International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Protection of Sensitive Personal Health Data in India: Examining the Legal Gaps in the DPDP Act, 2023

Pragati Singh[1], Dr. Ruchika Sharma[2]

[1]LLM Student, University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India.
[2]Associate Professor, University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India.

Abstract

Electronic health records, telemedicine platforms, wearable diagnostic devices, and the country's digital health infrastructure have all helped to rapidly digitize healthcare delivery in India, leading to unprecedented volumes of private medical data. The Digital Personal Data Protection Act, 2023, and the Digital Personal Data Protection Rules, 2025, break away from established domestic and international precedent by discarding the statutory classification of sensitive personal data. This is despite the reality that health information is a well-established category in privacy jurisprudence that requires enhanced legal protection on account of the irreversible harm caused by unauthorized disclosure. This study examines the legal gaps related to personal health data in the Indian data protection system critically using a doctrinal and comparative legal research methodology. It traces the journey from the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, to the uniform data model of the 2023 Act; examines the impact of the removal of Section 43A of the Information Technology Act, 2000, on the compensatory remedies available to individuals; investigates the wide consent exemptions for medical emergencies and state welfare programs under Section 7; and scrutinizes the institutional governance gaps under the Ayushman Bharat Digital Mission Health Data Management Policy. The study ends with recommendations for a statutory sub-classification of health data, fiduciary duties in specific sectors, explicit data portability rights, and restorative compensation mechanisms. The framework of India is compared with Article 9 of the EU General Data Protection Regulation and the US Health Insurance Portability and Accountability Act.

Keywords: Sensitive Personal Health Data, Digital Personal Data Protection Act 2023, Medical Privacy, Informed Consent, Data Fiduciary Obligations, Health Data Governance

Introduction

Electronic health records, telemedicine platforms, wearable diagnostic devices and the country's digital health infrastructure have all helped to rapidly digitize healthcare delivery in India, leading to unprecedented volumes of private medical data. The Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 break away from established domestic and international precedent by discarding the statutory classification of sensitive personal data. This is despite the reality that health information is a well-established category in privacy jurisprudence that requires enhanced legal

protection on account of the irreversible harm caused by unauthorized disclosure. This study examines the legal gaps related to personal health data in the Indian data protection system critically using a doctrinal and comparative legal research methodology. It traces the journey from the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 to the uniform data model of the 2023 Act; examines the impact of the removal of Section 43A of Information Technology Act, 2000 on the compensatory remedies available to individuals; investigates the wide consent exemptions for medical emergencies and state welfare programs under Section 7; and scrutinizes the institutional governance gaps under the Ayushman Bharat Digital Mission Health Data Management Policy. The study ends with recommendations for a statutory sub-classification of health data, fiduciary duties in specific sectors, explicit data portability rights and restorative compensation mechanisms. The framework of India is compared with article 9 of the EU General Data Protection Regulation and the US Health Insurance Portability and Accountability Act.

1. Introduction:

Healthcare information is a very personal area of human life. Clinical diagnoses, genetic predispositions, reproductive histories, psychiatric assessments and prescription records reveal the most sensitive aspects of a person's physical and mental identity. Health information, once stolen, is never recoverable – unlike contact numbers or banking credentials, which can be changed or reissued after a security breach. The unauthorized leakage of medical data can lead to long-lasting social stigma, employment discrimination, denial of insurance coverage, and psychological suffering for individuals [1].

In Justice K. S. Puttaswamy (Retd.) The constitutional basis of medical privacy in India was laid down by the Supreme Court in a nine-judge bench in Justice K.S. Puttaswamy (Retd.) and Others v. Union of India & Ors. [2017] [2] The court said that informational self-determination and bodily autonomy are an integral part of the fundamental right to life and personal liberty under Article 21 of the Indian Constitution. After years of discussions in the legislature, Parliament on August 11, 2023, passed the Digital Personal Data Protection Act, 2023. The Central Government announced the Digital Personal Data Protection Rules, 2025 on November 13, 2025 which will operationalize the statutory framework over the course of an eighteen-month implementation timeline that will conclude in May 2027 [3], [4].

The Digital Personal Data Protection Act, 2023 is a structural departure that creates serious problems for healthcare governance, although it is India's first comprehensive data privacy law. The 2023 Act abolishes the distinction between ordinary personal data and sensitive personal data. However, previous Indian subordinate legislation under the Information Technology Act, 2000 specifically identified medical records and physical, physiological and mental health conditions as sensitive personal data subject to heightened safeguards [5], [6]. The Act creates significant doctrinal and practical weaknesses in the protection of personal health data by placing clinical records on the same statutory footing as standard commercial identifiers.

This research paper will critically examine the legal framework governing sensitive personal health data under the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025, to protect patient autonomy and medical confidentiality, identify specific statutory and regulatory gaps, compare India's approach with international health privacy benchmarks, and suggest specific legal reforms.

2. Review of Literature and Research Methods

2.1 Previous Literature

The legal and bioethical literature is constantly pointing to the need for a specific regulatory protection of health information, due to the unequal power relations between patients and institutional health care providers. Lawrence O. Gostin (2000) explains that health privacy is fundamental for good public health outcomes and protecting individual dignity, because people will not seek prompt medical attention when they fear that sensitive conditions such as infectious diseases or mental illnesses will be disclosed without their authorization.

Committee of Experts headed by Justice B. N. Srikrishna (2018) recommended that health, genetic and biometric data be treated as sensitive personal data under Indian law, requiring explicit consent, stricter grounds for processing and mandatory data protection impact assessments [7]. Later academic analyzes of the Digital Personal Data Protection Act, 2023 have pointed out the consequences of abandoning this tiered approach. The academic literature on clinical and psychiatric practice in India suggests that the 2023 Act's one-size-fits-all approach to all types of digital personal data is blind to the high levels of stigma around mental health diagnoses and reproductive records, leading to compliance ambiguities for hospitals, diagnostic labs and digital health apps [1]. The recent analysis of the Digital Personal Data Protection Rules, 2025 [6], [8] suggests that the soon-to-be-removed Section 43A of the Information Technology Act, 2000 will end the requirement for civil compensation for victims of health data breaches. While the past literature has given a brief overview of the provisions of the Act, a detailed synthesis of the similarities and differences between the 2023 Act, the 2025 Rules and the policy framework of the Ayushman Bharat Digital Mission on health data privacy is yet to emerge.

2.2 Research Methodology

This work uses a doctrinal, analytical and comparative legal research techniques. The main legal sources studied are The Digital Personal Data Protection Act, 2023, Digital Personal Data Protection Rules, 2025, Information Technology Act, 2000, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Ayushman Bharat Digital Mission Health Data Management Policy, Supreme Court of India judgments, Regulation (EU) 2016/679 (General Data Protection Regulation) and United States Health Insurance Portability and Accountability Act of 1996. Secondary sources include peer-reviewed medical-legal publications, expert committee reports, and legislative commentary [1], [6]–[8].

3. Evolution of Health Data Protection in India: From SPDI Rules 2011 to DPDP Act 2023

Section 43A of the Information Technology Act, 2000, read along with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 was the main legal framework for electronic medical records in the private sector before the Digital Personal Data Protection Act, 2023 [5]. Sensitive personal data or information as defined under Rule 3 of the 2011 Rules [5] includes physical, physiological and mental health problems, sexual orientation, medical records and history and biometric information. Rules 4, 5 and 6 required corporations that handle such sensitive data to have prior written or electronic consent, follow strict guidelines on purpose limitation and data minimization, restrict disclosures to third parties and use certified security standards such as ISO/IEC 27001 [5].

The 2018 Srikrishna Committee Report proposed a two-tier taxonomy based on the high risk of major damage of ordinary personal data and sensitive personal data [7]. Health and genetic data are included in

the category of sensitive personal data. This categorization in tiers has been carried forward in the Joint Parliamentary Committee Report of 2021 and the Personal Data Protection Bill of 2019. However, the legislature completely abolished the category of sensitive personal data when the Ministry of Electronics and Information Technology proposed the streamlined Digital Personal Data Protection framework in 2022 and passed the Digital Personal Data Protection Act, 2023 [3], [6].

Crucially, Section 43A of the Information Technology Act, 2000 is repealed with effect from May 13, 2027 under Section 44(2) of the Digital Personal Data Protection Act, 2023. Consequently, the 2011 Sensitive Personal Data or Information Rules will no longer be in effect [3], [4], [6]. Thus, the Indian legal system moves from a specialized, calibration of sensitivity framework to a standard, consent-based framework that applies the same baseline norms to an oncology treatment record and a retail loyalty card.

4. An inquiry into the legal loopholes in the DPDP Act 2023 and the DPDP Rules 2025

A close reading of the statutory text reveals six important legislative gaps which have an impact on the protection of personal health data in India.Here are some examples of these loop holes: -!

To start. A pre-classification of sensitive health data is not required by law in any circumstance. Every piece of information that can be used to identify a specific person is considered to be personal data, according to Section 2(t) of the Digital Personal Data Protection Act, 2023 [3]. The Act does not create a separate legal category for health, genetic or biometric data [3], [6], and therefore the baseline requirements for notification (Section 5), consent (Section 6) and security measures (Section 8(5)) are the same regardless of clinical sensitivity. The volume and sensitivity of personal data processed by an entity is one of the discretionary factors for the Central Government to notify an entity as a Significant Data Fiduciary under Section 10(1)(a). Smaller clinics, diagnostic centers, fertility clinics, mental health practices, and health-technology start-ups are not Significant Data Fiduciaries and are not subject to enhanced statutory obligations [1], [3].

2. "Dilution of Consent Standards and Excessive Emergency Exemptions Under Section 7: Section 6 requires that consent be unequivocal, free, specific, informed and unconditional [3]. But patients who are seriously ill or who are dependent on institutions have little real bargaining power to insist on privacy conditions in therapeutic settings. More importantly, Section 7 defines a broad range of permissible nonconsensual uses [3]. Processing without consent is provided under section 7(g) to provide for medical treatment or health services during an epidemic, disease outbreak or any other threat to public health. Processing without consent is provided under section 7(f) to respond to a medical emergency involving a threat to the life or immediate threat to the health of the Data Principal or any other individual [3]. The wide and undefined ambit of the term “any other threat to public health” in Section 7(g) allows for wide state surveillance, mandatory health profiling, and unauthorized secondary data sharing during public health emergencies without sunset clauses.

3. Excluding Section 43A and absence of victim compensation: In case the exposure of sensitive medical data is caused by the negligence of a hospital, a person can directly claim civil compensation for wrongful loss under Section 43A of the Information Technology Act, 2000 [5], [8]. Section 44(2) deletes Section 43A without providing a substitute compensatory remedy. All pecuniary penalties – up to INR 250 Crore under the Schedule – are paid exclusively into the Consolidated Fund of India by the Digital Personal Data Protection Act, 2023 [3], [6], [8]. The Data Protection Board of India does not award statutory damages to a patient who has his HIV status, mental history or genetic disease leaked online. Instead, the patient has to file a long-drawn common-law tort lawsuit.

4. Removal of non-digitized/offline medical records. Section 3(a) limits the Act to personal data that is either acquired digitally or collected in a non-digital form and subsequently digitized [3]. In rural and semi-urban India, a lot of outpatient prescriptions, diagnostic slips and hospital admission registries are still completely paper based. The legislation does not cover physical medical records, resulting in arbitrary protection gap depending solely on the storage media and not on the sensitivity of the patient's health condition.
5. No Right to Data Portability and Limitations on Interoperability: The Act does not create a legislative right to data portability, notwithstanding Sections 11 and 12 which grant Data Principals the right to view a summary of processed personal data and to request correction or deletion [3]. Patients are routinely transferred from hospitals to specialists to insurance companies in today's health care system. Patients risk vendor lock-in and fragmented continuity of care without an enforceable right to get structured, machine-readable electronic health data and transfer them securely to another provider.
6. Lack of Specific Secondary Research and Clinical Trial Safeguards: Section 17(2)(b) grants an exemption from the core obligations of the Act for processing that is necessary for research, archiving or statistical purposes if the personal data is processed in accordance with prescribed guidelines, and is not used to make any decision that is unique to a Data Principal [3]. Even after direct identifiers have been removed, re-identification risks remain substantial in biomedical research, genome sequencing, and artificial intelligence model training using hospital databases. Pseudonymisation is not tightly regulated by law, these cohorts of patients are not under an institutional ethics board, there are no algorithmic bias audits and they are commercially exploitable.

5. The policy of responsible business management and regulation in the sector is the fifth item on the list. Governance and institutional breakdown

Despite the fact that the Digital Personal Data Protection Act, 2023 contains a number of legal loopholes, the situation is made even more complicated by the numerous regulations that govern the healthcare industry in India. The Ayushman Bharat Digital Mission by the National Health Authority connects longitudinal medical information of people through unique Ayushman Bharat Health Accounts. The primary source of governance for this ecosystem is the Ayushman Bharat Digital Mission Health Data Management Policy, which has provisions for opt-out procedures, granular consent artifacts, and privacy-by-design principles [9]. However, the Health Data Management Policy only governs the organizations that are part of the federated digital health network. The Health Data Management Policy does not have independent legislative enforcement authorities as it is an administrative policy framework, not a parliamentary act [9].

The Human Immunodeficiency Virus and Acquired Immune Deficiency Syndrome (Prevention and Control) Act, 2017 (which prescribes stringent informed consent and confidentiality protocols), the Clinical Establishments (Registration and Regulation) Act, 2010, the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002, and the Mental Healthcare Act, 2017 (which protects the confidentiality of mental health records under Section 23. In addition, only certain large e-commerce, online gaming and social media intermediaries are subject to the mandatory three-year data deletion timelines for inactive users under the Third Schedule to the Digital Personal Data Protection Rules, 2025. As such, data retention periods for health apps and diagnostic platforms are mainly determined by vague purpose-limitation criteria in the absence of sectoral regulations [4].

6. Comparative Legal Analysis: HIPAA in the US, GDPR in the EU and India

A comparison of India's statutory model with established overseas health privacy regimes highlights structural flaws caused by the absence of a special-category data structure.

Table 1: Comparative Analysis of Health Data Protection Regimes

Regulatory Dimension	India (DPDP Act, 2023 & Rules, 2025)	European Union (GDPR, 2016).	United States (HIPAA Privacy and Security Rules)
Classification of Health Information	No separate category; treated as ordinary digital personal data	Special category of personal data under Art. 9(1) (health, genetic, biometric)	PHI subject to certain federal regulations
Default processing rules	Permitted by general consent (Section 6) or under wide legitimate uses (Section 7)	Article 9(1) prohibits by default unless a strict Article 9(2) exception applies	Permitted for treatment, payment and health care operations otherwise requires authorization
Data Protection Impact Assessments	Required for notified Significant Data Fiduciaries (Section 10)	required by Article 35(3)(b) for processing of health data on a large scale	Enterprise-wide Security Risk Analysis required by 45 CFR 164.308(a)(1)
Individual's Right to Data Portability	Chapter III Data Principal rights absent	Explicitly justified in a structured machinereadable format under Article 20	Right of access and electronic transmission to third parties 45 CFR 164.524
Individual Compensation for Victims	State gets penalties accruing on repealing Sec 43A IT Act	Right to material and non-material compensation from controller under Art. 82 9.	No private right of action under HIPAA, but state tort and statutory remedies may be invoked

The processing of genetic data, biometric data for the purpose of uniquely identifying a natural person and data concerning health is generally prohibited in accordance with Article 9(1) of the EU General Data Protection Regulation unless the controller is subject to one of the specific exceptions in Article 9(2), such as explicit consent, occupational or preventive medicine under the obligation of professional secrecy or a substantial public interest supported by proportionate statutory safeguards [10]. Also, Article 82 guaranties the right to financial compensation for any material or non-material damage caused to the data subject by a breach of the Regulation and Article 9(4) provides Member States with the possibility of retaining or introducing further conditions and limitations in relation to genetic, biometric or health data [10].

Similarly, the United States Health Insurance Portability and Accountability Act of 1996 provides a specific regulatory framework for Protected Health Information among covered entities and business associates. It uses technological, administrative and physical safeguards specifically designed for health care operations, such as audit trails, role-based access restrictions, mandatory encryption and minimum-necessary disclosure standards. In contrast, Indian health sector entities do not have any mandatory clinical

security standards, as India relies on a uniform standard under Section 8(5) of the Digital Personal Data Protection Act, 2023 and Rule 6 of the Digital Personal Data Protection Rules, 2025.

7. Recommendations and Future Directions

To close the legal loopholes in India's health data protection system and bring statutory governance in line with Article 21's right to privacy, the following legislative and regulatory changes are suggested:

First of all. Parliament should amend Section 2 of the Digital Personal Data Protection Act, 2023 to define Sensitive Personal Data that includes genetic information, medical records, physical and mental health conditions, and biometric identifiers. Reintroduce Sensitive Personal Data Sub-Classification: A special clause should be added requiring explicit, unbundled consent and higher security standards for processing such data.

Two. Notify Healthcare Entities as Significant Data Fiduciaries: To bring hospitals, diagnostic chains, health insurance companies, digital health platforms and genomic repositories processing large-scale or high-risk health data within the ambit of required Data Protection Impact Assessments and independent annual audits, the Central Government should exercise its power under Section 10(1) to notify these entities as Significant Data Fiduciaries.

Thirdly. The Digital Personal Data Protection Act, 2023 should be amended to allow the Data Protection Board of India to provide direct civil remedies to Data Principals who have suffered financial loss, discrimination or emotional distress due to the unauthorized disclosure of their personal health data under Section 33.This would mitigate the effects of repealing Section 43A of the IT Act, 2000.

Exemptions for Public Health in Section 7(g) The Central Government is required to create regulations that are legally binding in accordance with Section 7(g) in order to allow the processing of health data without the consent of the individual in situations where there is an epidemic or a threat to public health.Such rules will only apply to notified public health authorities, and will be subject to strict purpose limitation and mandatory anonymization or deletion after the public health emergency is over.

Fifth. 'Amendment to Chapter III of the Act to provide for a right to data portability. This will allow patients to easily transfer their electronic health information from one health care provider to another. Sectoral Retention Rules should also be created. In order to bring the Digital Personal Data Protection Rules, 2025, into alignment with the framework of the Ayushman Bharat Digital Mission, the Ministry of Health and Family Welfare and the Ministry of Electronics and Information Technology are required to also issue binding standards for the retention of data and anonymization of data in the health sector.

8. Briefly,

The Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 [3], [4] are a big step toward creating a legal framework for privacy in India's digital economy. The current framework, however, does not protect the intimate medical privacy protected under Article 21 of the Constitution as it removes the legal distinction between ordinary personal data and sensitive health information, repeals individual compensatory remedies under Section 43A of the Information Technology Act, 2000, and leaves broad non-consensual processing exemptions unregulated [2], [6], [8]. In addition to exposing vulnerable populations to the risk of irreparable stigma and discrimination, the treatment of sensitive health information as regular commercial data risks eroding patient confidence in digital healthcare ecosystems [1]. Tiered statutory safeguards for health data, mandatory clinical security and impact assessments and the reinstatement of restorative remedies for victims of breaches are necessary to

ensure technological innovation in Indian healthcare proceeds without compromising human dignity and informational autonomy.

References

1. M. M. Nagendra, D. Raveendranathan, and K. P. Muliyala, "The Digital Personal Data Protection Act 2023: Implications for mental healthcare practice in India," Indian J. Psychol. Med., vol. 47, no. 5, pp. 1–7, Sep. 2025. [Online]. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC12423081/
2. Supreme Court of India, "Justice K. S. Puttaswamy (Retd.) and Another v. Union of India and Others," Supreme Court Cases, vol. 10, pp. 1–636, 2017. [Online]. Available: https://indiankanoon.org/doc/127517806/
3. Ministry of Law and Justice, Government of India, "The Digital Personal Data Protection Act, 2023 (No. 22 of 2023)," The Gazette of India, Aug. 2023, pp. 1–21. [Online]. Available: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
4. Ministry of Electronics and Information Technology, Government of India, "Digital Personal Data Protection Rules, 2025 (G.S.R. 846(E))," The Gazette of India, Nov. 2025, pp. 1–38. [Online]. Available: https://www.dpdpa.com/DPDP_Rules_2025_English_only.pdf
5. Ministry of Communications and Information Technology, Government of India, "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (G.S.R. 313(E))," The Gazette of India, Apr. 2011, pp. 1–6. [Online]. Available: https://www.lexcyberia.com/pdf/The%20Information%20Technology%20(Reasonable%20Security%20Practices%20and%20Procedures%20and%20Sensitive%20Personal%20Data%20or%20Information)%20Rules,%202011.pdf
6. Taxmann Editorial Board, "SPDI Rules and the DPDP Act: What changes in May 2027," Taxmann Research Blog, Nov. 2026, pp. 1–8. [Online]. Available: https://www.taxmann.com/post/blog/spdi-rules-vs-dpdp-act
7. Committee of Experts under the Chairmanship of Justice B. N. Srikrishna, "A free and fair digital economy: Protecting privacy, empowering Indians," Ministry of Electronics and Information Technology, Government of India, Jul. 2018, pp. 1–213. [Online]. Available: https://prsindia.org/files/bills_acts/bills_parliament/2019/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill,%202018_0.pdf
8. Cyril Amarchand Mangaldas, "FAQs on the Digital Personal Data Protection Act, 2023," Cyril Amarchand Mangaldas Thought Leadership, Dec. 2025, pp. 1–24. [Online]. Available: https://www.cyrilshroff.com/wp-content/uploads/2025/12/FAQs-DPDPA.pdf
9. National Health Authority, Ministry of Health and Family Welfare, "Ayushman Bharat Digital Mission Health Data Management Policy," Government of India, 2022, pp. 1–32. [Online]. Available: https://abdm.gov.in/strapicms/uploads/privacypolicy_178041845b.pdf
10. European Parliament and Council of the European Union, "Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation)," Off. J. Eur. Union, L 119, pp. 1–88, May 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng