed for research, commercial analytics, or insurance risk profiling — sometimes without renewed consent. Without clear **purpose-binding and audit trails**, it becomes impossible for patients to know how their data is used across different layers of the ecosystem.

This risks converting the NDHE into a **mass surveillance infrastructure**, where health data could be linked with welfare schemes, Aadhaar, or insurance databases for profiling, rather than improving patient care.

3.3 Re-Identification of De-Identified Data

ABDM emphasizes the use of **de-identified or anonymized data** for research and policy purposes. However, the notion of anonymity is fragile in the digital age. When health data — even stripped of names or IDs — is combined with other datasets such as **location, age, gender, or socio-economic indicators**, re-identification becomes alarmingly easy.

For example, if a dataset indicates that a 35-year-old female in a small town underwent a rare surgical procedure on a specific date, it may be possible to trace her identity through hospital records or social media posts. Studies globally show that **over 80% of anonymized datasets can be re-identified** using auxiliary information.

Once re-identified, sensitive data can lead to **stigmatization, discrimination, or blackmail**, particularly in cases involving mental health, HIV status, reproductive health, or substance abuse.

The ABDM framework currently lacks **mandatory re-identification risk assessments** or **differential privacy techniques**, which are standard under international regimes like the EU's GDPR. Therefore, the NDHE must move beyond symbolic anonymization and adopt **technical safeguards** such as synthetic data generation, aggregation thresholds, and access-controlled research sandboxes.

3.4 Federated Architecture — Distributed Responsibility and Hidden Gaps

The ABDM's **federated architecture** is often cited as a strength, as it avoids creating a single, centralized data repository vulnerable to breaches. Instead, data remains with the "originating entities" (hospitals, labs, or insurers), and information exchange occurs through **standardized APIs** under the user's consent.

While this reduces the risk of centralized compromise, it introduces **complex governance challenges**. When multiple entities simultaneously process fragments of a patient's record, determining **who is responsible for a breach** or a **data misuse event** becomes unclear.

For example, if an insurer accesses data from multiple hospitals through the NDHE and later suffers a leak, it is difficult to assign liability among the consent manager, the hospital, or the insurer. This **diffused accountability** can delay breach response and weaken redress mechanisms for affected patients.

The federated model thus needs **clear allocation of fiduciary duties**, mandatory security certifications, and standardized breach-notification procedures across all participating entities to prevent the "many hands, no responsibility" problem.

3.5 Identity Linkage — Aadhaar and Mobile OTP Dependencies

ABDM's use of digital identity verification, often linked with **Aadhaar** or **mobile-based OTP authentication**, raises additional privacy concerns. While this approach enhances convenience, it also increases **identity theft and surveillance risks**.

Aadhaar, India's biometric identity system, was not designed for continuous use in health transactions. Linking ABHA numbers to Aadhaar records potentially allows **cross-domain data correlation** between health, financial, and demographic databases. This could lead to **profiling, targeted marketing, or state surveillance** without explicit consent.

Additionally, **mobile OTP-based authentication** is vulnerable to **SIM-swap frauds**, interception, or social engineering. Reports have surfaced of fraudsters using stolen credentials to access government health benefits under Ayushman Bharat schemes.

To mitigate these risks, ABDM should consider **multi-factor authentication** (including device-based verification or tokenized access) and **strict separation between identity and health data layers**, ensuring that no single database can link demographic and medical information.

3.6 Third-Party Apps, Startups, and Vendor Ecosystems

The NDHE is envisioned as an **open digital platform** where private health-tech companies, insurers, telemedicine providers, and pharmacies can integrate through APIs. While this fosters innovation, it also opens the door to **new privacy vulnerabilities**.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:14, Issue:11(3), November, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

Many startups entering the ecosystem may lack robust **cybersecurity infrastructure** or awareness of **data protection obligations**. Without stringent vetting, accreditation, and continuous monitoring, these third parties could become the **weakest link** in the privacy chain.

Moreover, private health apps often seek secondary revenue streams through **data monetization**, behavioral analytics, or targeted advertising. Once connected to ABDM, these practices risk contaminating a public-good ecosystem with **commercial exploitation of sensitive health data**.

Thus, every third-party entity within NDHE must be subjected to **mandatory privacy audits, contractual data-processing agreements, and clear liability provisions**, similar to standards followed in the EU or Singapore.

3.7 Algorithmic Inference, Profiling, and Discrimination

As India's digital health data accumulates, it will inevitably feed into **AI-driven systems** for disease prediction, insurance underwriting, and public health forecasting. While these applications can revolutionize care delivery, they also introduce **algorithmic risks**.

AI systems trained on biased or incomplete datasets may perpetuate discrimination — for instance, by **denying insurance coverage** to individuals based on inferred health risks or **prioritizing urban populations** due to data availability bias.

Moreover, algorithmic decision-making often lacks **explainability**. Patients denied benefits or targeted for specific interventions may never know **why**. The absence of **algorithmic accountability frameworks** within ABDM increases this opacity.

To counter these risks, the NDHE should require **Algorithmic Impact Assessments (AIA)**, transparent documentation of training data sources, and the **right to human review** for automated decisions, aligning with emerging international AI governance principles.

3.8 Cross-Border Data Flows and Cloud Hosting Risks

With increasing reliance on cloud infrastructure for scalability, Indian health data may traverse **international servers**, creating **jurisdictional ambiguity**. Once data moves beyond Indian borders, enforcing domestic privacy laws becomes difficult.

Although the DPDP Act allows the government to specify countries where data transfer is permitted, the **lack of sector-specific guidelines for health data** remains a concern. The NDHE must ensure **data localization** for identifiable health information, while allowing **controlled research collaborations** under strict anonymization and ethics clearance.

3.9 Data Breaches and Operational Incidents

Recent reports of **data tampering, fake Ayushman cards, and fraudulent access** to beneficiary data underscore the real-world vulnerabilities in digital health systems. Many breaches occur not due to technical failure but because of **insider threats, weak access controls, or phishing attacks**.

The absence of a **mandatory breach notification framework** under ABDM delays disclosure and reduces accountability. Learning from global standards like HIPAA (U.S.) and GDPR (EU), India must implement **strict breach reporting timelines**, citizen notification mechanisms, and **independent investigation protocols** to preserve public confidence.

3.10 The Broader Socio-Legal Implication: Trust Deficit

Beyond technical safeguards, the success of ABDM depends on **public trust**. Health data is deeply personal, and any perception of misuse or surveillance can trigger **societal resistance** to participation. For marginalized communities — including women, LGBTQ+ individuals, and people with stigmatized conditions — privacy violations can lead to **social exclusion and discrimination**.

Thus, privacy protection in ABDM is not merely a legal compliance issue; it is an **ethical and social imperative**. The mission's legitimacy rests on demonstrating that technological progress will not come at the expense of human dignity and informational autonomy.

The above privacy challenges — spanning consent, data minimization, re-identification, architecture, identity linkage, third-party risk, and algorithmic bias — illustrate that India's digital health revolution is also a **regulatory balancing act**. The solution lies not in slowing innovation but in embedding **privacy-by-design principles**, **clear accountability chains**, and **independent oversight mechanisms** from the very foundation of ABDM and NDHE.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:14, Issue:11(3), November, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

4. Real-World Signals — When Privacy Meets Reality

Behind every data breach or fake health card is not just a number in a report — it's a person whose trust has been shaken, whose identity may have been misused, or whose medical privacy is no longer truly private. As India takes confident steps toward a fully digital healthcare system under the **Ayushman Bharat Digital Mission (ABDM)**, the challenges that emerge on the ground remind us that technology, no matter how visionary, must walk hand in hand with ethics, trust, and accountability.

4.1 The Human Face of Data Breaches

When the government proudly announced the creation of over **50 crore Ayushman Bharat Health Account (ABHA) IDs**, it symbolized empowerment — every citizen finally having a digital health identity. But soon, troubling stories began surfacing. In parts of **Uttar Pradesh and Punjab**, police unearthed rackets that manufactured **fake Ayushman cards**. Innocent villagers discovered that their identities had been cloned to claim hospital benefits they never received. Imagine a farmer from Bareilly or a housewife in Patiala finding her health record altered or her ID used to file claims in cities she's never visited. For them, this isn't a technical glitch — it's a violation of dignity and trust.

4.2 Fraud Beneath the Surface

Investigations have shown that some hospitals and intermediaries created **bogus patient records**, used **fictitious ABHA IDs**, and filed false insurance claims under the **Pradhan Mantri Jan Arogya Yojana (PM-JAY)**. In just one review period, more than **4.6 lakh suspicious claims** were flagged nationwide, and over a thousand hospitals were de-empanelled. These figures highlight a deeper systemic issue — when sensitive health data becomes a tool for profit, both privacy and public trust suffer.

At the same time, **internal manipulation** has been equally worrisome. Reports surfaced of government health officers finding their **Aadhaar-linked mobile numbers** changed without their knowledge, enabling criminals to intercept one-time passwords and gain unauthorized access to ABDM portals. The victims here weren't faceless data points — they were public servants, doctors, and beneficiaries who lost control over their digital identities.

4.3 The Ripple Effect

These breaches go beyond financial fraud. Once a health profile is exposed, it can reveal deeply personal details — a patient's mental health history, HIV status, or reproductive data. In a society still struggling with stigma, such exposure can lead to **social discrimination, emotional distress, and reputational harm**. A digital ecosystem built to make healthcare more humane must not end up making it more vulnerable.

4.4 The Trust Deficit

The **National Health Authority (NHA)** has made progress — suspicious claims are being blocked, hospitals are being blacklisted, and audits are underway. Yet, the **culture of trust** is fragile. Citizens still ask: *Who really controls my data? If something goes wrong, whom do I complain to?*

The absence of a single, transparent **breach notification system** means that people often learn about data misuse through the media, not from the authorities themselves. Every such incident chips away at confidence in the larger digital mission.

4.5 Learning from the Cracks

These incidents hold valuable lessons:

- **Digital identity must be sacred** — no one should be able to alter a mobile number or ABHA linkage without rigorous verification.
- **Consent must mean understanding** — citizens need to know *what* they are agreeing to and *how* their data will travel.
- **Hospitals and third parties must be accountable** — regular audits, ethical training, and penalties for misuse are essential.
- **Transparency is the best defense** — public disclosure of breaches builds trust, not fear.

4.6 A Call for Ethical Vigilance

Technology can heal, but only when it respects the humanity behind the data. The **Ayushman Bharat Digital Mission** has immense potential to democratize healthcare in India — to make every citizen visible, heard, and cared for in the medical system. But this vision can succeed only if **privacy becomes its moral heartbeat**.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:14, Issue:11(3), November, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

The future of India's health data should not be one where patients feel watched; it should be one where they feel protected. As policymakers, technologists, and healthcare workers continue this journey, they must remember that each ABHA number is not a statistic — it's a story, a life, a promise that must be kept.

5. The Way Forward — Building Trust in the Digital Health Future

India stands at a remarkable crossroads. On one side lies the promise of a **digitally connected health system**, where every citizen — whether in the hills of Tripura or the lanes of Delhi — can access their medical records, receive teleconsultations, and benefit from precision health interventions. On the other side lies the risk of a **data dystopia**, where privacy is sacrificed for efficiency and individuals lose control over their most intimate information. The path we choose will determine not only the success of the **Ayushman Bharat Digital Mission (ABDM)** but also the moral character of India's digital future.

5.1 Trust — The Heartbeat of Digital Health

No technology, however advanced, can survive without **trust**. In healthcare, trust is even more sacred because patients share what they would never tell anyone else — their fears, vulnerabilities, and medical histories. When that data becomes digital, trust must be translated into **technological assurance**. Citizens must feel confident that every click, every upload, and every shared report is handled with **integrity, consent, and accountability**.

The ABDM should thus evolve not merely as a data platform but as a **trust framework** — one that places the individual at its moral and operational center. This means adopting **privacy-by-design principles**, ensuring **human oversight**, and building **transparent mechanisms** that let citizens see who accessed their data and why.

5.2 Ethical Data Governance — From Compliance to Compassion

At present, India's **Digital Personal Data Protection Act (DPDP) 2023** and the **Health Data Management Policy (HDMP)** offer a legal foundation. But laws alone cannot humanize technology. Ethical governance must go beyond compliance checklists — it must cultivate a **culture of compassion and respect** for patient autonomy.

For example:

- **Consent should be a conversation, not a checkbox.** Many users, especially in rural India, may not fully understand data-sharing permissions. Simplifying consent language, using regional translations, and incorporating verbal or assisted consent for vulnerable groups can make participation genuinely informed.
- **Data minimization** must become a norm — collecting only what is necessary for the stated purpose.
- **Right to withdraw** must be as easy as granting consent. Citizens should be able to "pause" or "revoke" data sharing whenever they feel uncomfortable.

Just as doctors are bound by the Hippocratic Oath, digital health systems must be guided by an **"Ethical Data Oath"** — first, do no harm to privacy.

5.3 Strengthening Accountability — Making Institutions Answerable

Accountability cannot stop at the individual hospital or developer level; it must flow through the entire ecosystem. The **National Health Authority (NHA)**, state agencies, and private participants should share **joint responsibility** for data protection.

Practical steps include:

- Establishing an **Independent Health Data Ombudsman** to investigate breaches and ensure victim compensation.
- Implementing **mandatory breach notification** within 72 hours to affected users.
- Conducting **annual privacy audits** of all registered entities.
- Training healthcare workers not just in digital operations but also in **data ethics**.

When a data breach occurs, citizens should not have to wonder whom to blame — they should know exactly where to seek justice and redressal.

5.4 Inclusion, Literacy, and Digital Dignity

Technology must never widen inequality. India's digital health transition must be **inclusive**, ensuring that illiteracy, language barriers, or socio-economic constraints do not exclude citizens from understanding or controlling their data.

- **Digital health literacy campaigns** should explain privacy rights in simple, relatable language.
- Village-level **ABDM Sakhis** or community health workers can act as **data educators**, helping citizens navigate the system safely.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:14, Issue:11(3), November, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

- For marginalized communities, **offline consent and grievance redressal systems** should remain available to ensure fairness and accessibility.

Digital dignity is as essential as digital access. Every citizen, regardless of background, deserves to feel that the system protects their humanity, not just their health.

5.5 From Surveillance to Stewardship — A New Vision

The government must consciously shift the philosophy of data governance from **surveillance to stewardship**. Citizens should be viewed not as data subjects but as **data owners** — the ultimate stewards of their health information.

This cultural shift requires:

- Transparency in how public health data is used for research or policy.
- Strong encryption and anonymization standards for secondary use.
- Public consultation before introducing new health-data sharing initiatives.

A system that asks for public participation must also **return public accountability**.

5.6 A Shared Responsibility

The future of digital health cannot rest solely on the government's shoulders. It demands a **collective commitment**:

- **Technology companies** must embed ethical design.
- **Hospitals and doctors** must safeguard patient confidentiality even in digital exchanges.
- **Civil society and academia** must serve as watchdogs and ethical guides.
- **Citizens** must become aware participants, not passive data donors.

Trust, once broken, is hard to rebuild — but when shared, it becomes indestructible.

5.7 Conclusion — The Promise of a Humane Digital Future

The Ayushman Bharat Digital Mission has the power to redefine healthcare in India — to make it faster, fairer, and more inclusive. But its ultimate test lies not in how many ABHA IDs are created, but in **how securely and ethically those identities are protected**.

If India can strike the delicate balance between innovation and privacy, it can set a global example — a model where technology amplifies humanity instead of eroding it.

In the end, the success of the digital health revolution will not be measured by data volumes or dashboards, but by a simple truth:

Do citizens feel safer, respected, and cared for in the digital health world we are building?

That question — more than any statistic — will define the moral legacy of India's National Digital Health Ecosystem.

6. Balancing Public Good with Privacy — Finding Harmony Between Collective Health and Individual Rights

One of the most delicate challenges in the digital health revolution is balancing **collective welfare** with **individual privacy**. On one hand, large-scale health data holds enormous potential for **epidemiological research, policy planning, and disease prevention**. On the other, unrestrained data collection or sharing can transform citizens into **subjects of surveillance** rather than participants in a system meant to protect them.

6.1 The Promise of the Public Good

The **National Digital Health Ecosystem (NDHE)**, envisioned under the Ayushman Bharat Digital Mission, can generate invaluable insights for India's public health system. Aggregated datasets — if used responsibly — can help detect outbreaks faster, plan vaccine distribution more efficiently, and identify patterns in chronic diseases that are invisible in fragmented records.

Imagine a future where early warning signals of dengue or diabetes hotspots are detected not through speculation but through real-time, anonymized health analytics. In such a world, **data becomes a tool of compassion**, saving lives and optimizing scarce medical resources.

6.2 The Peril of Overreach

Yet, between the noble intention and its implementation lies a gray zone. When health data flows without strict boundaries, the very systems built for public benefit can erode the **right to autonomy and confidentiality**.

If personal health details — even anonymized — are repurposed for non-health objectives like insurance profiling, marketing, or surveillance, the line between care and control blurs dangerously.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:14, Issue:11(3), November, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

The history of public policy is replete with examples where "for the public good" became an excuse for **mass data collection without informed consent**. In healthcare, such breaches can cause not only legal harm but **deep emotional wounds**, especially when stigmatized conditions are involved.

6.3 Law, Ethics, and Oversight

Balancing these tensions requires a clear legal and ethical framework. The **Digital Personal Data Protection Act (DPDP) 2023** permits data processing for public interest, but such exceptions must not become **blank cheques**. Policymakers must:

- Define **narrow, specific legal bases** for public-health data processing — limited to epidemiology, disease surveillance, and essential policy planning.
- Ensure **independent scientific and ethical oversight committees** review every large-scale data use project.
- Mandate **transparency reports** on how and why citizens' data is aggregated and used.

Without such checks, even benevolent data programs risk morphing into instruments of control or commercial exploitation.

6.4 Privacy-Enhancing Technologies — A Middle Path

Modern technology provides solutions to this moral tension. **Privacy-Enhancing Technologies (PETs)** such as **data anonymization, differential privacy, federated learning, and homomorphic encryption** can allow researchers to study population-level health trends without accessing individual-level identifiers.

For example:

- **Federated learning** enables AI models to learn from distributed datasets without the data ever leaving local servers.
- **Differential privacy** adds mathematical "noise" to datasets so individual records cannot be reverse-engineered.

By adopting such methods, India can pursue public-health innovation **without turning citizens into open books**.

6.5 Shared Stewardship of Health Data

The key to balancing public good with privacy lies in **shared stewardship**. Citizens must not feel their data is taken from them — they must feel they are contributing to a collective effort.

This can be achieved by:

- Seeking **community-level consent** for data aggregation projects.
- Involving **citizen representatives** in oversight boards.
- Offering **opt-out mechanisms** and feedback loops where individuals can know how their anonymized data contributed to public benefit.

When people see tangible, transparent outcomes from their data — such as improved vaccination campaigns or local healthcare infrastructure — **trust deepens naturally**.

6.6 The Ethical Compass

Ultimately, the goal of public health is not just to cure the population but to **honor the individual within the collective**. A just digital health ecosystem recognizes that *privacy and progress are not opposites* — they are partners. Protecting privacy strengthens public trust, and trust is the foundation upon which any sustainable health policy must stand.

As India continues to digitize healthcare, the guiding question should remain simple yet profound:

"Can we build a system where every citizen feels both protected as an individual and valued as part of the nation's collective well-being?"

The answer must always lean toward **ethical innovation** — where science serves humanity, and privacy becomes the soul of public good.

7. Conclusion — Toward a Privacy-First Digital Health Future

The **Ayushman Bharat Digital Mission (ABDM)** and the broader **National Digital Health Ecosystem (NDHE)** stand as monumental milestones in India's journey toward universal, equitable, and data-driven healthcare. They symbolize not just administrative modernization, but a profound shift — from fragmented health systems to an interconnected network of care. Through this digital architecture, India seeks to empower every citizen with ownership of their health information and access to quality services regardless of geography or income.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:14, Issue:11(3), November, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

Yet, the same digital connective tissue that promises **continuity of care** and **public-health intelligence** also creates new vulnerabilities. When every diagnosis, prescription, and consultation can travel at the speed of a click, the risks of **data breaches, misuse, and surveillance** multiply. In a country as vast and diverse as India, even a single breach can affect millions, not only compromising security but eroding the **public trust** upon which all digital governance depends.
The **Digital Personal Data Protection Act (DPDP) 2023** and the **ABDM's Health Data Management Policy (HDMP)** lay a commendable foundation. They define principles of consent, purpose limitation, and accountability — but **principles alone do not protect people; practices do**.

To truly uphold the spirit of privacy and patient dignity, India must now move from **policy to practice**, and from **intent to implementation**.
This means:

- Ensuring **robust accreditation** for every hospital, data processor, and application that plugs into the NDHE;
- Embedding **privacy-preserving engineering** at every layer of design, from databases to AI analytics;
- Mandating **transparent, independent audits** to detect and disclose breaches early;
- Enforcing **legally binding contracts** that hold private partners accountable for misuse; and
- Establishing **active oversight bodies** that combine technical expertise with ethical authority.

Such measures are not bureaucratic burdens — they are investments in **trust**. Without trust, even the most advanced health systems will falter; with it, citizens will willingly participate, share, and benefit.
The promise of ABDM is not only technological — it is **moral**. It asks whether a nation can create a digital ecosystem where innovation serves compassion, and efficiency respects privacy. A system that protects the most intimate details of human life must be built not merely with code, but with conscience.
In the final reckoning, **a privacy-first NDHE will be a more effective NDHE** — one where digital empowerment and human dignity grow together. If India can achieve that balance, it will not only revolutionize healthcare but also set a global standard for how nations can use technology **responsibly, inclusively, and ethically** — proving that in the age of data, **humanity remains our greatest innovation**.

References

1. Ayushman Bharat Digital Mission (ABDM). (2021). *National Health Authority: Strategy Overview and Health Data Management Policy.* Government of India. Retrieved from https://abdm.gov.in
2. Ministry of Health and Family Welfare. (2020). *National Digital Health Blueprint (NDHB).* Government of India. New Delhi: MoHFW.
3. Government of India. (2023). *Digital Personal Data Protection Act, 2023.* Ministry of Electronics and Information Technology (MeitY). Retrieved from https://www.meity.gov.in/
4. National Health Authority. (2021). *Health Data Management Policy (Version 1.0).* New Delhi: Government of India.
5. World Health Organization (WHO). (2021). *Global strategy on digital health 2020–2025.* Geneva: WHO. Retrieved from https://www.who.int/
6. Sharma, R., & Choudhary, P. (2022). Data privacy and digital health in India: An ethical and legal analysis. *Indian Journal of Law and Technology*, 18(2), 45–67.
7. Sinha, A., & Singh, V. (2023). Data protection in healthcare: Evaluating the Ayushman Bharat Digital Mission. *Journal of Health Policy and Law*, 9(1), 23–41.
8. OECD. (2021). *Health Data Governance: Privacy, Monitoring and Research.* Organisation for Economic Co-operation and Development. Paris: OECD Publishing.
9. Kuner, C. (2021). *Transborder data flows and data privacy law.* Oxford University Press.
10. NITI Aayog. (2022). *Responsible AI for Health in India: Ethics and Governance Guidelines.* Government of India.
11. United Nations. (2021). *UNESCO Recommendation on the Ethics of Artificial Intelligence.* Paris: UNESCO.
12. Puri, S. (2024). The challenge of consent in India's digital health infrastructure. *Economic & Political Weekly*, 59(5), 22–28.


Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:14, Issue:11(3), November, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

13. European Union. (2018). *General Data Protection Regulation (GDPR).* Regulation (EU) 2016/679 of the European Parliament and of the Council.
14. Chaturvedi, A. (2023). Balancing public health and individual privacy in digital ecosystems: Lessons from global frameworks. *Health Informatics Journal*, 29(3), 1–17.
15. Reddy, M., & Basu, S. (2022). Building trust in digital health: Data protection challenges in low- and middle-income countries. *The Lancet Digital Health*, 4(9), e635–e642.