Healthcare & Pharmaceuticals

DPDPA 2023 Implementation Handbook

Digital Personal Data Protection Act, 2023 • India

For hospitals, clinics, telemedicine platforms, pharmaceutical companies, diagnostics labs, and wellness apps.

1. Overview & Applicability

Healthcare entities process some of the most sensitive personal data — medical records, diagnoses, prescriptions, biometrics, and mental health information. The DPDPA treats health data as deserving of the highest level of protection. Patient consent must be granular and specific. Any breach involving health data carries the maximum penalty. Telemedicine platforms and digital health apps are among the most scrutinised entities.

2. Key Definitions Under DPDPA

These definitions govern how the Act applies to your sector:

Health Data	Medical records, diagnoses, prescriptions, lab reports, mental health records, genetic data — all constitute sensitive personal data.
Biometric Data	Fingerprints, retinal scans, facial recognition data used for patient identification.
Data Principal	The patient — who has the right to access, correct, and erase their health data.
Data Processor	Labs, radiology centres, diagnostic partners, cloud EMR providers — require DPAs.
Purpose Limitation	Data collected for treatment cannot be used for insurance profiling without fresh consent.
Nominee Rights	A patient may nominate a person to exercise their data rights — relevant for deceased or incapacitated patients.

3. Core Compliance Obligations

Every entity in this sector that processes personal data must comply with the following obligations:

1. **Patient Consent**
   Obtain explicit, informed, and written/digital consent before collecting health data. Consent must be purpose-specific — e.g., treatment consent does not cover research use.
2. **Electronic Medical Records (EMR) Security**
   Encrypt all patient records at rest and in transit. Implement role-based access — doctors see clinical data; billing staff see financial data only.
3. **Lab & Diagnostic Data**
   Patient reports must not be shared with third parties (insurers, employers) without explicit consent. Ensure lab partners execute DPAs.
4. **Telemedicine Platforms**
   Consultation recordings, prescriptions, and chat logs are personal data. Retention must be limited to the medically and legally necessary period.
5. **Clinical Trials**
   Research use of patient data requires separate research consent. Anonymise or pseudonymise data wherever possible.
6. **Pharmaceutical Marketing**
   Patient prescription data cannot be used for pharma marketing without explicit consent.
7. **Mental Health Data**

	Applies the highest standard of confidentiality. Do not share with employers, insurers, or family without consent.
8	**Breach Notification** A breach of health data must be reported to DPBI immediately. Coordinate with Ministry of Health guidelines.

4. Implementation Checklist

Use this checklist to track your DPDPA compliance readiness:

- ☐ Audit all patient data systems — EMRs, diagnostic databases, pharmacy records, billing systems.
- ☐ Implement granular patient consent forms — separate consent for treatment, research, insurance, and marketing.
- ☐ Encrypt all health data in storage and during transmission (TLS 1.2+ minimum).
- ☐ Implement strict role-based access controls — principle of least privilege for all staff.
- ☐ Execute Data Processing Agreements with all diagnostic labs, cloud providers, and EMR vendors.
- ☐ Build a patient rights portal — allow patients to access, correct, and request deletion of their health records.
- ☐ Establish a data breach response protocol and test it with a simulation drill.
- ☐ Review third-party data sharing — insurers, employers, researchers — and obtain fresh consent where required.
- ☐ Train all clinical and administrative staff on patient data privacy obligations.
- ☐ Appoint a Grievance Officer and display contact information in reception areas and on your website.
- ☐ Review retention schedules — clinical records (RBI equivalent: Medical Council guidelines), then delete/anonymise.
- ☐ For mental health services: implement the strictest confidentiality protocols and train counsellors separately.

5. Applicable Penalties

The Data Protection Board of India (DPBI) may impose the following penalties for non-compliance:

Rs. 250 Crore	Failure to implement reasonable security safeguards resulting in a personal data breach
Rs. 200 Crore	Breach of obligations related to processing children's personal data
Rs. 150 Crore	Failure to fulfill obligations as a Significant Data Fiduciary (SDF)
Rs. 50 Crore	Failure to comply with Data Principal rights or other provisions of the Act

6. Implementation Roadmap

Follow this phased approach to achieve full DPDPA compliance:

1	**Month 1: Data Discovery** Map all patient data — what is collected, where stored, who has access, how long retained.
2	**Month 2: Consent Redesign** Design DPDPA-compliant consent forms for treatment, research, insurance, and marketing separately.
3	**Month 3: Security Hardening** Implement encryption, access controls, and audit trails across all health IT systems.
4	**Month 4: Vendor Compliance** Execute DPAs with diagnostic partners, cloud EMR providers, and billing processors.
5	**Month 5: Rights & Grievance** Build patient rights request system and appoint/train Grievance Officer.
6	**Month 6+: Review & Training** Annual clinical privacy audits, staff training refreshers, and breach simulation exercises.

🚨 Critical: Health data breaches attract the maximum penalty of Rs. 250 Crore. Invest in robust cybersecurity infrastructure now — it is far less costly than a breach and regulatory penalty.