DOI: 10.21088/jha.2582-3566.9225.3

Journal of Hospital Administration
Volume 9 Number 2, July - December 2025

REVIEW ARTICLE

# The Digital Personal Data Protection Act, 2023: Forensic and Medicolegal Implications in Healthcare Administration

**Adjourno Contentie CH Mark[1], Arijit Dey[2], Ninad Vilas Nagrale[3]**
**Venkatesh Janarthanan[4], Oinam Gambhir Singh[5]**

**HOW TO CITE THIS ARTICLE:**

***Adjourno Contentie CH Mark, Arijit Dey, Ninad Vilas Nagrale et. al,*** The Digital Personal Data Protection Act, 2023: Forensic and Medicolegal Implications in Healthcare Administration. RFP Journal of Hospital Administration; 2025; 9(2): 71-77.

## ABSTRACT

The rapid digitization of India's healthcare sector has amplified the need to protect sensitive patient data and ensure accountability in hospital administration. Earlier frameworks such as the Information Technology Act, 2000 offered only limited safeguards and proved inadequate against evolving cybersecurity threats. The Digital Personal Data Protection (DPDP) Act, 2023 introduces a consent-driven framework that strengthens patient rights, enforces fiduciary obligations on hospitals, and aligns India with global data protection practices. This paper explores its implications for healthcare institutions, particularly in the management of electronic health records, digital consent, and hospital information systems. It also examines national initiatives like the Ayushman Bharat Digital Mission (ABDM) and platforms such as MEDLEAPR, which enhance secure record-keeping and data transfer. By addressing gaps and recommending measures such as encryption, role-based access, and trained Data Protection Officers, the Act aims to build trust, strengthen governance, and ensure resilience in healthcare data management.

## KEYWORDS

• DPDP Act 2023 • Healthcare Data Protection • Electronic Health Records • Patient Privacy

**AUTHOR'S AFFILIATION:**

[1] Junior Resident, Department of Forensic Medicine and Toxicology, All India Institute of Medical Sciences, Kalyani, West Bengal, India.

[2] Associate Professor, Department of Forensic Medicine and Toxicology, All India Institute of Medical Sciences, Kalyani, West Bengal, India.

[3] Additional Professor, Department of Forensic Medicine and Toxicology, All India Institute of Medical Sciences, Kalyani, West Bengal, India.

[4] Assistant Professor, Department of Forensic Medicine and Toxicology, All India Institute of Medical Sciences, Kalyani, West Bengal, India.

[5] Professor, Department of Forensic Medicine and Toxicology, All India Institute of Medical Sciences, Kalyani, West Bengal, India.

**CORRESPONDING AUTHOR:**

**Arijit Dey,** Associate Professor, Department of Forensic Medicine and Toxicology, All India Institute of Medical Sciences, Kalyani, West Bengal, India.

**E-mail:** arijit.forensic@gmail.com

➢ **Received:** 26-09-2025 ➢ **Accepted:** 01-12-2025

## INTRODUCTION

Hospitals and healthcare institutions manage vast amount of patient information, both digital and non-digital. Protecting personal data is essential for fostering trust between patients and the healthcare system. Under Article 21 of the Indian Constitution stating the right to privacy forms a vital part of individual liberty, thereby necessitating robust data protection frameworks in today's digital era.

Medical and research institutes often collect personal data for patient care and research purposes. However, no specific legislation previously regulated the privacy and use of such data. The Information Technology (IT) Act, 2000 was a crucial starting point for digital data protection in India; however, with technology advancing by leaps and bounds over the past two decades, the Act has become vague and outdated, leaving it inadequate to address modern data protection and cybersecurity challenges. This void is what the Digital Personal Data Protection (DPDP) Act, 2023 now seeks to fill with a more comprehensive, consent-based, and globally aligned framework.[1]

**International Data Protection Laws:**

**1. China:** The People's Republic of China (PRC) has developed a multi-layered legal framework for personal data protection, built primarily on three core legislations: the Personal Information Protection Law (PIPL), the Cybersecurity Law (CSL), and the Data Security Law (DSL). Of these, the PIPL (2021) stands out as China's first comprehensive, nationwide law dedicated to personal information protection, significantly strengthening earlier mechanisms. In addition to these pillars, data security in the PRC is governed through a wide array of supplementary laws and regulations, including the Decision on Strengthening Online Information Protection (effective December 28, 2012), the Draft Regulation on Network Data Security Management (released for consultation on November 14, 2021), the Measures for the Security Assessment of Outbound Data Transfers (effective September 1, 2022), and the Network Data Security Management Regulation (effective January 1, 2025). Collectively, these instruments aim to safeguard online data security, uphold the legal rights and interests of individuals and organizations, and preserve national security as well as public interests.[2]

**2. Japan:** In Japan, the Act on the Protection of Personal Information (APPI, Act No. 57 of 2003) is the principal law governing personal data collection and processing. The law is overseen by the Personal Information Protection Commission (PPC), which also issues guidelines, including those on cross-border transfers. Major revisions in 2017 and 2022 strengthened privacy safeguards. The 2022 amendment restricts use of personal data beyond the consented purpose, significantly affecting medical research. Unless institutions like university hospitals explicitly allow dual use for clinical practice and research, written patient consent specifying project details is mandatory. Similar safeguards could strengthen India's digital healthcare framework.[3]

**3. Singapore:** Singapore's Personal Data Protection Act (PDPA) is the primary law regulating the collection, use, and disclosure of personal data. It establishes a baseline standard of protection aimed at safeguarding individuals' information while ensuring that organisations manage such data responsibly and transparently. Beyond the PDPA, several industry-specific regulations exist, complementing its objectives and tailoring requirements to sectoral needs. The Act applies broadly to all organisations operating in Singapore, including healthcare providers, regardless of their industry. Under the PDPA, entities must obtain informed consent before handling personal data, provide individuals with access to their information upon request, and maintain strong security measures to protect against unauthorised use, disclosure, or breaches, thereby enhancing accountability and trust.[3]

**4. United Kingdom:** The UK Data Protection Act 2018, aligned with the General Data Protection Regulation (GDPR), governs secure data transfers and is enforced by the Information Commissioner's Office (ICO), which protects privacy rights and regulates sensitive data, including health information. Health data, classified as a "special category," requires stricter safeguards and can only be processed under conditions such as explicit consent, medical necessity, public health interest, or scientific research, often with an appropriate policy document. Additionally, the EU Artificial Intelligence (AI) Act, effective August 1, 2024, applies extraterritorially to AI systems used in the EU. India's DPDP Act

could adopt similar accountability and risk-based approaches.[3]

**5. United States of America:** The U.S. Department of Health and Human Services (HSS) introduced Health Insurance Portability and Accountability Act (HIPAA), to safeguard healthcare data, preventing the unauthorised disclosure of patients' personal information. It applies to health plans, healthcare clearinghouses, and healthcare providers transmitting health information.[3]

**Legal Frameworks Governing Personal Data Protection in India:**

Globally, numerous countries have established legal frameworks for digital data protection. India, as the world's most populous nation and one of the largest internet markets, witnesses an immense volume of data being generated and exchanged every second. India has witnessed several significant data breach incidents in recent years. The country's biometric database was compromised, potentially exposing the records of 1.1 billion registered citizens. In the healthcare sector, a major breach occurred in October 2023, when the COVID-19 testing data of 815 million individuals was stolen from the Indian Council of Medical Research (ICMR). Similarly, on 23rd November 2022, the All India Institute of Medical Sciences (AIIMS), New Delhi, one of India's premier government hospitals suffered a ransomware attack that severely disrupted its digital operations.[4]

India, has formulated new criminal laws in 2023, multiple legal frameworks and digital platforms mentioned as follows on an attempt to protect the personal data security threats:

- **Bharatiya Nyaya Sanhita, 2023:** Section 319 BNS defines impersonation including the digital identity misuse, Section 72 BNS protects victim privacy, including digital contexts, Section 238 BNS tampering of evidence. The absence of explicit legal definitions for digital data theft and cyber infractions remains a critical gap.[5]
- **Bharatiya Nagarik Suraksha Sanhita, 2023:** The BNSS, 2023 facilitates the use and admissibility of electronic/digital records in criminal investigations and trials, but it does not regulate personal data collection, processing, or privacy (Section 105 and 176).[6]
- **Bharatiya Sakshya Adhiniyam, 2023:** BSA governs admissibility of evidence, including digital and electronic records in the court of law (Section 61-68 BSA). It ensures procedural safeguards so that only authentic, certified, and tamper-proof electronic records are admitted in court. For healthcare, this means EHRs, telemedicine records, and digital consents are admissible only if properly certified, thereby indirectly protecting patient data integrity.[7]
- **Information Technology Act, 2000:** India's first legislation on electronic governance and cybercrime, indirectly addressed aspects of data protection relevant to healthcare. While not sector-specific, certain provisions applied to the handling of sensitive health information: Section 43A, Section 66C-Identity theft Section 72 and 72A- Breach of confidentiality and privacy by service providers. Despite these provisions, the Act had limitations: it lacked clear definitions of health-specific data rights, did not establish a dedicated regulatory body for enforcement, and failed to keep pace with advancements in telemedicine, electronic health records, and digital health research.[8]
- **Information Technology (Reasonable security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011:** The IT (Reasonable Security Practices and Sensitive Personal Data or Information) Rules, 2011 elaborated on "sensitive personal data," including medical records and health information. These rules required explicit patient consent before collection, processing, or sharing of such data.[9]
- **Telemedicine Practice Guidelines, 2020:** Before 2020, India lacked clear legal guidelines, creating ambiguity for practitioners. The Telemedicine Practice Guidelines legally empower Registered Medical Practitioners to use telemedicine with the same ethical standards as in-person care, ensuring patient safety, consent, privacy, documentation, and accountability, while expanding access to healthcare across India even to remote and rural areas.[10]

- **Ayushman Bharat Digital Mission (ABDM) / ABHA / UHI:** The Ayushman Bharat Health Account (ABHA) was first introduced in India on 27 September 2021 under the Ayushman Bharat Digital Mission (ABDM) to provide every citizen with a unique Health ID for digitally linking and accessing their medical records across hospitals, clinics, and laboratories. India's mission includes a national digital health ecosystem to achieve universal health coverage. This system creates a unified health data infrastructure with registries for facilities and professionals. It uses health information exchanges and a consent management framework to enable the secure, interoperable exchange of health data. The goal is to provide efficient, accessible, and affordable healthcare by leveraging open digital systems while ensuring the privacy, security, and confidentiality of personal health information, giving individuals control over their data.[11]
- **Electronic Health Record Standard of India:** India's healthcare sector is legally regulated by the Electronic Health Record (EHR) Standards of India,[2] which focus on maintaining confidentiality, security, and privacy in electronic health records to enable safe exchange of health information.
- **Other EHRs:** Apart from national digital health initiatives, several private electronic health record (EHR) and telemedicine platforms are also being used across India. Examples include Bharat E Health, an AI-powered EHR and telemedicine system, and MediBank, a centralized cloud-based EHR platform.[12,13] These services provide digital healthcare solutions but may not always be fully integrated with national or regulatory frameworks. In addition, many states and private hospitals have adopted their own Hospital Information Management Systems (HIMS) to manage appointments, maintain medical records, and streamline services such as online outpatient scheduling and record keeping.[14]
- The aforementioned legal frameworks contain loopholes, hence inadequate in providing clear, specific guidelines for safeguarding personal data. With emerging advancement of technology and artificial intelligence, the digital world has become more complex. Cyberthreats such as: a) Malware (Malicious Software) can damage systems, steal data, or demand ransom, b) Insider Threats by Employees or contractors misusing access to steal or leak sensitive information, c) IoT (Internet of Things) Attacks-exploiting vulnerabilities in smart devices, d) Supply Chain Attacks-targeting third-party vendors or software providers to compromise end users. All these poses serious risks to healthcare data and other personal information online, as they can lead to unauthorized access, data theft, disruption of services, and large-scale privacy breaches.[15]

The DPDP Act, 2023 marks a major shift in India's legal framework for protecting personal data, with direct implications for the healthcare sector, where sensitive health information is routinely collected, processed, and stored.

### Implications of the Digital Personal Data Protection (DPDP) Act, 2023 in Healthcare

As illustrated in Figure 1, the framework of the DPDP Act, 2023 within hospital administration underscores patient consent, fiduciary responsibilities, secure management of health records, and accountability through the Data Protection Board of India.

### 1. Patient Registration

During patient registration, the DPDP Act, 2023 mandates hospitals to obtain free, informed, specific, and unambiguous consent before collecting personal data. Implied consent is no longer sufficient, and patients must be clearly informed about the purpose of data use, such as treatment, insurance, or research. For children and persons with disabilities, lawful guardian consent is required. This ensures that registration systems not only collect essential details but also respect patient autonomy and privacy, thereby strengthening the trust between healthcare providers and patients.

### 2. Electronic Health Record (EHR) Management

The DPDP Act strengthens patients' rights in the management of Electronic Health Records. Patients, as data principals, now enjoy the

right to access, correct, and erase their health information. Healthcare providers must stop processing data immediately if consent is withdrawn, except where legally mandated. This requires EHR systems to have built-in mechanisms for real-time updates, corrections, and consent management. By enforcing data minimization and accuracy, the Act ensures that only necessary medical details are stored, protecting patients from over-collection and unauthorized disclosure of sensitive health information.

### 3. Clinical Research

In clinical research, the Act places emphasis on explicit patient consent for data usage. Researchers and healthcare institutions must ensure that participation is voluntary and based on a clear understanding of the purpose, risks, and scope of data processing according to the DPDP Act. Sensitive data such as genetic information, diagnostic results, or treatment histories can only be accessed with specific approvals. Documentation of consent and secure handling of records are essential. These requirements foster ethical research practices while maintaining confidentiality, thereby balancing scientific advancement with the protection of individual privacy.

### 4. Telemedicine Consultation

Telemedicine has expanded healthcare accessibility, but it brings risks of data exposure. The DPDP Act requires that all patient interactions through digital platforms be conducted with strong privacy safeguards. Consent for virtual consultations must be documented, and patient information transmitted over telecommunication channels must remain encrypted and secure. Healthcare providers must ensure that only authorized professionals access the data. This framework not only builds patient confidence in telemedicine but also ensures compliance with data protection norms, reducing risks of data leaks during digital consultations.

### 5. Data Storage and Security

Hospitals and research institutes, as data fiduciaries, are obligated to ensure secure storage and protection of patient data. The Act emphasizes data minimization, accuracy, and confidentiality. Large healthcare providers, designated as Significant Data Fiduciaries, must appoint Data Protection Officers to oversee compliance. Medicolegal records, including autopsy reports, forensic lab findings, and toxicology data, require strict chain-of-custody protocols, which are increasingly maintained through digital platforms like MEDLEAPR.[16] These measures safeguard sensitive health and forensic data from unauthorized access, leaks, or tampering, ensuring accountability in data management.

### 6. Data Breach Handling

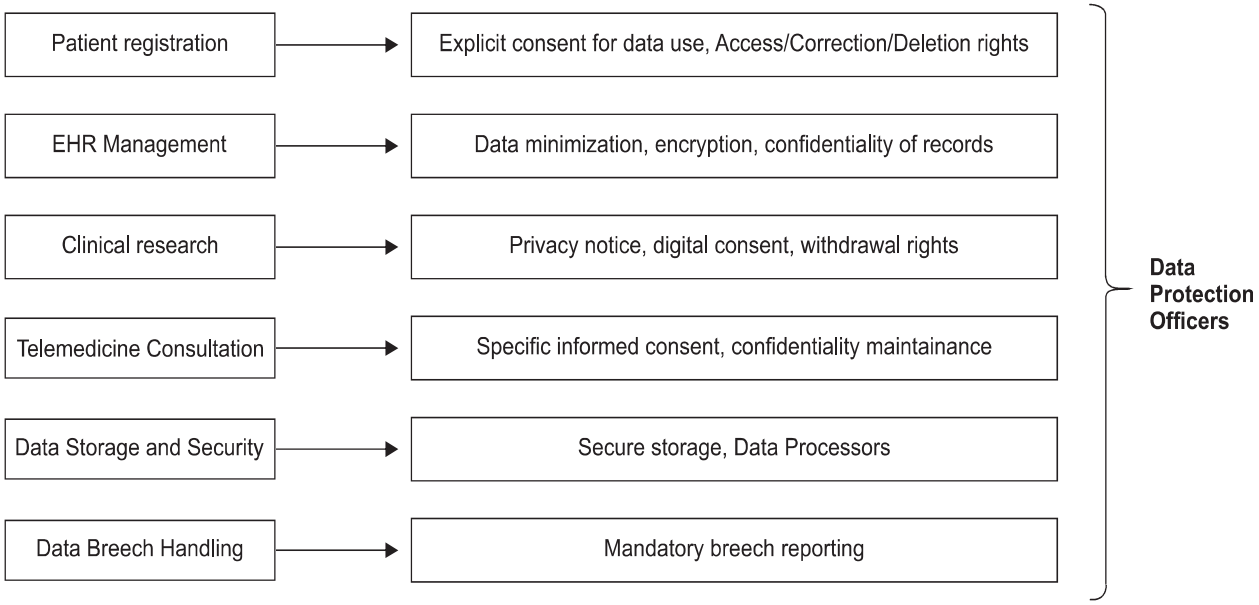


**Figure 1:** Workflow of Data Privacy in Hospital Administration under the DPDP Act, 2023

The DPDP Act imposes strict responsibilities on healthcare institutions in cases of data breaches. Any unauthorized access, leak, or misuse of health records must be reported both to the Data Protection Board of India and to affected patients without delay. Institutions are required to investigate breaches, document corrective measures, and ensure transparency. Cross-border transfer of patient data is restricted only to countries approved by the Central Government. Limited exemptions exist for emergencies, such as epidemics, but safeguards remain necessary. These provisions ensure swift response and accountability in breach scenarios.

## RECOMMENDATIONS

To ensure the prevention of data breaches, every hospital administration should establish a dedicated Medical Records Department overseen by a trained Medical Records Officer. All data handling, storage, and transfer processes must be carried out with utmost precision. In the case of medicolegal records, it is critical to maintain a chain of custody, particularly for documents such as Medico-Legal Case (MLC) files, Forensic Science Laboratory (FSL) reports, and post-mortem reports. Several hospitals have already adopted MEDLEAPR,[16] a digital platform designed to ensure secure transfer and tracking of medicolegal records, and its implementation should be extended to more institutions to strengthen accountability and transparency.

In compliance with the DPDP Act, 2023, healthcare institutions must also appoint trained Data Protection Officers (DPOs) to safeguard personal and sensitive health information.[1] Additionally, hospitals should adopt robust access control mechanisms, ensuring that only authorized personnel can view or process sensitive records. Regular audits and compliance checks must be mandated to identify vulnerabilities and enforce corrective measures.

**Other key recommendations include:**

- **Data Encryption:** All patient data, both in transit and at rest, should be encrypted to prevent unauthorized access.
- **Role-Based Access:** Implement strict role-based access systems so that medical and administrative staff only access data relevant to their duties.
- **Awareness & Training:** Conduct regular training for healthcare staff on data privacy, cybersecurity practices, and medico-legal obligations.
- **Digital Infrastructure Upgradation:** Hospitals should invest in secure electronic medical record (EMR) systems that are compliant with national and international data security standards.
- **Incident Response Protocols:** Establish a clear protocol for responding to data breaches, including mandatory reporting, mitigation strategies, and communication with affected patients.
- **Learning from Global Best Practices:** India can take cues from countries like China and Singapore, which enforce strong digital governance, advanced cybersecurity frameworks, and continuous monitoring systems to protect personal health data.

By combining strong legal frameworks with institutional readiness, technology-driven safeguards, and well-trained personnel, India's healthcare sector can ensure patient trust while complying with constitutional protections under Article 21 and the requirements of the DPDP Act, 2023.

## CONCLUSION

The DPDP Act, 2023 is a progressive step towards building a robust data protection regime in India. In healthcare, it will not only enhance patient trust and safety but also establish medico-legal accountability for institutions handling sensitive health data. However, successful implementation will depend on strengthening digital infrastructure, increasing awareness, and balancing privacy with innovation in medical research and telehealth.

## REFERENCES

1. Government of India. The Digital Personal Data Protection Act, 2023. No. 22 of 2023. New Delhi: Ministry of Law and Justice; 2023. Available from: https://www.meity.gov.in
2. DLA Piper. Data Protection Laws of the World: China. 14th ed. London: DLA Piper LLP; 2025. Available from: https://www.dlapiperdataprotection.com/

**3.** Khanna V, Kotwal A. 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;22:381.doi:10.1186/s12982-025-00757-6.

**4.** Komnenic M. Top 10 Biggest Data Breaches of All Time [Internet]. Termly; 7 Jan 2025 [cited 2025 Sep 15]. Available from: https://termly.io/resources/articles/biggest-data-breaches/

**5.** Bharatiya Nyaya Sanhita, 2023 (No. 45 of 2023). Gazette of India, Ministry of Law and Justice. New Delhi, 25 December 2023.

**6.** Bharatiya Nagarik Suraksha Sanhita, 2023 (No. 46 of 2023). Gazette of India, Ministry of Law and Justice. New Delhi, 25 December 2023.

**7.** Bharatiya Sakshya Adhiniyam, 2023 (No. 47 of 2023). Gazette of India, Ministry of Law and Justice. New Delhi, 25 December 2023.

**8.** Government of India. The Information Technology Act, 2000. No. 21 of 2000. New Delhi: Ministry of Law, Justice and Company Affairs; 2000. Available from: https://www.indiacode.nic.in

**9.** Government of India. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. New Delhi: Ministry of Communications and Information Technology; 2011. Available from: https://www.indiacode.nic.in

**10.** Board of Governors in supersession of the Medical Council of India. Telemedicine practice guidelines: enabling registered medical practitioners to provide healthcare using telemedicine. New Delhi: Medical Council of India; 2020 Mar 25.

**11.** Govt of India. Ayushman Bharat Digital Mission (ABDM) [Internet]. National Portal of India; [Accessed: 2025 Sep 16]. Available from: https://www.india.gov.in/spotlight/ayushman-bharat-digital-mission-abdm

**12.** BharatEHealth. BharatEHealth: AI-powered EHR and Telemedicine Platform [Internet]. BharatEHealth; c2025 [cited 2025 Sep 16]. Available from: https://bharatehealth.com/

**13.** MediBank. MediBank: Cloud-based Electronic Health Records Platform [Internet]. MediBank; c2025 [cited 2025 Sep 16]. Available from: https://medibank.in/

**14.** Healthray. eHospital: Hospital Information Management System (HIMS) [Internet]. Healthray; c2025 [cited 2025 Sep 16]. Available from: https://www.healthmedtechnologies.com/ehospital.html

**15.** Imperva. Cybersecurity threats. [Internet]. Imperva; [Accessed: 2025 Sep 16]. Available from: https://www.imperva.com/learn/application-security/cyber-security-threats/

**16.** Jain R, Bansal GS. MedLEaPR – first step towards ICT enabled integrated justice delivery system. Informatics. New Delhi: National Informatics Centre, Govt of India; 2013 Apr;21(1):12-14.