VOLUME 7 | ISSUE 1

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

A CRITICAL ANALYSIS ON THE LEGAL FRAMEWORK GOVERNING HEALTHCARE DATA UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

- Muthu Kumar K[1] & Harish Karthick M[2]

ABSTRACT

The rapid change to digital deployment in India's healthcare sector has changed the way how healthcare services are provided. This includes telemedicine, electronic health records, health apps, digital health care platforms, and online consultations. Although these technological advances in this field have made it easier and more efficient to deliver healthcare, they have also created important concerns about how the personal health data is collected, processed, stored, and shared. Health data is very sensitive and also require a strong legal framework to protect the privacy, confidentiality, and to prevent misuse of such data. The Digital Personal Data Protection Act, 2023 is a crucial step towards establishing a solid legal structure for managing the personal data in India.

However, implementing this Act in the healthcare sector creates several legal and regulatory challenges. This paper will also examine the legal framework that governs the healthcare data under the Digital Personal Data Protection Act, 2023. It will also check whether the current rules are sufficient to protect patient's personal data in the fast-changing digital healthcare industry. When we look into the current healthcare situation, we can see that digital health projects like the Ayushman Bharat Digital Mission, electronic health records, telemedicine platforms, and AI-based healthcare services rely heavily on processing large amounts of personal health data.

Although the Act provides rules for protecting personal data, there are still many issues in the healthcare sector. These include obtaining patient consent, sharing health data securely, protecting it from cyberattacks, sending health data outside India, and ensuring that hospitals

[1]Research Scholar – Ph.D. in Law, Lamrin Tech Skills University, Punjab
[2]Research Scholar – Ph.D. in Law, Lamrin Tech Skills University, Punjab

© 2026 International Journal of Advanced Legal Research

and healthcare providers protect patients' information properly. This research paper will also discuss the responsibilities of hospitals, healthcare professionals, digital health platforms, and other stakeholders in adhering to the Digital Personal Data Protection Act, 2023.

Also, the paper suggests that managing the healthcare data in India needs a regulatory approach that focuses on the sector itself. This includes the factors such as improving patient consent mechanisms, enhancing cybersecurity standards, ensuring more transparency in data processing practices, and creating effective oversight mechanisms to protect sensitive healthcare data. These actions would help balance technological progress with the right to privacy and strengthen public trust in India's digital healthcare system.

KEYWORDS: *Digital Personal Data Protection Act, 2023, Healthcare Data Governance, Patient Privacy, Digital Health, Data Protection.*

I. INTRODUCTION

India finally got data privacy law. After more than two years and 5 attempts of drafting, Parliament passed the Digital Personal Data Protection Bill and it was approved then got president signature on August 11, 2023[3]. It wasn't easy. but it's now the law which enshrined In K.S. Puttaswamy v. Union of India,[4] the Supreme Court declared that privacy is a fundamental right of every Indian citizen. This Act turns that court ruling into an actual working law. This is India's first law specifically built to protect people's personal data online.

There is a dedicated legal structure that tells everyone, individuals and organizations have their rights and responsibilities are when it comes to data. It covers only digital personal data. The Data Protection Board of India is the central authority set up to handle complaints and violations. Once it comes into full effect, it will override Section 43A of the IT Act 2000 and the IT (Sensitive Personal Data) Rules 2011[5].

[3]Subhajit Saha, Surjashis Mukhopadhyay, a new age of data privacy laws in india: review of digital personal data protection act, 2023,International Journal of Law and Social Sciences (IJLS) Volume 10, Issue 1, 2024 Print ISSN: 2454-8553, Online ISSN: 2583-8644

[4]Justice K.S.Puttaswamy(Retd) And Anr. vs Union Of India And Ors. on 24 August, 2017, https://indiankanoon.org/doc/91938676/

[5]Saha, supra note 1

© 2026 International Journal of Advanced Legal Research

The DPDP Act 2023 is a general law but this paper ecifically deals with health care data. Healthcare is not general and that gap creates real problems. India's healthcare system has gone heavily digital. Programmes like Ayushman Bharat Digital Mission, electronic health records, telemedicine, and AI-driven medical tools all run on large volumes of personal health data. That data is sensitive, and the risks of mishandling it are serious.

Does the DPDP Act 2023 actually protect patients in India's fast-changing digital healthcare environment or does it fall short. The key problem areas this paper looks at Consent of patients genuinely informed before their health data is collected and used or not. When hospitals, labs, and platforms exchange patient data, is it done securely and whether the Act deals with it.

Healthcare systems are frequent targets so the current protections are strong enough to protect the privacy of health care data and whether the Act gives a specific rules regarding that. The hospitals, doctors, and digital health platforms clear on what the law requires of them and the how law requires them to implement it and what is the punishment it provided when such stakeholders didn't comply with the law.

II. BACKGROUND OF THE STUDY

Part III of Indian Constitution lists the fundamental rights. It is called the Magna Carta of the Constitution. Privacy is not written into Part III. In Justice K.S. Puttaswamy v. Union of India (2017), a bench of nine judges ruled that the right to privacy is a constitutional right not a privilege, not a policy choice. They traced it through several fundamental rights, most importantly Article 21, which guarantees every person the right to life and personal liberty.

Privacy has evolved from an older understanding of personal seclusion and transformed into a modern constitutional and informational right. In India, the Supreme Court first discussed privacy in cases such as Kharak Singh and later in Gobind, and the position was decisively settled in Justice K.S. Puttaswamy v. Union of India, where privacy was held to be a fundamental right under Articles 14, 19, and 21 of the Constitution[6]. That modern understanding is important because it moves privacy beyond physical space and treats control over our health.

[6]Justice K.S.Puttaswamy(Retd), supra note 2

© 2026 International Journal of Advanced Legal Research

Health care data deals with highly sensitive privacy information, including diagnosis, treatment history, test results, and digital health identifiers. The Government of India's Ayushman Bharat Digital Mission framework expressly relies on Security and Privacy by Design and the Health Data Management Policy states that it sets minimum standards for privacy protection across the ABDM ecosystem [7].The ABDM say that data sharing is meant to occur through consent based and federated architecture, rather than a centralized repository, which makes healthcare data governance a distinct legal issue[8].

The DPDP Act, 2023 is now the central general statute governing digital personal data in India. It lawful processing, consent based use, security safeguards, notice, rights of the data principal, and certain permitted processing in public interest or emergency-type contexts. For healthcare, the Act is important and creates the general baseline, but it does not give sector specific detail that health data governance often requires.

India has older and parallel legal rules that affect digital and medical information. The IT Act, 2000 contains provisions on compensation for failure to protect data and punishment for breach of confidentiality and privacy, including Sections 43A, 72, and 72A[9]. These provisions deals with healthcare institutions and digital health platforms handle electronic records and sensitive privacy information, so the IT Act remains relevant even after the DPDP Act. Healthcare data protection in India has developed through layered laws rather than a single code.

There is also a strong need for a clearer legal framework for healthcare data collection and use. Indian legal system now recognizes privacy as a constitutional right, while digital health systems such as ABDM rely on consent, security, and controlled sharing . The existence of multiple overlapping regimes like constitutional privacy, DPDP Act, the IT Act, and ABDM policy shows why healthcare data needs more precise rules on collection, storage, sharing, retention, and accountability .

[7]Health Data Management Policy Of Ayushman Bharat Digital Mission (ABDM), https://www.india.gov.in/category/health-wellness/subcategory/health-care-promotion-products/details/health-datamanagement-policy-of-ayushman-bharat-digital-mission-abdm?utm_source=perplexity, (last visited Aug 3,2026)

[8]Ministry of Health and Family Welfare, National Digital Health Ecosystem, Union Health Ministry has adopted a holistic approach to safeguard the IT system from critical security threats across computational layers https://www.pib.gov.in/PressReleasePage.aspx?PRID=1942715&utm_source=perplexity&reg=48&lang=2, (last visited Aug 3,2026)

[9]Information Technology Act, 2000, (21 of 2000) Section 42, 72.

© 2026 International Journal of Advanced Legal Research

This is especially important because healthcare data is not just ordinary personal data. It affect bodily integrity, treatment access, insurance, and future discrimination risks. This leads a space for the critical analysis of the provisions enshrined in the DPDP Act 2023. But the notification No G.S.R 843(E) The Ministry of Electronics and Information Technology officially notified on November 13, 2025 that the DPDP Act 2023 will not come into full force all at once. Instead, different parts of the law will activate on three separate dates.

- Immediately from November 13, 2025: Sections 18 to 26, which set up the Data Protection Board of India, came into force on the day this notification was published. Along with these, several administrative and penalty related provisions under Sections 35, 38 to 43, and sub-sections (1) and (3) of Section 44 also came into effect. The definitions clause under Section 2 was also activated.
- One year later by November 13, 2026: Sub-section (9) of Section 6 on consent management and clause (d) of sub-section (1) of Section 27 relating to the Board's functions will come into force.
- Eighteen months later by May 13, 2027: The core obligations of the Act kick in which includes Sections 3 to 5-scope and applicability of the Act, Sub-sections (1) to (8) and (10) of Section 6-rules around valid consent, Sections 7 to 17-rights of individuals and duties of data fiduciaries, Sections 28 to 34 and 36 to 37-functions and powers of the Data Protection Board, Sub-section (2) of Section 44-remaining transitional provisions[10].

Exercise of powers conferred by sub-sections (1) and (2) of section 40 of the Digital Personal Data Protection Act, the Central Government notified in GSR 846 E which contains 23 rules followed by seven detailed Schedules that provide specific standards, exemptions, and operational guidelines. These are the current ecosystem regarding the health care data.

III. KEY PROVISIONS DEALS WITH HEALTH CARE DATA

Section 7 of the Digital Personal Data Protection Act, 2023 and Rule 12, 4th schedule of the DPDP Rules, 2025 are the primary provisions that directly deal with healthcare, medical emergencies, and health data.

[10]MEITY [F. No. AA-11038/1/2025-CL&ES] New Delhi, the 13th November, 2025

© 2026 International Journal of Advanced Legal Research

1. Medical Emergencies and Public Health Crises (Section 7)[11]

Section 7 of the Act outlines certain legitimate uses where a Data Fiduciary can process an individual's personal data without requiring their explicit, formal consent.

- Section 7(f) - Individual Medical Emergencies: A Data Fiduciary may process personal data for the purpose of responding to a medicak emergency that involves a threat to the life or an immediate threat to the health of the Data Principal (the individual) or any other person
- Section 7(g) - Public Health Threats: Personal data can be processed to take measures to provide medical treatment or health services to individuals during an epidemic, an outbreak of a disease, or any other major threat to public health.

This ensures that in life-or-death situations, or during wide- scale events like a pandemic, healthcare providers, the State, or emergency responders do not face legal bottlenecks regarding data consent.

2. Consent and Purpose Limitation in Healthcare Apps

Section 6[12] generally covers the requirements for valid consent, the Act explicitly uses a healthcare example to explain purpose limitation. The principle or company can only collect data necessary for the specific service provided.

If an individual downloads a telemedicine app and is asked to consent to both processing their personal data for telemedicine services and accessing their mobile phone contact list the consent for the contact list is invalid. Because the phone contact list is not necessary for providing telemedicine services, the consent is strictly limited to the data actually needed for the medical consultation.

Section 7 uses an illustration of a customer voluntarily giving their personal data to a pharmacy to receive a payment receipt via mobile message. The pharmacy is permitted to process this data specifically for sending the receipt.

[11]Digital Personal Data Protection Act, 2023(No.22 of 2023) Section 7
[12]Digital Personal Data Protection Act, 2023(No.22 of 2023) Section 6

© 2026 International Journal of Advanced Legal Research

3. Processing Children's Healthcare Data (Rule 12 & Fourth Schedule, Part A)

Section 9 of the Act strictly requires verifiable parental consent before processing any personal data of a child (under 18) and completely bans tracking or behavioural monitoring of children. However, Rule 12 of the DPDP Rules 2025 provides crucial exemptions specifically for healthcare entities to ensure children can receive necessary medical care without administrative friction.

Under Part A of the Fourth Schedule, parental obligations do not apply to Clinical Establishments, Mental Health Establishments, and Healthcare Professionals. They are exempt from the strict parental consent and tracking bans, provided that the data processing is strictly restricted to providing health services to the child, to the extent necessary to protect the child's health.

Allied Healthcare Professionals are similarly exempt, provided the data processing is strictly restricted to supporting the implementation of a healthcare treatment or a referral plan recommended for the child's health protection.

These providers do not need to obtain verifiable parental consent or adhere to tracking behavioural monitoring restrictions under Section 9(1) and 9(3) of the Act

4. Health Data of Persons with Disabilities (Rule 11)

For individuals with physical, mental, intellectual, or sensory impairments who are unable to take legally binding decisions such as those with severe autism, cerebral palsy, or mental retardation, the Act requires obtaining verifiable consent from their lawful guardian. Data Fiduciary must observe due diligence to verify the person granting consent on behalf of the patient is a lawful guardian appointed by court of law, designated authority, local level committee as per the Rights of Persons with Disabilities Act, 2016, or the National Trust Act, 1999.

IV. APPLICATION AND ADEQUACY OF HEALTHCARE DATA UNDER THE DPDP ACT

1. Who are all Stakeholders in DPDP Act

The DPDP Act 2023 applies to every entity that collects, processes, or uses the digital personal data of Indian citizens. In healthcare, this covers a hospitals, clinics, individual

© 2026 International Journal of Advanced Legal Research

doctors, health insurers, diagnostic laboratories, HealthTech startups, and research institutions.[13]

- Patients are classified as Data Principals, meaning the individuals to whom the data belongs.
- Healthcare providers and institutions are classified as Data Fiduciaries, meaning they decide why and how patient data is processed.
- Entities that handle especially large volumes of sensitive patient data, additionally classified by the government as Significant Data Fiduciaries[14]

This classification brings extra obligations including appointing a dedicated Data Protection Officer[15] and conducting periodic audits. Third party service providers such as cloud storage companies or electronic health record software vendors are classified as Data Processors, operating under the instructions of the fiduciary.

2. How the Act Governs Consent, Data Use, and Patient Rights

The Act establishes several core principles that directly shape how healthcare data must be handled. Consent sits at the centre of the entire framework. Before any patient data is collected or processed, the healthcare provider must obtain consent that is free, specific, informed, and unconditional, accompanied by a notice written in plain language.

For mental healthcare professionals (M-HCP) they must obtain clinical consent in Mental health care Act, 2017 for treatment at the same time as navigating the Act's legal consent requirements for data processing[16]. Doing both simultaneously in an early stage, where a patient is already anxious and trust is still being established, risks damaging the therapeutic relationship before it begins. The Act does recognise the explicit consent is not always possible.

[13]Vasudha Khanna and Atul Kotwal,Examining the significance of the digital personal data protection act, 2023 in the context of the healthcare industry: a comprehensive analysis Discover Public Health 2025 (https://doi.org/10.1186/s12982-025-00757-6)

[14]Manik Inder Singh Sethi et al. The Digital Personal Data Protection Act 2023: Implications for Mental Healthcare Practice in India, Indian Journal of Psychological Medicine | Volume XX | Issue X | XXXX-XXXX 2025Website: journals.sagepub.com/home/szj DOI: 10.1177/02537176251370651 2025)

[15]Khanna, supra note 11

[16]Seith, supra note 12

© 2026 International Journal of Advanced Legal Research

It permits data processing without consent in genuine medical emergencies involving a threat to life, and during public health crises such as disease outbreaks or epidemics[17]. Where children are involved, the Act generally requires verifiable parental consent before their data is processed[18]. The 2025 Rules carve out an important exception here clinical establishments and healthcare professionals may process a child's data without strict parental consent if it is strictly necessary to provide health services and protect the child's wellbeing.

Beyond consent, the Act requires healthcare entities to practice data minimisation collecting only what is necessary for the specific service being provided and to delete data once that purpose has been fulfilled.

Any personal data breach must be reported immediately to both the Data Protection Board of India and the affected patients. The Act also introduces Consent Managers2(g), which are registered platforms that serve as a single point of contact, allowing patients to give, manage, review, and withdraw their consent across different hospitals and health applications in an interoperable way.

3. Where Implementation Breaks Down in the Real Healthcare Environment

India's healthcare sector is currently undergoing rapid and large-scale digitisation, driven by initiatives like the Ayushman Bharat Digital Mission and the Integrated Health Information Platform. Implementing the DPDP Act within this fast moving environment exposes serious practical difficulties.[19]

Indian doctors routinely share patient scans, reports, and clinical information over WhatsApp or email to get quick expert opinions, coordinate emergency referrals, and run multidisciplinary case discussions which is not negligence. It is how clinical collaboration actually works in India's healthcare system. But under the strict requirements of the DPDP Act, this routine practice may now constitute a data protection violation carrying severe financial penalties, leaving clinicians caught between providing timely care and protecting themselves legally[20].

[17]Shruti Singh, et al, Addressing Bias, Privacy, Security, and Patient Autonomy in Artificial Intelligence (AI)-Driven Healthcare: A Review of Current Guidelines Cureus 18(2): e103999. DOI 10.7759/cureus.103999).
[18]Digital Personal Data Protection act, 2023(No. 22 of 2023 section 9).
[19]Khanna, supra note 11
[20]Anubhuti Sood, Deepika Mishra, Challenges and recommendations for enhancing digital data protection in Indian Medical Research and Healthcare Sector https://doi.org/10.1038/s41746-025-01448-x, 2025)

© 2026 International Journal of Advanced Legal Research

The compliance burden also falls unevenly. Large hospitals with dedicated legal and technology teams can absorb the cost of encryption software, staff training, audit log systems, and vendor agreements. Solo practitioners, small clinics, and rural health facilities cannot. For them, the Act's requirements represent a financial and administrative load that bears no relationship to their actual capacity[21].

On AI front, Indian health startups frequently collaborate with hospitals to train AI models on patient data. While the Act exempts genuinely anonymised data, true anonymisation is technically difficult to achieve, and advanced algorithms have demonstrated the ability to reidentify individuals from datasets that were considered anonymous. Research data sharing currently sits in a legal grey area that requires careful pseudonymisation and ethics committee oversight, neither of which the Act clearly mandates or guides[22].

4. Where the Law Itself Falls Short Sensitive Data and the Right to Erasure

When the Act is assessed honestly against the needs of the healthcare sector, its inadequacies become difficult to ignore. The most fundamental problem is that the Act treats all personal data identically. Unlike the European GDPR or the earlier Indian IT Rules of 2011, the DPDP Act creates no special category for sensitive personal data.[23]

A name and their HIV status, psychiatric diagnosis, or documented history of suicide attempts all receive exactly the same level of legal protection. This prevents any proportional or risk based approach to data security and represents a serious departure from the standards that global data protection frameworks consider basic.

A second problem arises from the patient's right to request erasure of their own data under section 12 of the Act. In most contexts, the right to erase is a reasonable privacy protection. In healthcare, it can be clinically dangerous. If a patient deletes records documenting drug allergies, prior treatment failures, or suicide risk, the next clinician who treats them is working without critical safety information. The Act provides no guidance on how to resolve this tension between individual data rights and clinical continuity of care.

[21]Seith, supra note 12
[22]Singh, supra note 15
[23]Seith, supra note 12

© 2026 International Journal of Advanced Legal Research

5. The Deeper Structural Failures Oversight, State Power, AI, and Regulatory Gaps

The Act also relies on a centralised Data Protection Board to oversee all sectors, with no specialised health data regulator. Without an authority that understands clinical practice, medical ethics, and health system realities, ambiguous terms like reasonable security will be interpreted without any sector-specific knowledge, producing inconsistent and potentially unworkable outcomes across vastly different healthcare settings.[24]

Section 17[25] compounds this by granting the Central Government broad discretionary power to exempt government agencies from data protection obligations on grounds as wide as sovereignty or public order[26]. In a healthcare context where the government operates large national health registries and interoperable digital health databases, these exemptions create a real risk of unchecked mass surveillance, with no requirement to meet the constitutional tests of necessity and proportionality that the Supreme Court established in the Puttaswamy judgment.

The Act is also entirely silent on artificial intelligence and automated decision-making. It offers no safeguards against algorithmic profiling or bias, no right to an explanation when an AI system makes a decision affecting a diagnosis or insurance coverage, and no framework for accountability when AI-driven tools produce discriminatory outcomes[27].

Finally, health data sits at the intersection of multiple regulatory domains, but the Act establishes no formal coordination between the Data Protection Board and sectoral authorities like the National Health Authority or the National Medical Commission.

Earlier proposals, such as the now abandoned Digital Information Security in Healthcare Act, had envisioned a dedicated National eHealth Authority precisely to fill this gap. The DPDP Act leaves that gap open.[28]

[24]Singh, supra note 15
[25]Digital Personal Data Protection Act, 2023(No.22 of 2023) Section 17
[26]Digital Personal Data Protection Act, 2023(No. 22 of 2023) Section 17.
[27]Sonia Nath and Rumi Dhar, An Analysis of the Digital Personal Data Protection Act 2023. Christ University Law Journal 2026, Vol. 15, No. 1, 93-120 ISSN 2278-4322/https://doi.org/10.12728/culj.28.5)
[28]Singh, supra note 15

© 2026 International Journal of Advanced Legal Research

V CRITICAL GAPS AND CHALLENGES

All Personal Data Is Treated the Same even though it is highly Sensitive. A closer look at the Act reveals that it treats all personal data the same way, with no special category for sensitive information. This is a major departure from global laws like the GDPR in Europe or HIPAA in the United States, both of which treat health data with a higher level of protection. Under the DPDP Act, a patient's HIV status or psychiatric history receives the exact same legal protection as their email address. This approach is not just inadequate, it is dangerous.

When there is No Court Oversight the problem in deepens. Section 17, which gives the Central Government wide power to exempt government agencies from data protection obligations on broad grounds such as national security, public order, or sovereignty. These exemptions are not tested. There is no requirement to narrow these exemptions, no prior judicial approval, and no periodic review. The large interoperable health databases like the National Digital Health Ecosystem and the Ayushman Bharat Digital Mission, this level of unchecked government access creates a real risk of mass surveillance and patient profiling without any meaningful oversight.

The Act creates confusion for doctors and healthcare workers. Indian medical practitioners routinely share patient scans, reports, and case details over platforms like Whatsapp or email because speed often determines outcomes. The Act requires explicit and specific consent before data is processed, but it says nothing about this kind of informal clinical collaboration[29]. Whether sharing a patient's MRI for a quick second opinion violates the law remains genuinely unclear. This ambiguity leaves doctors caught between providing timely care and fearing legal penalties. This situation of law currently unresolved.

For mental healthcare professionals, the problem is Introducing long privacy notices into a first clinical consultation in DPDP Act rule 3 and Mental Healthcare Act, 2017.[30]. The DPDPA adds a separate, distinct layer of consent specifically for data processing. Where a patient is already anxious and vulnerable. Small clinics face a real financial burden in meeting the compliance requirements such as upgrading software, implementing encryption, and managing consent platforms.[31]. Even where consent is obtained, research consistently shows that patients rarely read or understand complex privacy notices. They just agree and

[29]Sood, supra note 18
[30]Seith, supra note 12
[31]Khanna, supra note 11

© 2026 International Journal of Advanced Legal Research

move on. This does not constitute genuine informed consent. It is paperwork that creates a legal shield for organisations while offering patients very little actual protection.

There is also a direct conflict between the patient's right to erase their data and basic clinical safety. The Act gives individuals the right to request deletion of their personal data. In healthcare, it is potentially life-threatening. If a patient erases records the next doctor who treats them has no access to that history. The National Digital Health Mission envisions patients controlling their own electronic health records, but the DPDP Act does not provide any clear guidance on how to balance this right against the clinical duty to preserve safety critical information.[32]

The enforcement mechanism designed to address violations. The Data Protection Board of India has its own structural problem. The Central Government[33] alone appoints its Chairperson and Members, which compromises its independence, especially when investigating violations committed by government health agencies. Beyond this, if a patient suffers a data breach, the Act does not give them any explicit right to compensation. Financial penalties imposed on violators go into the Consolidated Fund of India[34] not to the patients. Appeals go to the Telecom Disputes Settlement and Appellate Tribunal under section 29[35], a body with no specific expertise in healthcare data or constitutional privacy law. The enforcement architecture, in short, is built to collect penalties rather than deliver justice to affected individuals.

The Act is silent on artificial intelligence[36] a significant omission given how rapidly AI is entering Indian healthcare. Diagnostic tools, insurance platforms, and treatment recommendation systems all rely on large patient datasets and automated decision making. If an AI system makes a biased or incorrect decision about a patient's treatment or insurance eligibility, the Act offers no right to an explanation and no right to challenge that decision. More concerning, the Act exempts anonymised data from its scope, but research shows that advanced AI can often reidentify individuals from supposedly anonymous datasets by cross referencing them with other health surveys or public records.

[32]Seith, supra note 12
[33]Digital Personal Data Protection Act, 2023(No.22 of 2023) Section 19
[34]Digital Personal Data Protection Act, 2023(No.22 of 2023) Section 33(1) schedule)
[35]Digital Personal Data Protection Act, 2023(No.22 of 2023) Section 29
[36]Singh, supra note 15

© 2026 International Journal of Advanced Legal Research

Without a dedicated health data regulator this kind that was envisioned under the now-abandoned Digital Information Security in Healthcare Act proposal[37]. There are no sector specific standards for true anonymisation or algorithmic fairness. The DPDP Act has no answer for these challenges.

VI RECOMMENDATIONS

Addressing the gaps in the DPDP Act 2023 requires practical changes at multiple levels clinical, technological, constitutional, and structural. The recommendations that emerge from a careful reading of the Act and its healthcare implications fall fixing the daily realities of clinical practice, governing artificial intelligence and cybersecurity responsibly, and reforming the law's constitutional foundations.

There must be legal exemption for healthcare workers who share patient data with other professionals for emergency consultations. When a patient themselves initiates sharing their data with a doctor through a digital platform, the law should legally recognise implied consent[38] rather than leaving clinicians in ambiguity.

Complicated privacy notices that patients sign without reading and instead adopt layered consent models. These would separate essential clinical data processing from optional data sharing, and use standardised symbols and healthcare pictograms that patients can actually understand[39].

For smaller clinics who cannot afford to build compliance infrastructure from scratch, the government should provide ready to use DPDPA-compliant portals. Given that penalties under the Act can reach up to ₹250 crore[40], enforcement in the early years should prioritise resource for healthcare settings and research.

On artificial intelligence and cybersecurity, the recommendations are equally specific. When personal medical data collected for patient care is later repurposed for AI training or research, the organisation handling that data must ensure it is properly pseudonymised or anonymised

[37]Singh, supra note 15
[38]Sood, supra note 18
[39]Seith, supra note 12
[40]Digital Personal Data Protection Act, 2023(No.22 of 2023) Schedule 1

© 2026 International Journal of Advanced Legal Research

first, and must obtain prior written approval from an Institutional Review Board or Ethics Committee before proceeding.[41]

The current Act places the entire legal burden on hospitals as data fiduciaries, but when AI technology companies develop and deploy tools that process patient data, liability for violations should be shared between the healthcare provider and the technology vendor, with the degree of responsibility determined by the principle of proportionality.

To prevent AI systems from producing biased outcomes that discriminate against certain patient groups, mandatory bias assessments[42] and the use of diverse training datasets should be required.

Researchers and developers should also be encouraged to use privacy preserving methods such as federated learning, where AI models are trained locally without centralising patient data, and differential privacy techniques.

Government healthcare budgets must allocate dedicated funding for regular Vulnerability Assessment and Penetration Testing[43], and significant health institutions must appoint full time cybersecurity teams.

Section 17, which currently allows the Central Government to exempt state agencies from data protection obligations on vague grounds like public order or sovereignty, must be significantly narrowed. Any exemption the State claims should be required to meet strict tests of demonstrable necessity and proportionality, be limited to a specific and clearly stated purpose, and be subject to mandatory periodic review and sunset clauses so that exemptions do not become permanent by default.[44]

The Data Protection Board of India, which is currently controlled by the executive branch, needs to be structurally independent. This means replacing the current appointment process with a transparent, multi stakeholder mechanism involving the judiciary or Parliament, granting Board members fixed and protected tenures, and ensuring the Board has full financial and operational autonomy.

[41]Sood, supra note 18
[42]Singh, supra note 15
[43]Sood, supra note 18
[44]Aashi dixit, Data protection in india after the digital personal data protection act, 2023: a critical evaluation of privacy and state power, indian journal of legal review (ijlr), 6 (1) of 2026, pg. 116-130, apis – 3920 – 0001 &issn -2583-2344. Doi –https://doi.org/10.65393/ldeo6679).

© 2026 International Journal of Advanced Legal Research

Patients who suffer real harm from data breaches must also be given an explicit statutory right to compensation. currently all penalty money goes into the Consolidated Fund of India, leaving victims with nothing.

Private sector organisations designated as Significant Data Fiduciaries are required to conduct Data Protection Impact Assessments, large-scale government health programmes routinely escape this requirement. Mandatory impact assessments and public disclosures for state run health registries must be introduced to ensure that government led data processing is held to the same standard of transparency that the Act demands from everyone else.

VI CONCLUSION

The DPDP Act 2023 is a necessary but necessity alone does not make a law sufficient. A careful assessment against the constitutional test. The Court established that any interference with the right to privacy must meet strict tests of necessity and proportionality. But this Act currently stands, fails this test in critical ways. Its broad exemptions for state agencies, its diluted consent requirements, and the structural dependence of the Data Protection Board on the executive branch collectively weaken the law's ability to restrain intrusive government data practices. Without urgent correction, the risk is not merely that the Act will be ineffective but it becomes an instrument of state surveillance and control rather than a genuine protection of individual privacy and autonomy.

In the healthcare sector specifically, the Act represents a watershed moment[45] in principle. For the first time, India has a law that enforces consent and data security across the healthcare system, which has the potential to meaningfully improve patient trust and institutional accountability[46] But the gap need to be resolved as we discussed. What the healthcare sector needs is not a softer version of the law, but a smarter one. Health specific rules that account for clinical realities, provide clear guidance on edge cases, and build enforcement around remediation and capacity-building before punishment. The are necessary conditions for the Act to function in a real healthcare environment without becoming a source of frivolous litigation against well intentioned medical professionals.

The ethical, privacy, and governance challenges that AI brings to healthcare are algorithmic bias, reidentification of anonymised data, automated decisions with no right to explanation

[45]Sood, supra note 18

[46]Khanna, supra note 11

© 2026 International Journal of Advanced Legal Research

require continuous regulatory attention, not a one-time legislative mention. Human oversight must always remain in control of AI-supported medical decisions.

Taken together, the evidence points to one overarching conclusion. The DPDP Act 2023 is a vital foundation, but it was built with one eye on administrative flexibility and state convenience, and not enough attention to robust individual rights. For the Act to genuinely protect patients, enable responsible innovation, and fulfil the constitutional promise of the Puttaswamy judgment, it requires structural reform of its institutional architecture, health specific regulatory guidance that reflects clinical realities, and serious investment in the capacity of healthcare providers, especially smaller ones, to understand and meet their obligations under the law.

© 2026 International Journal of Advanced Legal Research