PRANAVITA AI · pranavitahealthtech.com

Privacy Policy

Your health data. Your rights. Your control.

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

Pranavita AI is committed to protecting your personal health information under the Digital Personal Data Protection Act, 2023 (DPDPA), the Information Technology Act, 2000, and applicable Indian health data regulations.

1. Who We Are & Scope

Pranavita AI (Pranavita, we, our, us) is a health information technology platform providing AI-assisted health services. We operate as an IT Intermediary under Section 79 of the IT Act, 2000, and as a Data Fiduciary under the DPDPA, 2023.

This Policy applies to all users of the Pranavita mobile application (Android and iOS), our website at pranavitahealthtech.com, and all associated services.

IMPORTANT: Pranavita AI is a health information and technology platform, not a licensed medical provider. Our AI-generated insights do not constitute medical advice. Always consult a qualified healthcare professional for clinical decisions.

2. Data We Collect

We collect only data that is strictly necessary to provide and improve our services:

Category	Data Types	Collection Method
Identity Data	Name, phone number, email, age, gender, profile photo	User registration
Health Data	Lab reports, test results, biomarkers, health scores, medical history, allergies, medications, family history, conditions	User upload / lab integration
Wearable Data	Heart rate, sleep, steps, SpO2, activity data	Device integration (with consent)
Conversational Data	AI chat history, health queries, voice inputs	In-app interaction
Hospital Records	Discharge summaries, prescriptions, radiology reports	User upload
Location Data	City-level location for lab discovery; precise location with explicit consent only	Device GPS (optional)
Device & Usage Data	Device type, OS version, app usage patterns, crash logs	Automatic collection
Payment Data	Transaction IDs, payment method type (not card numbers)	Payment processing

We do NOT store full payment card details. All payment processing is handled by PCI-DSS compliant third-party gateways (Razorpay).

3. How We Use Your Data

Your data is used for the following purposes, each tied to a specific legal basis:

Purpose	Legal Basis
Providing AI health analysis, HealthScore, and conversational responses	Consent + Legitimate interest
Lab report OCR, biomarker extraction, and trend analysis	Consent
Connecting patients with labs for test booking	Contract performance
Facilitating telemedicine consultations with licensed doctors	Consent + Contract
Health memory storage for continuity of care	Consent
Medication and habit reminders	Consent
Improving AI model accuracy (anonymised aggregate data only)	Legitimate interest
Fraud prevention and platform security	Legitimate interest
Regulatory compliance and legal obligations	Legal obligation

We do not use your health data for advertising, insurance profiling without consent, or sale to third parties. We do not train external AI models on your data without explicit opt-in consent.

4. Data Sharing & Disclosure

We share your data only in the following limited circumstances:

4.1 With Your Explicit Consent:

- Diagnostic labs: your name, contact, and test order details are shared with the lab you book with.
- Doctors on platform: your health summary and relevant records are shared with a consulting doctor only when you initiate a consultation.
- ABDM ecosystem: if you link your ABHA ID, your health records may be shared per your consent artefact.

4.2 With Service Providers (Data Processors):

- Cloud hosting providers (AWS/Azure — India region servers)
- Payment gateways (Razorpay)
- SMS/OTP service providers (for authentication)
- Analytics providers (anonymised/aggregated data only)

4.3 Legal Disclosure:

We may disclose data when required by law, court order, or government authority under Indian law. We will notify you wherever legally permitted to do so.

> We never sell, rent, or trade your personal health data to advertisers, data brokers, or insurance companies.

5. Data Localisation & Storage

- All personal health data of Indian users is stored on servers located within the Republic of India.
- Primary database infrastructure: AWS Asia-Pacific (Mumbai) region.
- Cross-border transfer occurs only to jurisdictions with adequate data protection frameworks, under contractual safeguards, and with your explicit consent.
- Backup servers are also located within India.

6. Security Measures

Security Measure	Implementation
Encryption in transit	TLS 1.3 for all data transmission
Encryption at rest	AES-256 for all stored health records and lab reports
Access controls	Role-based access control (RBAC); audit trails for all PHI access
Authentication	OTP-based login; optional biometric lock in-app
Audit logs	All data access events logged and retained for 12 months
Security audits	Annual third-party penetration testing
Breach notification	Affected users and Data Protection Board notified within 72 hours

7. Your Rights as Data Principal (DPDPA 2023)

Right	What This Means	How to Exercise
Right to Access	Obtain a summary of personal data we hold	Settings → My Data → Download
Right to Correction	Correct inaccurate or incomplete personal data	Edit profile or contact support
Right to Erasure	Request deletion of your data	Settings → Delete Account
Right to Grievance Redressal	Lodge complaints about data processing	Grievance Officer below
Right to Nominate	Nominate another person to exercise rights	Contact Grievance Officer
Right to Withdraw Consent	Withdraw previously given consent	Settings → Privacy → Manage Consent

We will respond to all data rights requests within 30 days of receipt.

8. Consent Management

We operate a granular consent framework. You provide separate consent for:

- Core app functionality (required for using the platform)
- AI analysis of your health records
- Wearable and IoT device data integration
- Sharing records with consulting doctors
- ABDM health locker linkage
- Marketing communications and health tips

You may manage and withdraw consent at any time through Settings → Privacy → Manage Consent.

9. Children's Privacy

Pranavita AI is not intended for persons under 18 years of age without verifiable parental or guardian consent. Family health tracking for minor dependents requires the account holder (parent/guardian) to be 18+ and to provide explicit consent.

10. Data Retention & Deletion

Data Type	Retention Period
Account & identity data	Duration of account + 12 months post-deletion
Health records & lab reports	7 years (per Clinical Establishments Act) or until deletion request
AI conversation history	24 months from last interaction, unless deleted earlier
Payment transaction records	8 years (Income Tax Act requirement)
Audit logs	12 months
Anonymised analytics data	Indefinitely (cannot be re-identified)

When you delete your account, we will erase or anonymise your personal data within 30 days, except where retention is required by law.

11. Policy Changes

We will provide at least 15 days' notice of material changes via in-app notification. Continued use of Pranavita after the effective date constitutes acceptance of the updated policy.

Contact & Grievance

Grievance Officer	Subham Pratik Mahanand

Designation	Grievance Officer – Founding Team
Phone	+91-9337039267
Email	subham@pranavitahealthtech.com
Support Email	support@pranavitahealthtech.com
Website	https://pranavitahealthtech.com
Effective Date	May 18, 2026

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