Vishwaas.ai

Industry Brief

Healthcare

DPDP Act Compliance for Hospitals, Diagnostic Chains, Digital Health Platforms & Insurers

Healthcare Data Is the Most Sensitive Personal Data Under the DPDP Act

The DPDP Act 2023 does not create a separate "sensitive personal data" category — but health and medical data is universally recognised as the category that warrants the highest degree of protection and scrutiny. A data breach involving financial records is damaging. A breach involving a patient's HIV status, psychiatric history, or cancer diagnosis can destroy a life.

Healthcare organisations in India — hospitals, diagnostic chains, telemedicine platforms, digital health apps, pharmaceutical companies, and health insurers — hold precisely this data at scale. They are also among the least prepared for systematic DPDP compliance, having historically operated under a fragmented regulatory landscape (Clinical Establishments Act, IT Act, MoHFW guidelines) with no unified data protection framework.

The DPDP Act changes this materially. It establishes enforceable consent obligations, a 72-hour breach notification clock, and a right of erasure — all of which create significant operational requirements for healthcare data custodians.

The Four Healthcare-Specific Compliance Challenges

Challenge 1: Consent Is Not One Thing in Healthcare

A patient interacting with a hospital gives — or withholds — consent in multiple distinct contexts, each with different legal implications:

Context	Data Involved	Consent Type Required
Clinical treatment	Medical history, diagnosis, prescription	Informed clinical consent (pre-DPDP) + DPDP notice
Diagnostic test results sharing	Lab reports, imaging	Purpose-specific DPDP consent for digital delivery
Insurance claim processing	Diagnosis codes, treatment summary	Explicit consent for sharing with insurer
Telemedicine / app health records	Vitals, symptoms, prescriptions	Explicit digital consent with notice
Health data for research / anonymisation	Aggregated clinical records	Explicit opt-in (DPDP Act is strict on research use)
Marketing communications	Name, email, health categories	Separate explicit consent; must not be bundled with clinical consent
Third-party sharing	Diagnosis, medication history	Explicit consent; highly scrutinised by DPBI

Bundling all of these into a single "patient registration form" consent is the most common — and highest-risk — compliance failure in healthcare today.

Vishwaas AI solution: The Purpose Catalogue supports unlimited purpose definitions per tenant, each with its own lawful_basis, data_categories, and requires_explicit_opt_in flag. A hospital configures separate purposes for each context above. Consent is collected, stored, and evidenced granularly — not as a single undifferentiated patient consent.

Challenge 2: Health Data Moves Across Many Parties

A patient's diagnostic report travels a surprisingly long path from collection to storage:

Patient → Hospital / Clinic
→ Diagnostic Lab (outsourced)
→ Radiologist (outsourced reading)
→ Health Insurer (claim processing)
→ Third-Party Administrator (TPA)
→ Reinsurer
→ Pharmacy (prescription fulfilment)
→ Digital Health App (patient-facing record)

Each handoff is a data processing event that, under the DPDP Act, either requires documented consent or a registered data processing agreement (DPA) that defines the processor's permitted uses. Without visibility into this chain, a hospital cannot demonstrate compliance when the DPBI asks: "Who has this patient's data and on what basis?"

Vishwaas AI solution: The Vendor Management module tracks every third-party data processor — labs, TPAs, insurers, health tech platforms — with DPA status, risk tier, data category scope, and cross-border transfer flag. Each vendor relationship is linked to the consent purposes it relies on. When a patient withdraws consent for insurer data sharing, the Consent Propagation module fires a webhook to the insurer's system within 5 seconds.

Challenge 3: Retention, Erasure, and Medical Records Law

The DPDP Act's right of erasure under Section 12 presents a direct tension with healthcare's retention obligations:

Regulation	Retention Requirement
Clinical Establishments Act	Patient records: 5 years minimum
MoHFW Guidelines	Medico-legal records: 10 years
IRDA (Health Insurance)	Claim records: 7 years
Telemedicine Practice Guidelines	Consultation records: 7 years

When a patient submits a DPDP erasure request, a healthcare organisation cannot simply delete the clinical record — doing so may violate other laws. But it can delete non-clinical personal data (marketing preferences, push notification history, wellness app behavioural data) while retaining the clinical record under a legitimate legal basis.

Vishwaas AI solution: The Data Map module associates each data category with its applicable retention policy and legal basis. When a DPR erasure request is processed, Vishwaas AI: 1. Identifies which data categories are subject to statutory retention obligations — flags these as "retention hold" rather than deleting them 2. Proceeds with erasure of all data categories not covered by a statutory retention obligation 3. Documents the rationale for non-deletion in the DPR audit trail — providing defensible evidence if the patient escalates to the DPBI

Challenge 4: The 72-Hour Breach Clock with Patient Data at Stake

A data breach involving patient health records is a worst-case scenario on multiple dimensions:

- The **DPDP** Act requires DPBI notification within 72 hours
- The **IT Act / CERT**-In requires notification within 6 hours for certain healthcare providers
- Affected patients must be individually notified
- Breached health data cannot be "un-leaked" — the reputational and human consequences are permanent

Healthcare organisations often discover breaches slowly — a ransomware attack on a diagnostic system may go undetected for days before the 72-hour clock even starts. Without a structured incident management process, the notification obligations pile up faster than any team can manage.

Vishwaas AI solution: The Breach Management module starts the 72-hour DPBI countdown the moment an incident is logged. It tracks all mandatory steps — internal assessment, DPBI notification draft and submission, patient notification template and delivery, remediation actions — with a live countdown visible to the DPO. Each step is timestamped and audit-logged. The DPBI evidence package (incident timeline, affected data categories, patient count, notification proof) is generated in one click.

Healthcare Use Cases — Vishwaas AI in Action

Use Case 1: Multi-Specialty Hospital Chain — Patient Consent at Digital Registration

Scenario: A 25-hospital chain is migrating to digital patient registration. Every patient needs to consent to: treatment, digital records, insurance sharing, and optionally to research and marketing.

Current risk: Paper-based consent forms are collected at reception. No digital record. No way to evidence consent at scale when the DPBI calls. Marketing SMS are sent to all patients — including those who never agreed to marketing communications.

With Vishwaas AI: 1. Patient registration kiosk / mobile app integrates the Vishwaas AI Consent SDK 2. Five separate consent prompts — each in the patient's preferred language (22 Indian languages) 3. Each consent is hash-chained with a TSA timestamp — the exact text shown to the patient at the exact time is captured in the consent record 4. Marketing consent is propagated in real time to the hospital's CRM; non-consenting patients are never added to marketing lists 5. Patients can log into the patient portal to review and withdraw any consent at any time — satisfying DPDP Act Section 6's easy-withdrawal requirement

Use Case 2: Diagnostics Chain — Lab Report Delivery and Third-Party Access

Scenario: A national diagnostics chain processes 2 million tests per month. Reports are shared digitally with patients, referring doctors, hospitals, and insurers.

Current risk: Reports are shared via WhatsApp and email to whatever contact the front desk collected — no documented consent for digital delivery or for third-party sharing. Insurance companies receive diagnostic data on the basis of a blanket authorisation buried in the policy document.

With Vishwaas AI: 1. Consent is collected at sample registration: (a) digital report delivery to patient, (b) sharing with referring doctor, (c) sharing with insurer/TPA 3. Each sharing event is linked to its governing consent record — creating a traceable chain from data collection to disclosure 4. Insurer and TPA are registered as vendors in the Vendor module with a DPA defining permitted data uses 5. When a patient withdraws consent for insurer sharing, the propagation webhook fires to the insurer's claims system; the DPR module can orchestrate a deletion request to the TPA

Use Case 3: Telemedicine / Digital Health Platform — App Data and Research Consent

Scenario: A telemedicine platform has 5 million users. It collects vitals, symptoms, consultation histories, and prescription data. It sells anonymised population health insights to pharmaceutical companies.

Current risk: The privacy policy buries research and analytics data use in general "data use" language. The platform's anonymisation is partial — records retain date-of-birth and pincode, which in combination with a diagnosis can re-identify individuals in small population segments.

With Vishwaas AI: 1. Separate consent purposes are defined for: (a) clinical consultation records, (b) wellness tracking, (c) anonymised research use, (d) pharmaceutical analytics sharing 2. Research and analytics consent requires explicit opt-in — not pre-ticked, not bundled with app registration 3. The Data Map module documents exactly which fields are shared with pharma partners — supporting a vendor DPA with defined data minimisation requirements 4. The Privacy Notice module delivers a DPDP Rules 2025 Rule 3–compliant notice in the user's app language, with a standalone notice link — not buried in 40 pages of terms

Regulatory Alignment

Regulation	Relevant Obligation	Vishwaas AI Module
DPDP Act §5	Notice in accessible language before consent	Notice Module — 22 languages, standalone format
DPDP Act §6	Specific, granular, non-bundled consent	Consent Module — purpose catalogue, requires_explicit_opt_in
DPDP Act §8(6)	Breach notification to DPBI within 72 hours	Breach Module — countdown, notification workflow
DPDP Act §11	Right to access personal data	DPR Module — data discovery and export
DPDP Act §12	Right to erasure (with retention hold for legal obligations)	DPR Module — selective erasure; Data Map — retention policies
DPDP Act §13	30-day grievance resolution	DPR Module — SLA tracking, DPBI escalation
Clinical Establishments Act	5-year patient record retention	Data Map — retention policy; DPR erasure hold
Telemedicine Practice Guidelines 2020	7-year record retention; patient consent for teleconsultation	Consent Module + Data Map retention
MoHFW Health Data Management Policy	Patient rights; data fiduciary obligations for hospitals	All modules
RDAI Health Insurance Regulations	Policyholder data confidentiality; claim data sharing	Vendor Module — TPA/insurer DPA; Consent Module
CERT-In Directions 2022	Breach reporting within 6 hours for certain entities	Breach Module — parallel notification workflow

What Healthcare DPOs Need to Know

Consent at the point of care: Vishwaas AI's embeddable Consent SDK integrates with patient registration systems, electronic health record (EHR) platforms, and telemedicine apps. Consent is collected digitally, in the patient's language, at the exact moment it is needed — not on a paper form that gets filed away.

Legal defensibility for sensitive health data: When a patient disputes what they consented to — or when the DPBI investigates a complaint — Vishwaas AI produces a signed consent record: the exact text shown to the patient, the timestamp verified by an RFC 3161 Timestamp Authority, and a cryptographic hash chain that proves the record has never been altered. No competitor in the Indian market provides this level of evidence for health data consent.

Retention holds for clinical records: The right of erasure does not override the Clinical Establishments Act or Telemedicine Practice Guidelines. Vishwaas AI's retention policy engine flags records with statutory holds, ensuring erasure requests are handled correctly — neither refusing all deletions nor deleting records that must be retained.

India data residency: All patient consent and health data processed through Vishwaas AI is stored exclusively in AWS Mumbai (ap-south-1). No patient data leaves Indian jurisdiction. This aligns with the MoHFW Health Data Management Policy's data localisation expectations and the DPDP Act's India residency framework.

+1 888 208 5076
+91 901 926 6824

sales@crossidentity.com

www.crossidentity.com