

The Evolution and Importance of DPDP Act in Healthcare in the Present Context of Healthcare Development

C.L. Avadhani

Research Scholar, B.Sc., AMIE, MBA, M.Phil, MMM, PGDFM, PGDMM, PGDBA, PGDHRM, PGDPM & IR, PGDIPR, DLL, LLM, Project Consultant, Ph.D. Research Scholar, Department of Business Administration, Annamalai University.

Abstract-- The rapid growth of the healthcare sector has increased the collection, storage, processing, and exchange of patients' personal and medical information, making data privacy and security essential concerns. As India's healthcare landscape undergoes a wide increase of digital transformation and patient data has been made as a critical asset in healthcare facility. The Digital Personal Data Protection (DPDP) Act, 2023, represents an important development in India's legal framework for protecting digital personal data. Every healthcare facility and clinical establishment that keeps a digital patient record is a Data Fiduciary under this Act. Healthcare data is considered to be sensitive personal data under Sec 3(c) of the DPDP Act. The aim and objective of this article is to examine the evolution, significance, and importance of the DPDP Act in the context of contemporary healthcare development, with particular emphasis on the responsibilities of healthcare providers, hospitals, clinics, and healthcare professionals. It discusses key provisions relating to informed consent, purpose limitation, data minimization, data accuracy, retention of medical records, security safeguards, breach notification, and patients' rights to access, correct, and erase personal data, subject to applicable legal obligations. The electronic health records, third-party data sharing, cloud-based healthcare systems, digital patient communication, and staff handling of confidential information are the significant challenges arising in the Healthcare sector. The importance of institutional preparedness, employee training, effective grievance-redressal mechanisms, and appropriate technical and organizational safeguards. The analysis indicates that effective implementation of the DPDP Act can strengthen patient trust, improve accountability, and promote responsible digital healthcare practices. Proactive compliance is therefore essential for healthcare institutions to protect patient confidentiality, reduce legal and reputational risks, and support secure and sustainable healthcare development in India.

Keywords-- Digital Personal Data Protection (DPDP) Act, 2023, healthcare data privacy, sensitive personal data, Data Protection Board of India, healthcare providers, healthcare professionals, electronic health records, Data Fiduciaries, data breach notification, patient rights, data security safeguards, NABH and JCI accreditation, medical record retention, regulatory compliance.

I. AIM AND OBJECTIVE

The aim and objective of this article is to examine the evolution, significance, and importance of the DPDP Act in the context of contemporary healthcare development, with particular emphasis on the responsibilities of healthcare providers, hospitals, clinics, and healthcare professionals.

II. INTRODUCTION

India's Digital Personal Data Protection Act, 2023 (DPDP) is the country's first comprehensive data protection law passed by Parliament in August, 2023 and is enforceable from May, 2027, it governs how personal data must be collected, stored, used and protected by organizations operating in India.

This Act herein after called as DPDP Act is mainly for "healthcare professionals" and "healthcare providers" matters more than it might initially appear. In India, especially infact globally, healthcare is highest-risk categories under DPDP Act. In any Healthcare facility when a patient goes for procedure, every interaction of the patient with healthcare professionals generates personal data such as names, phone numbers, diagnosis, prescriptions, lab reports/results and X-ray films. This data provided by the patient to the healthcare professionals when he visits healthcare facility is personal and sensitive in nature and any breach of this data to a third party, it is not just inconvenience to the patient, it is exposed private health conditions of the patient to "employers, insurers and the public". In an healthcare facility, when a patient approaches an healthcare professional to come out from the ailment, a relationship is built between a patient and healthcare professional on trust; because there cannot be any contract/obligation between the patient and healthcare professional except a trust between the two and the patient have utmost confidence in the healthcare professional that his personal data is not shared by the professional to a third party and at the same time the healthcare professional should induce confidence in the mind of the patient that his personal medical data will not be used/shared with third party under any circumstances.



International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 10, October 2026)

The legal terminology it is nothing but an “implied contract”. In this event the DPDP Act formalizes what the patients have always expected from the healthcare professional, that their information will be handled carefully, used only for the purpose it was given and never shared without their knowledge.

When the Government of India opened up the economy and allowed participation of healthcare professionals and big industrial houses to take part in healthcare sector decade or so back when healthcare was purely under (both state and central) there is a mushroom growth of healthcare facilities that have come up with healthcare sectors as joint ventures with healthcare facilities from developed countries to bring latest technology, technological procedures, equipment, sophisticated equipment, software and machine learning so that to boost the healthcare facilities and give maximum procedure to the patient satisfaction in India. Subsequently the acts that provided NABH by Government of India and JCI, an International Accredited Certificate from India have become the tools that provided to categorize certain facilities with International Standards. NABH namely (National Accreditation Board for Hospitals) JCI (Joint Commission International), the first one being Accreditation Board for Healthcare facilities in India and the second one international recognition for any healthcare facility in the Globe, when a healthcare facility accredited by NABH or JCI to attract international patients from other parts of the Globe. The DPDP Act that is going to be enforceable from May 2027, formalizes the expectations of a patient namely that their information will be handled carefully and used only for the purpose it was given on or never shared without their knowledge because the personal information/data has to be handled carefully not only by the healthcare professionals but also the healthcare providers when the people connected with the data information of the patients and should be used for the purpose it was given and never shared without their knowledge, written compliance of the patient or their guardians if the patient is a minor or if there is any legal enforceable order from judiciary. The DPDP Act empowers the “Data Protection Board of India” to investigate complaints and impose penalties of upto 250 crores for significant violations for a clinic, hospital or healthcare facility that is not merely a fine but it is an essential event that can cause irreparable financial and reputational loss. Hence all the clinical establishments/healthcare facilities should prepare themselves to click to the rules and regulations of DPDP Act else after May 2027 when the Act comes into force for non compliance, the healthcare facilities/clinics/hospitals will face the music.

III. LITERATURE REVIEW

There is not much literature on this subject because the Act is passed in the Parliament and a Gazette Notification is issued by the Central Government but still it has not come into force. This Act will come into force in India on or after May 2027. This Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023) and was commenced on 19.11.2023 is pertaining to Hospitals and Healthcare and also to the providers. This is one of the Act that was promulgated by the Central Government through a Gazette Notification and all the state and Union Territories have to endorse the same. The Government has given nearly four years of time to make necessary changes as per the Act in all the Healthcare Facilities in India so that no penalty amounting to Rs. 250 crores (for not compliance of the Act) can be levied. Hence Government has given sufficient time till May 2027 to adopt the rules and regulations that are strictly implemented according to the Act. This Act comprises of nine chapters under the headings preliminary, obligations of data fiduciary, Rights and Duties of Data Principal, special Provisions, Data Protection Board of India, Powers, Functions and Procedure to be followed by Board, Appeal and Alternate Dispute Resolution, Penalties and Adjudication, Miscellaneous.

According to the Act, 2023 to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto. This is one of the important aspects of making a law in healthcare with respect to personal data of the patients and how to protect, if violated by the healthcare facilities or professionals or anybody how to punish.

In my opinion it is better to give an comprehensive idea about the activities of the Act that are beneficial to patients, healthcare providers and professionals I will make an attempt to explain the same. This Act provides in India “who is covered”, what the obligations are?, what patients can now demand” and what happens gets it wrong?”.

“Patient data is among the most sensitive personal data that exists the DPDP Act brings Indian Healthcare into the modern data-protection era-but hospitals that treat it a just another regulatory box-tick will be caught off of guard when the rules are notified and enforcement begins.” – Dr. Namit Gupta, Senior Medico-Legal Expert, Medico Legal Services, New Delhi.

In the article titled “Digital Personal Data Protection Act, 2023 – What it means for Hospitals and Doctors in India” written by Dr. Namit Gupta, Senior Medico-Legal Expert, Medico Legal Services, New Delhi published on 29.06.2026 in www.medicolegalservices.in, it was mentioned that about the Act, “India has attempted Data Protection Legislation before – draft bills in 2018 and 2021 were withdrawn. The 2023 Act is the first to pass parliament. It draws heavily from the GDPR framework but is tailored to India’s context. It applies to Digital Personal Data only (not paper records), and it creates a domestic enforcement authority called the Data Protection Board of India.”

Key features relevant to healthcare through this Act are,

1. Applies to personal data processed within India in digital form, and to digital data collected outside India if it is used to offer goods or services to individuals in India.
2. Does not distinguish “sensitive” personal data from other personal data as a separate category (unlike the GDPR’s Article 9 or India’s earlier Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011)
3. Establishes consent as the primary legal basis for processing with limited legitimate-use exceptions
4. Creates enforceable rights for Data Principals (patients)
5. Introduces financial penalties through an adjudicatory process before the Data Protection Board

The same article also discussed about the Key definitions such as - Who is What in the healthcare context?

a. Data Principal – The Patient

“The individual to whom personal data relates, in healthcare this is ordinarily the patient where the patient is a minor (under 18) or a person with a disability requiring a guardian, the consent of the guardian is required.

b. Data Fiduciary – The Hospital/Healthcare Facility or Doctor/Healthcare Professional

“Any person who processes personal data on behalf of a Data Fiduciary. If your hospital uses a cloud-based Electronic Medical Records (EMR) platform or stores patient data on a third-party server, that vendor is your Data Processor. The Hospital (Data Fiduciary) remains responsible for ensuring the processor follows the Act – this must be addressed through a data processing agreement.

c. Significant Data Fiduciary

“The Central Government may designate certain Data Fiduciaries as Significant Data Fiduciaries based on the volume and sensitivity of data they process, the potential risk to the rights of Data Principals, national security concerns, or public order implications. Large multi-specialty hospitals, hospital chains, and health-tech platforms are the most likely candidates in healthcare. Significant Data Fiduciaries face additional obligations including mandatory appointment of a Data Protection Officer (DPO) resident in India and mandatory Data Protection Impact Assessments.”

In the same article the authors presented the definition of Personal Data in the Healthcare context,

“The Act defines Personal Data as any data about an individual (patient) who is identifiable by or in relation to such data in Healthcare is called Personal Data. A Patient’s name and UHID (Unique Hospital ID) together constitute the personal data of the Patient.

It also include a diagnosis, prescription, lab results, imaging report or discharge summary attached to an identifiable patient is called the personal data of that particular patient. Also an IP address or device ID that can be linked to an identified patient is also called personal data. A photograph from a clinical record is also called as personal data. The other important aspect of this Act is “De-identified data is excluded – if data is truly anonymised so that no individual can be identified from it directly or in combination with other data, it falls outside the Act’s scope. Hospitals/Healthcare facilities that use patient data for research or analytics must genuinely anonymise it to claim this exclusion.

Data Type	Personal Data?	Notes
Name+Diagnosis	Yes	Clearly identifiable – core personal data
Anonymised aggregate statistics	No	Excluded if truly de-identified
Lab result with patient ID	Yes	Identifiable via hospital record
CCTV footage of hospital	Yes (if faces visible)	Biometric data; identifiable individuals

In the same article, the author mentioned about **“Obligations on Hospitals as Data Fiduciaries”**,

a. Purpose Limitation: A hospital/healthcare facility may process a patient’s personal data for a specific purpose for which consent was obtained from the patient or if the patient is a minor from the guardian as the case may be. It is also mentioned in the Act that by virtue of access to the personal telephone number of the Patient or Guardian, an healthcare facility or professionals cannot sent any promotional messages without specific consent.

b. Data minimization: The healthcare facilities/ professionals/providers are authorized to collect the data of the patient that is necessary for the procedures or stated purpose. The other important aspect is the healthcare facilities who are asking about Aadhaar Number, Marital Status or income details are only for the purpose of to register the name of the patient for an outpatient consultation, when the patient is not required to be admitted into the healthcare facility.

Data Fiduciaries must make reasonable efforts to ensure that patients personal data is accurate and updated instead of making incorrect entries in patients records. In the personal data, the healthcare facilities are also required to collect data regarding “wrong drug allergy, incorrect date of birth, wrong diagnosis code – are not just clinical risks but they are now with the introduction of this Act became potential compliance issues.

c. Storage limitations: According to Indian Legal System personal data of the patient must not be retained beyond the period of limitations (3years) for the purpose for which it was collected unless retention is required by law. Once the period of limitation is over the healthcare facilities are at liberty to retain or remove the details.

d. Security safeguards of the data: According to the existing legal system and the Digital Personal Data protection Act data of a patient must be given organizational measures from, “to prevent personal data breaches meaning encrypted storage and transmission of EHRs, role based access controls (not all staff) should be able to give all records, audit trails, end point security and periodic security assessments though the minimum security standards for healthcare records are not yet defined by rule must be reasonable – which quotes and the board will bench mark against sector norms.

e. Accountability and breach notification: When a personal data of the patient is accessed, a hacker accessing the EHR, an employee emailing the third patients record to a third party, a server of the computer left unencrypted, the data fiduciary must notify the data protection board and each affected data principal, this notification must be prompt, in accordance with the rules and regulations and timeline and failure to notify such Acts that carries the highest penalty upto 250 crores according to the Act 2023.

f. Consent under the DPDP Act: A written consent must be free, specific, informed, unconditional and unambiguous. The healthcare facilities must provide a notice before or at the time of collecting data as,

- i. What personal data is being collected?
- ii. The purpose of the processing;
- iii. The rights of the Data Principal and how to exercise them;
- iv. The manner in which a complaint may be made to the Data Protection Board;

The notices that are being issued in such situations “clear, plain language, where a patient has limited English language the notice should be available in the patient’s preferred language”. The written consent must be separate from any terms and conditions of agreement – it means buried consent clauses in registration paper work will not satisfy the Act.

The patient or guardian or who gives the written consent on behalf of the patient and the same person who gave the consent has the right to withdraw without any hindrances and the healthcare facility is not authorized if consent is withdrawn to delete the records required by law. However the healthcare facilities must stop further processing beyond the legally mandated retention.

g. Sensitive health data: How DPDP differs from GDPR: The important structural difference between DPDP Act and GDPR, the Indian Legal System does not create a separate specific category for sensitive personal data (health, genetic, biometric, religious, political data). Under Article 9 of GDPR, health data of a person is his/her personal data subject to the same rules. There is no statutory standard for it, though it is very likely that the rules and significant data fiduciary designation process will create sector specific obligations for healthcare.

According to the information technology (reasonable security practices) rules, 2011 did list health information as “sensitive personal data”, requiring heightened safeguards. Those rules under that Act, continue to apply to body corporate until the government specified otherwise, creating an overlapping compliance obligation for hospitals interim period. Under this Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, it was mentioned that, “8. Reasonable Security Practices and Procedures.— (1) A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies. (2) The international Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" is one such standard referred to in sub-rule (1). (3) Any industry association or an entity formed by such an association, whose members are selfregulating by following other than IS/ISO/IEC codes of best practices for data protection as per sub-rule(1), shall get its codes of best practices duly approved and notified by

the Central Government for effective implementation. (4) The body corporate or a person on its behalf who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified under sub-rule (3) shall be deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried out by an auditor at least once a year or as and when the body corporate or a person on its behalf undertake significant upgradation of its process and computer resource.”

h. Cross border data transfer restrictions: The DPDP Act, allows the Central Government to restrict the transfer of personal data of a patient to countries or territories outside India. In this context, transfers will be permitted to notified countries and transfer of records to non notified countries will require specific justification or approval. For healthcare facilities using Cloud EMR. ON the otherhand transfer of information to non notified countries will require specific approvals by accepting justification for the purpose for healthcare facilities using Cloud EMR system where data may be stored on services outside India. This is a critical contract with International cloud vendors must be reviewed for data residency provisions. However, the Indian Health Sector may eventually required to store Patient’s data on servers located in India. Data retention and interaction with existing Medical Records rules,

“The DPDP Act introduces a storage limitation principle, but it also recognizes that legal retention obligations override that principle. India's existing rules on medical records retention include:

- Clinical Establishments (Central Government) Rules, 2012: Maintain medical records for a minimum of 3 years from the date of treatment
- Maharashtra Medical Council: 7 years for patient records
- Karnataka: Minimum 5 years
- Consumer Protection Act, 2019: Limitation period for complaints is 2 years from the cause of action, so records supporting a potential dispute should be retained for at least this period beyond the date of treatment
- Minor patients: Records should be retained until the patient reaches 18 + 3 years (or until local limitation periods expire for any potential claim by the minor on reaching majority)

- ICU and surgical records: Many hospital policies specify 10 years; given litigation risk, this is prudent

The DPDP Act does not override these retention requirements. What it adds is an obligation to delete or anonymise data that is no longer required to be retained under any applicable law or for the stated purpose. In practice, hospitals must map their data categories, apply the longest applicable retention period, and build a data deletion process for records that have passed that period.”

i. Rights of Patients under data principals under DPDP Act: Under this Act, any patient may request a summary of the personal data from an healthcare facility that holds about them and information on its processing, including the identities of data fiduciaries and data processors with whom the data was shared.

j. Right to correction and erasure: The Patients of that particular records may request correction of inaccurate or misleading personal data and completion of incomplete data and erasure of data that is no longer of necessary for the purpose it was collected or where the patient has withdrawn consent and no obligation of legal retention applies.

k. Right to grievance redressal: Every data fiduciary have a published grievance mechanism. If the grievance is not resolved to the satisfaction of the patient/guardian, the patient/guardian is at liberty to approach to data protection board for the same.

l. Right of nomination: A data principal (patient) may nominate another individual to exercise his/her rights as per the Act in the event of death or incapacity – relevant in the clinical context where a patient’s next of kin may need to access or act on the patient’s data.

The functions of the Data Protection Board and Penalties: As per the Act, 2023 the Data Protection Board of India which is adjudicatory body, will hear complaints from data principals and can impose fines/penalties under schedule 1 of the Act.

- Failure to notify a personal data breach: Up to ₹250 crore
- Failure to implement adequate security safeguards: Up to ₹200 crore
- Breach of obligations regarding children's data: Up to ₹200 crore

- Breach of additional obligations by Significant Data Fiduciaries: Up to ₹150 crore
- Other violations of the Act or Rules: Up to ₹50 crore

The action of the Data Protection Board is civil in nature because it is quasi-judicial in nature and can impose penalties and the penalties imposed by the board are significant enough to be existential for small mid-sized healthcare facilities but it can be upto a maximum of 250 crores.

m. Practical Compliance Checklist for Hospitals: Large Hospitals and Hospital Chains

- Conduct a data mapping exercise: What patient data do you collect, from where, for what purpose, stored where, shared with whom?
- Review and update patient consent forms and registration documents to meet the DPDP Act's consent standard
- Draft a clear, multilingual Privacy Notice to be displayed at reception and on your hospital website
- Audit your EMR vendor and all other Data Processors — enter into formal data processing agreements that bind them to Act compliance
- Implement breach detection and notification protocols (internal escalation, Board notification, patient notification)
- Prepare for possible designation as a Significant Data Fiduciary — identify a potential DPO candidate and conduct a Data Protection Impact Assessment
- Review cloud and cross-border data transfer arrangements
- Train clinical and administrative staff on data-handling obligations

Small Clinics and Solo Practitioners

If you use a digital system at all — an appointment app, a messaging service to share prescriptions, a WhatsApp group for patient follow-ups, an online booking system — you are a Data Fiduciary. Your obligations under the Act are the same in principle, even if the scale is different. At a minimum, small practices should: obtain valid consent before collecting patient data digitally, use password-protected devices and encrypted storage, not share patient data over unsecured channels, and have a basic mechanism to respond to patient access requests.

IV. DISCUSSIONS AND ANALYSIS

Government of India to protect the rights of the Patients/healthcare providers/healthcare professionals because Government has taken healthcare on priority basis and also in the present environment of digitalization of records and introduction of Information technology/Artificial Intelligence/Machine learning taken initiative and made an attempt to bring out country's first comprehensive Data Protection Law which was passed by Parliament in August, 2023 that is enforceable starting May, 2027 and this Act, governs how Personal Data must be collected, stored, used and protected by healthcare organizations operating in India. This law after enforcement in 2027 matters more to the healthcare providers facilities and professionals that it might initially appear; in the present environment healthcare is among the highest categories under DPDP Act. The Government of India has given nearly three to four years of time to the healthcare organizations to implement the provisions of the Act and make necessary arrangements in healthcare facilities in accordance with the Act so that they can avoid penalty if not properly implemented. Once the Act comes into force the Government/Judiciary have got armory to punish the guilt and impose fine to the tune of 250 crores. Off late Government of India has recognized the Personal Data of a Patient and its importance and how to safeguard the same except in certain circumstances where directions from the Government or from the Judiciary are pending. The DPDP Act formalizes what the patients have expected so far, the main thing is the Personal Data/Information of a Patient is his/her property that cannot be shared by the healthcare facilities/providers/professionals except where there is directions from the respective organizations who are authorized to do so. In short, healthcare becomes a Global Trade and people are coming to India or going to other places in need of better healthcare procedures for their ailments in such circumstances, the personal data/healthcare records that are in Electronic Form (HER) have to be transmitted to the place where the patient intends to take further procedures or advanced treatment. In such cases, the Personal Data of the Patient should have to be transmitted in Digital Form from the home country to the healthcare facility of that country where the patient intends to have further treatment. Hence in these circumstances, the DPDP Act empowers the Data Protection Board (established under this Act) of India to investigate complaints and impose penalties of upto 250 crores for significant violations of the Act, for a clinic or healthcare facility and this is not merely a fine but it is an existential event that can cause not only irreparable financial loss but also the reputation of the facility.

Hence, it is obligatory on the part of the healthcare facilities big or small to comply with the provisions of the Act before May, 2027, wherein the enforcement of the Act will come into play.

Following are the specific risks to doctors and facilities face under DPDP Act violations:

1. *Patient consent on website:* If a clinic/healthcare facility's has a contact form, an appointment booking widget, or any filed where a patient enters their name, phone number or email address, you are collecting personal data. Under the DPDP Act, this requires a lawful basis – and in healthcare, valid consent is the primary route. That consent must be specific, informed, and freely given (no pre-ticked boxes). Most clinic websites collect this data without a compliant consent banner, a privacy notice, or a mechanism for patients to withdraw consent. Each such collection is a potential violation.

2. *WhatsApp Patient Communication:* With the introduction of healthcare technology in healthcare sector, the total phase of the healthcare has changed a lot. It is so because to minimize the clinical work, to reduce storage of problems of the patients that are to be preserved for a minimum period under Indian Legal System. In addition even after the procedure is over and patient is discharged the healthcare facility/clinics may have to contact the patient to give additional instructions during sojourn, hence they have to use the personal WhatsApp number or phone number for the purpose. In this regard, the healthcare facilities/clinics will obtain a consent from the patient to do so. The Patients Phone number/contact number during registration/admission at the reception counter will obtain the patients consent to make use of the phone number/WhatsApp to transmit any important message/information pertaining to the Patient's ailment/suggestions. For this purpose if the DPDP Act comes into force the healthcare facilities/hospitals have to invariably obtain written consent for the same, else it is punishable under new Law.

3. *Review collection and testimonials:* The Healthcare Facilities/Hospitals asking a patient to leave a google review and to read their experience or provide their suggestions to better improve the healthcare facilities/procedures. Now under the coming DPDP Act, "consent for the specific use must be captured separately from any consent obtained for clinical purposes only." A patient who consented to receiving appointment reminders has not thereby consented to appearing.

4. *Third party data sharing:* As already mentioned above, sometimes the Patient wants to change the healthcare facility/hospital within the country or outside the country it is necessary for the receiving facility to get the past data of the patient to continue the procedure/change the procedure for better results. That is why presently healthcare data is maintained in the form of Electronic Health Records (previously Medical Health Records). The clinics/facilities have got an opportunity to remove the Health Records of a Patient once the statutory legal period is over of in circumstances where judicial compliance is there.

5. *CRM Systems and Databases:* Many clinics maintain patient information in Excel sheets, Google Sheets, or third-party CRM platforms. Under the DPDP Act, Data Fiduciaries have obligations around the security of data they store, the retention period, and deletion when no longer needed. A database maintained indefinitely without adequate security is a compliance failure waiting to be exposed. The Act also requires that personal data be used only for its collected purpose: contact details for reminders cannot be repurposed for marketing without fresh consent.

6. *Employee Handling of Patient Data:* Clinic staff routinely access patient records, handle appointment systems, and use WhatsApp for patient communication, often from personal devices. The DPDP Act holds the clinic responsible for data breaches caused by its employees. An untrained receptionist who saves a patient's lab report to her personal phone creates direct legal exposure. Compliance requires not just policies, but documented training - of the kind Starlex Consultants has delivered to over 5,000 professionals across India.

7. *Children's Data:* Pediatric clinics and any practice collecting data from patients under 18 face heightened obligations. Processing a child's personal data requires verifiable parental or guardian consent. Clinics must implement age-verification mechanisms and must not subject children's data to behavioural monitoring or targeted advertising under any circumstances. Practices that treat minors without separate consent procedures are almost certainly non-compliant.

8. *Data Breach Notification:* Under the DPDP Act, if a data breach occurs - if patient records are accessed by an unauthorised person, a device is stolen, or a vendor suffers an incident - the clinic must notify the Data Protection Board of India and the affected patients. Most clinics have no breach response protocol: no designated person, no process, and no template.

Under the DPDP Act, failure to notify can constitute a separate violation with penalties upto INR 200 crores. (written by Mimansa Ambastha, Managing Partner, Starlex Consultants LLP in <https://www.doublesure.health/services/dpdp-compliance-healthcare>)

It is quite appropriate to mention five questions for doctors and clinic owners framed for the benefit of the readers by Mimansa Ambastha, Managing Partner, Starlex Consultants LLP which are most relevant appropriate with due respects I am reproducing them for the benefit of readers without any change.

1. Is my clinic legally required to comply with the DPDP Act?
2. What is the penalty for non-compliance with DPDP for a healthcare practice?
3. Do I need a separate consent form for collecting patient data on my website?
4. If I use a WhatsApp Business account to communicate with patients, does DPDP apply?
5. What is a Data Processing Agreement and do I need one with my marketing agency?

I am herewith discussing about the importance of the provisions of the Act:

Complaint Mechanism Notice: Under Section 5(1)(iii) of the Act, "transparency goes beyond just listing what data you collect; you must clearly explain the complaint mechanism DPDP mandates. This means your privacy notice must explicitly inform the Data Principal of the DPDP grievance process, specifically detailing how they can escalate issues to the Data Protection Board of India if their concerns aren't resolved internally. It ensures users aren't just aware of their rights but also know the exact data protection board complaint procedure to seek a remedy."

The important affect of this Complaint Mechanism Notice is

a. *Executive Takeaway:* The privacy notice is incomplete without a clear escalation path to the Data Protection Board. Omitting this specific disclosure is a direct violation of Section 5, rendering the notice (and subsequent consent) invalid.

b. *Why this matters:*

- Missing complaint details renders the privacy notice non-compliant, potentially invalidating the consent obtained based on that notice.
- Clear escalation paths reduce legal friction by ensuring users understand the regulatory hierarchy (Fiduciary first, then Board).

c. What “Good” looks like:

- A privacy notice that includes a dedicated section titled 'Grievance Redressal' or 'Complaints' with clear instructions on contacting the Board.
- Digital links or prescribed forms for filing complaints to the Board are easily accessible within the notice

While issuing a Complaint Mechanism Notice, by the concerned persons they should keep in mind the questions and the respective answers in their complaint notice so that the notice will be seen in proper perspective by the Data Protection Board to take cognizance of the notice;

What complaint mechanism must be mentioned in privacy notice?

Section 5(1)(iii) mandates that the notice must inform the Data Principal of the manner in which they may make a complaint to the Data Protection Board of India, in such manner as may be prescribed.

How to file complaint with Data Protection Board of India?

The Data Protection Board of India operates as a digital office. Complaints regarding personal data breaches or breach of obligations can be made to the Data Protection Board of India in the form and manner prescribed, typically via an online mechanism.

What information about complaints must be in privacy notice?

The notice must specifically include the manner in which the Data Principal may exercise their rights and the manner in which they may make a complaint to the Data Protection Board of India.

Who can file complaints under DPDP act?

A Data Principal can file a complaint with the Data Protection Board of India in respect of a personal data breach or a breach in observance of obligations by a Data Fiduciary or Consent Manager.

What is the complaint process for data protection violations?

The Data Principal must first exhaust the opportunity of redressing their grievance with the Data Fiduciary (Section 13(3)). If unresolved, they may then approach the Data Protection Board of India.

How long does Data Protection Board take to resolve complaints?

The Act does not specify a fixed timeline for the Data Protection Board of India's resolution, but it requires the Data Fiduciary to respond to grievances within a prescribed period (typically 90 days) before the Data Protection Board of India is approached.

Can data principals complain directly to authorities?

No, Section 13(3) explicitly states that a Data Principal shall exhaust the opportunity of redressing her grievance with the Data Fiduciary before approaching the Data Protection Board of India.

What are the grounds for filing DPDP complaints?

Complaints can be filed for a personal data breach or a breach in observance of obligations by a Data Fiduciary in relation to personal data or the exercise of Data Principal Rights.

At this juncture it is appropriate to mention the contents of an article “DPDP Act Compliance in Hospitals: What Every Hospital Leadership Team should know about the DPDP Act” written by Nitin Ray published on 20.07.2026 in www.ruleexpert.com/dpdp-act-compliance-in-hospitals-guide

In this aspect, in the article it is categorically mentioned regarding DPDP Act compliance in hospitals protecting patients data and ensuring compliance, it is mentioned that, “DPDP Act Compliance in Hospitals is no longer a peripheral IT concern, it is a foundational pillar of modern clinical governance and Patients trust”. The Digital Personal Data Protection (DPDP) Act which is yet to be enforceable coupled with the rules under the Act, 2025 shows India’s comprehensive framework in safeguarding personal data of a patient with the phased enforcement of the Act, is under way. This is because the government of India has given ample time of nearly four years for the healthcare organizations to comply with the same and avoid penalties and punishments. Hence all the healthcare facilities and hospitals earnestly put their efforts in comply with Act and subsequent rules for the benefit of hospitals and the patients. For this one should have iron hand and determined mind in strictly applying the compliance, because this Act involving potential financial penalties upto 250 crores for each violation and more importantly if once imposed the fine or penalty, the healthcare facility will lose its sanctity, recognition and name and fame, which is more important in this sector.”

The main important thing in this Act is the Digital Personal Data of a Patient that includes any health related information collected and put into the form of digital should be protected at any cost under any circumstances else it will damage the character, future of the patient thereby the healthcare facility will lose its position in the sector. When one goes deep into the provisions of the Act, it has clearly mentioned specific responsibilities and the role to be played by the healthcare providers/facilities/professionals/data entry and keeping personnel and the Patients. That is why the government of India has given such long time so that a breathing time is given to the healthcare facilities/providers/hospitals to comply the same without any lapses.”

Once this DPDP Act comes into force, compliance in hospitals demands shift from adhoc data management through a systematic compliancy first culture. By enforcement of this Act following are the benefits for the healthcare facility:

1. Consent management excellency
2. Granular consent: It means moving away from the present position of blanket consent and shifting towards specific authorization for different processes such as treatment vs research vs marketing.
3. Revocability: The Act provides to the patients to withdraw their consent at any time instead of endless time by explaining the reasons for the same.
4. Rigorous data minimization: DPDP Act compliance in healthcare facilities/hospitals “requires the disciplined approach collect only what is strictly necessary from the patient/guardians for procedures and billing purpose. If healthcare record is no longer required for the specified purpose for which it is collected including judicial obligations, the healthcare facility/hospital must erase the information by intimating the same to the patient.
5. Strengthening Vendor governance: Hospitals/Healthcare facilities will not operate in isolation but have to share the data with diagnostic labs, insurers and healthtech platforms. To make the DPDP Act compliance in its entirety the hospitals/healthcare facilities should make due diligence with the third parties as mentioned with whom they are partnering by keeping in mind,
 - i. Confidentiality in non disclosure:
 - ii. Strict adherence to the hospitals/healthcare facilities security standards and finally
 - iii. mandatory notification protocols to be applied in the event of any breach.

The other important aspect of compliance of DPDP Act provisions is “advanced security safeguards” – The present safeguards that are being used by Software people such as Encryption and Firewalls are no longer enough. On the other hand the DPDP Act mandates reasonable security safeguards such as layered approach or any advanced security safeguards that can make it impossible to trespass into it.

Using Role based access controls (RBAC) only authorized persons can access the patients sensitive files (EHR). The hospitals/healthcare facilities must establish a clear, time tested responsible plan that ensures the healthcare facility/hospitals can report a data breach to the data protection board and affected patients with legally mandated timelines. This comes into force only when the Act is enforceable. Finally in my considered opinion, and knowledge I can strongly say that, “even the most expensive software cannot guarantee DPDP Act, DPDP Act compliance by hospitals and healthcare facilities, if the staff who are involved in maintaining the EHRs cannot take the responsibility of privacy for the purpose the healthcare facilities and hospitals must pay attention and invest on advanced training of the personnel involved in the maintenance and maintaining confidentiality of Electronic Health Records to stop any breach because Data breach is not just a hackers attack, it is just like a healthcare report of a patient to wrong email addresses, by chance, or to the wrong hands by intention.”

According to the Act, the Multispecialty, Super specialty, Chain of hospitals/healthcare facilities, the executive boards of that hospitals to put forth a mechanism to evaluate whether the chain of hospitals/healthcare facilities are giving importance to the DPDP Act and should appoint a DPO to look after the activities of the healthcare facility. It is not that much easy to implement the provisions of this Act because Legacy data silos, operational inconsistency and documenting.

V. CONCLUSION

The Digital Personal Data Protection Act, 2023, marks an important step towards strengthening the protection of digital personal data in India, particularly in the rapidly evolving healthcare sector. The increasing use of electronic health records, digital consultation platforms, cloud-based storage systems, and technology-enabled medical services has made the protection of patients’ personal information a fundamental responsibility of healthcare institutions.

The analysis presented in this article highlights the importance of informed consent, purpose limitation, data minimization, appropriate security safeguards, accountability, and effective grievance-redressal mechanisms in maintaining patient confidentiality and trust.

The successful implementation of the Act requires hospitals, clinics, healthcare professionals, and associated service providers to adopt systematic data protection practices rather than treating compliance as merely a legal formality. Regular security assessments, appropriate access controls, secure data-sharing arrangements, employee training, and clearly defined procedures for responding to data breaches are essential components of effective compliance. Healthcare institutions must also ensure that patients understand their rights and that personal information is processed only for lawful purposes, subject to applicable legal requirements.

Although implementation may present challenges, particularly for smaller healthcare facilities and organizations managing legacy records and complex digital systems, proactive preparation can reduce legal and reputational risks while improving institutional accountability. Ultimately, the significance of the DPDP Act extends beyond regulatory compliance: it supports a healthcare environment in which technological advancement is accompanied by respect for privacy, confidentiality, and individual rights. Effective implementation of its applicable provisions can contribute to a more secure, transparent, trustworthy, and sustainable digital healthcare ecosystem in India.

The DPDP Act of 2023, which is going to be enforced from May, 2027 is not an hurdle in healthcare systems, on the other hand it acts a catalyst. Due to the availability of healthcare information in internet and other sources the patients are getting more informative with respect to healthcare and the relevant information and patients are becoming increasingly aware of their rights and duties of the professionals and healthcare facilities. For those who want to question the compliance of healthcare in healthcare facilities are the providers or the professionals, the patients will have every right and authority to question the same on the erring personnel and even get compensation for the loss and punishment to the guilty.

Hence it is obligatory and essential on the part of healthcare facilities/providers/professionals to comply the same in toto before the deadline of 2027. Failing which, the maximum penalty on the facility is around 250 crores. Offlate the Government of India has rightly identified the drawbacks of the healthcare laws and how the patients are bullies for their ignorance. Finally in my opinion, it is the duty of healthcare providers and facilities to publicly made it appear with respect to the essentials of DPDP Act 2023. In addition, the healthcare providers should also make it known the provisions of DPDP Act to all the people concerned in healthcare so as to avoid any penalty.

REFERENCES

- [1] DPDP Act compliance in hospitals: What every hospital leadership team should know about the DPDP Act – Nitin Ray – 20-06-2026 – Ruleexpert.com
- [2] Doctors & Hospital Data & DPDP – DPDP compliance for healthcare & hospitals – Dr. Prashant Mali – February 01, 2026 – www.dpdpa.com
- [3] The Digital Personal Data Protection Act 2023: Implications for mental healthcare practice in India – Manik Inder Singh Sethi – Narayana Manjunatha – Naveen Kumar Channaveerachari, Tanmoy Chakraborty, Suresh Bada Math, Chittaranjan Andrade – Indian Journal of Psychological Medicine
- [4] The Digital Personal Data Protection Act, 2023 – Act No. 22 of 2023
- [5] Digital Personal Data Protection Act, 2023 – What it means for hospitals and doctors in India – Namit Gupta – June 29, 2026 – www.medicolegalservice.com
- [6] When a patient files a DPDP Complaint Against a Hospital: What actually happens next and why most hospitals are not prepared – Sujeet Katiyar, Data Privacy, AI Governance & Regulatory Advisor, DPDP Compliance & Implementation – Healthcare Data Governance – www.linkedin.in
- [7] Compliance Mechanism Notice Requirements DPDP Act section 5 – Watchdog Security
- [8] DPDP Compliance for hospitals : Patient Records, ABDM and the retention conflict – Sarthak Kalucha – 30 sept 2026 – www.consentos.in
- [9] What is the DPDP Act and why does it matter for healthcare? – Mimansa Ambastha, Managing Partner, Sarlex Consultants LLP – October 01, 2026 – www.doublesure.health/services
- [10] DPDP Act compliance for hospitals in India 2026: The complete guide for CIOs, Compliance Heads & MDs – Saurabh Gupta, CISM, CIPP/E – www.myitmanager.in
- [11] DPDP act for hospitals & healthcare – What every provider must do before May 2027 – www.lexwin.co.in