PRANAVITA AI · pranavitahealthtech.com

DPDPA 2023 — Compliance Framework

Our obligations as Data Fiduciary under the Digital Personal Data Protection Act, 2023

Effective: May 18, 2026 · Version 1.0 · Jurisdiction: Republic of India

Pranavita AI acknowledges its obligations as a Data Fiduciary under the Digital Personal Data Protection Act, 2023 (DPDPA). As a platform processing sensitive personal health data, we apply the highest standards of data protection and privacy.

§1 Our Role Under the DPDPA

DPDPA Role	Pranavita's Position
Data Fiduciary	Pranavita AI — determines the purpose and means of processing personal data
Data Processor	Our cloud providers, analytics vendors, and AI infrastructure partners (bound by data processing agreements)
Data Principal	All users of the Pranavita platform whose personal data is processed
Significant Data Fiduciary	To be determined based on data volume thresholds set by the Central Government

§2 Data Protection Principles

Principle	How We Apply It
Purpose Limitation	Data is collected only for specific, defined purposes and not used beyond those purposes without fresh consent.
Data Minimisation	We collect only what is strictly necessary for the stated purpose. No bulk or speculative collection.
Accuracy	We maintain mechanisms for users to correct inaccurate data and take reasonable steps to keep data up to date.
Storage Limitation	Data is retained only for as long as necessary for the purpose, then deleted or anonymised.
Integrity & Confidentiality	Appropriate security measures protect data against unauthorised access, disclosure, or loss.
Accountability	Pranavita is responsible for and can demonstrate compliance with all DPDPA obligations.

§3 Consent Architecture

Under Section 6 of the DPDPA, consent must be free, specific, informed, unconditional, and unambiguous.

3.1 Consent Notice (Section 5 Compliance)

Before collecting any personal data, we present a clear Consent Notice specifying:

- The personal data to be processed
- The specific purpose of processing
- The right to withdraw consent
- The right to access a grievance mechanism
- Identity and contact details of the Data Fiduciary

3.2 Granular Consent Categories

Processing Activity	Consent Type	Can Be Withdrawn?
Core platform account creation	Necessary (still requires free consent)	Yes — by deleting account
AI analysis of health records	Explicit, purpose-specific	Yes — toggleable in settings
Wearable device data integration	Explicit, device-specific	Yes — per device in settings
Sharing with consulting doctor	Explicit, per-consultation	Yes — before consultation starts
Lab data transmission	Explicit, per-booking	Yes — before booking confirmed
ABDM ABHA linkage	Explicit, ABDM consent artefact	Yes — unlink ABHA in settings
Marketing communications	Opt-in, separate	Yes — unsubscribe anytime
AI model improvement (anonymised)	Opt-in only	Yes — opt-out in settings

We do NOT bundle or bundle-condition consent. Refusing optional consent categories does not restrict access to core platform features.

§4 Data Principal Rights Implementation

Right (DPDPA Section)	How We Implement It	Response Timeline
Right to Information (§11)	Privacy Policy, in-app data summary, and Consent Notice available at all times	Immediate
Right to Access (§11)	Downloadable data export in JSON/PDF format via Settings → My Data	Within 30 days
Right to Correction & Erasure (§12)	Profile editing and account deletion flow in-app; support escalation for complex corrections	Correction: 15 days; Deletion: 30 days
Right to Grievance Redressal (§13)	Dedicated Grievance Officer + in-app complaint form	Acknowledgement: 48hr; Resolution: 30 days
Right to Nominate (§14)	Nomination form available via Settings; nominee can exercise rights per DPDPA §14	Within 30 days

§5 Data Fiduciary Obligations

5.1 Security Safeguards (Section 8)

- AES-256 encryption at rest for all personal health data
- TLS 1.3 encryption in transit
- Role-based access controls (RBAC) with least-privilege principle
- Multi-factor authentication for admin access
- Regular vulnerability assessments and penetration testing

5.2 Breach Notification (Section 8(6))

- Notification to the Data Protection Board of India within 72 hours of becoming aware of a breach
- Notification to affected Data Principals in a timely manner with details of the breach and remediation steps
- Incident Response Plan (IRP) reviewed annually

5.3 Data Retention & Deletion (Section 8(7))

We have implemented automated data retention policies that flag data for deletion or anonymisation when the purpose for which it was collected has been fulfilled.

§6 Cross-Border Data Transfer (Section 16)

- Primary data storage: India (AWS Mumbai) — no cross-border transfer for stored PHI
- AI inference processing: may use cloud AI APIs in permitted jurisdictions only, under contractual data processing safeguards that prohibit training on user data
- Analytics: only anonymised, aggregated data is processed in cross-border contexts
- We will update our practices promptly upon notification of any jurisdiction restrictions by the Central Government

§7 Children's Data — Additional Safeguards (Section 9)

- Verifiable parental or guardian consent is obtained before processing any data of a minor (under 18)
- We do not process children's data in a manner detrimental to their wellbeing
- We do not serve behavioural tracking or targeted content to children
- Age-gating mechanisms are implemented at registration

§8 Data Protection Officer & Governance

If designated a Significant Data Fiduciary by the Central Government, Pranavita will comply with the additional obligations under Section 10, including:

- Appointment of a Data Protection Officer (DPO) based in India
- Independent Data Audit by a registered auditing firm
- Data Protection Impact Assessment (DPIA) for high-risk processing activities
- Algorithmic accountability for AI health analysis systems

Pranavita proactively applies SDF-level protections as best practices even before formal designation, given the sensitivity of health data we process.

Contact & Grievance

Grievance Officer	Subham Pratik Mahanand
Designation	Grievance Officer – Founding Team
Phone	+91-9337039267
Email	subham@pranavitahealthtech.com
DPO Email	dpo@pranavitahealthtech.com
Website	https://pranavitahealthtech.com
Grievance Email	subham@pranavitahealthtech.com

For data protection concerns, regulatory queries, or to exercise your rights, contact the Grievance Officer above. Response guaranteed within 48 hours.