Health Data & the DPDP Act—Navigating India's Healthcare Privacy Frontier

Article by Samagra Law, AI & Data Privacy Governance practice desk
Rakhi Shanker Tewari (Partner)
Radhalakshmi. R (Sr. Associate) Shashi Yadav (Associate)

With the Indian government notifying the much-awaited Digital Personal Data Protection Act, 2023 ("**DPDP Act"**) and rules thereunder, patient privacy is no longer just a compliance requirement but a core aspect of ethical healthcare and responsible business practice.

The DPDP Act read with the Digital Personal Data Protection Rules, 2025 ("**DPDP Rules**") creates a data protection framework for all digital personal data, including health data.

I. *What is Health Data?*

Unlike its initial draft, the DPDP Act does not provide a separate category for health data. However, guidance on what constitutes heath data can be taken from the following policies/regulations:

i. Health Data Management Policy under the Ayushman Bharat Digital Mission;[1]
ii. Electronic Health Record (EHR) Standards for India, 2016;[2]

Additionally, the Ministry of Health and Family Welfare had also sought to define health data under its draft legislation Digital Information Security in Healthcare Act, 2018 ("**DISHA**"), resembling the Health Insurance Portability and Accountability Act, 1996 commonly known as HIPAA of the United States of America. This initiative was, however, shelved in favour of a more comprehensive legislation i.e. the DPDP Act.

All the above-mentioned frameworks broadly refer to health data as any information that relates to the physical or mental health of an individual, the healthcare services provided to them, or payments made for such services. It generally includes identifiers that can directly or indirectly link the information to a specific individual, such as demographic details, contact information, medical records, diagnostic reports, treatment histories, and administrative or transactional data.

II. *Health Data Governance under the DPDP Act and DPDP Rules*

Digital health data that includes personal information comes under the purview of the DPDP Act read with the DPDP Rules. Healthcare providers are data fiduciaries[3] and are obligated to process all digital personal data in accordance with the provisions of the DPDP Act. Hence,

[1] Para 4(y), 4(z) & 4(aa) of National Digital Health Mission: Health Data Management Policy available at https://abdm.gov.in/publications/policies_regulations/health_data_management_policy
[2] See 'PERSONAL HEALTH INFORMATION' at page 19 of ELECTRONIC HEALTH RECORD (EHR) STANDARDS FOR INDIA, 2016 available at https://esanjeevani.mohfw.gov.in/assets/guidelines/ehr_guidlines.pdf
[3] Section 2(i) 'Data Fiduciary' of DPDP Act

processing should be for a lawful purpose and for which the patient, i.e. Data Principal,[4] has given consent in the prescribed manner:

i. ***Collection.*** At the time of collection of personal data, a separate written notice in plain and clear language providing itemised description of personal information required and the purposes for which it will be used should be given. Additional information to be included in the notice is: (a) how a Data Principal may exercise their rights; and (b) manner in which they may file a complaint with the Data Protection Board of India ("**Board**"). This is a shift from existing practices under which notices bundled with other terms and conditions were pushed for consent and itemized data type and use was not a requirement.

ii. ***Consent.*** Consent must be free, specific, informed, unconditional and unambiguous that signifies agreement to processing of personal data for specified purposes. The consent provision becomes stricter when obtaining consent for processing of personal data related to children and persons with disability. For processing personal data of a child or a person with disability, the new law requires obtaining verifiable consent from a parent or lawful guardian. They must also verify the identity of the consenting adult using reliable details or virtual tokens (such as Digital Locker Service Provider).[5]

iii. ***Exemptions for processing a child's data***: Processing children's personal data requires verifiable parental consent. However, as per the provisions of the DPDP Act, the central government may notify specific classes of data fiduciaries who are exempt from (a) the requirement to obtain verifiable parental consent and (b) the restriction on tracking or behavioural monitoring of children. Such data fiduciaries may include certain healthcare providers, such as, clinical establishments, mental health facilities, and medical professionals. This is not a blanket exemption. It applies only when the government formally notifies these healthcare providers, and only when the child's data is being processed to deliver essential, lawful health or welfare services in the child's best interest.[6]

iv. ***Data breach of patients***: If a healthcare provider becomes aware of a data breach, they must inform every affected patient of the nature of breach and its likely impact on them. Within 72 (seventy-two) hours of the breach, information regarding breach is also required to be given to the Board clearly explaining the nature of the breach, the potential risks to the patient, steps being taken to resolve the issue, along with the report regarding intimations given to the patients.[7]

v. ***Grievance redressal system***: All healthcare providers and, where applicable, consent managers must publish their grievance redressal system through which patients can submit their grievances. The healthcare provider must respond to grievances received through such published channels within 90 (ninety) days.[8] However, it is important to understand that this 90 (ninety) days period applies only to resolving grievances. It does not extend to situations where a patient seeks to exercise their other rights under the DPDP

[4] Section 2(j) 'Data Principal' of DPDP Act
[5] Section 9 'Processing of personal data of children' of DPDP Act read with Rule 10 'Verifiable consent for processing of personal data of child' and Rule 11 'Verifiable consent for processing of personal data of person with disability who has lawful guardian' of DPDP Rules
[6] Rule 12 'Exemptions from certain obligations applicable to processing of personal data of child' of DPDP Rules
[7] Rule 7 'Intimation of personal data breach' of DPDP Rules
[8] Rule 14 'Rights of Data Principals' of DPDP Rules

Act, such as requesting access to their data, asking for corrections, seeking erasure, or withdrawing consent. These rights-based requests follow a separate framework under the DPDP Act and DPDP Rules. There is no prescribed period for replying to data principal rights requests and data fiduciaries are free to determine their own response time (which should be published on their website) and to ensure compliance with the same.

vi. ***Personal medical data used for research, archiving, or statistical purposes***: Healthcare organisations can avail an exemption from the applicability of the DPDP Act when they process personal health data for research, archiving, or statistical purposes, provided they comply with the Second Schedule of the DPDP Rules[9] and if the personal data is not to be used to take any decision specific to the concerned Data Principal.

Additionally, the DPDP Act establishes a separate category of data fiduciary, called as Significant Data Fiduciary ("**SDF**") based on the scale, volume and sensitivity of the data they process. If healthcare providers such as hospitals and insurance companies are designated as SDF by the central government, due to the processing of huge amounts of sensitive data by them, the following additional obligations will have to be complied with:

i. Appoint a data protection officer who is based in India;
ii. Appoint an independent data auditor to carry out data audit;
iii. Undertake periodic Data Protection Impact Assessment, once in every period of 12 (twelve) months and furnish its findings to the Board;
iv. Conduct due diligence to verify that the technical measures adopted by it do not risk the rights of Data Principals; and
v. Ensure that its personal health data is not transferred outside India.[10]

III. *Best Practices for Healthcare Providers*

It is important for the healthcare sector to comply with the relevant legal provisions and implement a robust framework and practices for safeguarding patient data and other health related information. Healthcare providers such as hospitals, clinics, pharmacies, laboratories, insurance companies or digital platforms, that process any digital health data or information can adopt the following best practices to assure the data protection of all stakeholders-

Obtain valid consent	Patient's consent must be obtained before collecting or using their health data. Such consent must be free, specific, informed, unambiguous and given through clear affirmative action.
Usage of health data for specified purpose only	Patient must be informed about what kind of data is collected, the reason for such collection and the usage of the data.
Clearly inform patients of their rights	Patients must be given a notice in plain and simple language (in English or any other scheduled language). The notice must include the following-

[9] Rule 16 'Exemption from Act for research, archiving or statistical purposes' of DPDP Rules
[10] Section 10 'Additional Obligations of Significant Data Fiduciary' of DPDP Act read with Rule 13 'Additional Obligations of Significant Data Fiduciary' of DPDP Rules

	• Health data being collected; • Purpose of processing such data; • Patient's right to withdraw their consent anytime; • Procedure for grievance redressal; and • Procedure to approach the Board. Providing a notice and obtaining consent are two separate steps. The notice simply informs the patient about what data is being collected, why it is needed, and how they can withdraw consent or file grievances. This notice by itself does not amount to consent. Consent must come through a clear, affirmative action by the patient such as signing a consent section, completing a separate consent form, or giving explicit digital consent. A countersignature on the notice is acceptable only if the document clearly separates the notice from the consent portion and requires the patient to actively indicate agreement. In short, patients must first be informed through the notice, and then must separately and explicitly consent to the processing of their data.
Consent update from patients	If the patient's consent was obtained before the DPDP Act was notified, the aforementioned notice must be sent to such patient. An opportunity to confirm or withdraw their consent should be provided to the patient.
Maintain transparency and control	It must be easy for patients to access, correct, complete or update their data usage by the healthcare provider.
Exercise caution while processing children's data and data of persons with disability	It is mandatory to obtain verifiable consent from a parent/lawful guardian before collecting or using the personal health data of a child or a person with disability. Healthcare providers cannot track, profile or monitor children's behaviour and cannot undertake any activity which may harm their well-being, unless exempted.
Ensure accuracy of data and limit data retention	Reasonable steps must be taken to ensure data accuracy of the patient. This does not mean the healthcare provider must independently verify every detail, but they must put in place practical measures such as asking patients to confirm their information at the time of collection, enabling easy correction requests, and updating records when patients notify them of changes. In this sense, accuracy becomes a shared responsibility: the patient must provide correct information, and the healthcare provider must take reasonable steps to maintain and update it when needed. Similarly, all health data must be deleted after its intended purpose is served or the patient has withdrawn their consent, unless retention is required as per Rule 8(3) of the DPDP Rules or any other law that

	mandates longer storage. This ensures that data is retained only for legitimate, lawful purposes and not beyond what is necessary.
Obligations of data processors	The healthcare provider remains fully accountable for compliance under the DPDP Act. They must engage data processors only through valid contracts and must ensure appropriate security safeguards for all personal data processed by them or on their behalf.
Set up a grievance redressal system	The healthcare provider must prominently publish its grievance-redressal process and contact details, and is required to respond to patient queries within a reasonable period not exceeding 90 (ninety) days
In case of data breach, notify patients and the Board	Affected patients and the Board must be notified of any data breach within 72 (seventy-two) hours of such breach. Such notification must also include details of the breach, potential risks to patients and any protective measures taken.
Implement data protection safeguards	Necessary technical and organizational safeguards must be taken to prevent any breach, misuse or unauthorized access of data. The healthcare provider must monitor any AI or algorithmic system used, to ensure they do not cause harm to the patient's health data.
Appoint a Data Protection Officer	A dedicated point of contact must be made available along with contact information to enable patients to raise any issues related to their health data.

IV. *Way Forward for Healthcare Providers*

The DPDP Act and DPDP Rules mark a pivotal shift in how health data must be protected in India. As digital healthcare expands, providers must prioritise privacy, transparency, and robust data governance. Even before further classifications like SDFs are notified, hospitals, laboratories, insurers, and digital platforms should strengthen internal processes, secure their systems, and align with the new compliance standards. Proactive preparation today will ensure regulatory readiness and help build stronger patient trust in the evolving healthcare ecosystem.

With the coming into force of the Act, Healthcare institutions should conduct readiness assessments, build internal data governance frameworks, and train staff on new compliance requirements to ensure a smooth transition to the new regulatory regime.
