PRIVACY POLICY

Effective Date: 14/08/2026

1. INTRODUCTION

1.1 This Privacy Policy explains how VITHOS, operating under the Google Play Store developer/publisher name "Vithos Labs" ("VITHOS", "the Company", "we", "our" or "us"), collects, uses, stores, shares, protects, retains and deletes Personal Data in connection with the VITHOS mobile application, and related digital products and services (together, the "Platform" or "Services").

1.2 VITHOS is not yet incorporated as a distinct legal entity under Indian law and currently operates as an individual/unregistered developer under the name "Vithos Labs". Once VITHOS incorporates a formal legal entity to operate the Platform, this Privacy Policy will be updated to reflect that entity's name, registered office and corporate identification details, and references to "VITHOS" will be read accordingly.

1.3 VITHOS provides a digital health record management platform through which Users may upload, store, organise, access, retrieve, manage and, where the feature is enabled, share health records relating to themselves and to family members or dependants they are lawfully authorised to manage.

1.4 Health records are highly private in nature. VITHOS applies the principles of data minimisation, purpose limitation, transparency, security, accountability and privacy-by-design to all Personal Data It Processes, to the extent reasonably practicable at its current stage of operation.

1.5 VITHOS intends to act as a Data Fiduciary under the Digital Personal Data Protection Act, 2023 ("DPDP Act") in respect of Personal Data for which it determines the purpose and means of Processing. VITHOS is presently in the process of aligning its practices with the DPDP Act and is not yet fully compliant with every obligation applicable to a Data Fiduciary. This Privacy Policy describes VITHOS's target compliance framework, where a right, mechanism or safeguard described here is not yet fully implemented, VITHOS will give effect to it through the best available alternative means until it is, and will update this Policy as its compliance measures mature.

1.6 This Privacy Policy should be read together with VITHOS's Terms of Use and any privacy, cookie or feature-specific consent notice made available on the Platform. It does not, by itself, constitute Consent for every Processing activity undertaken by VITHOS. Where Applicable Law requires Consent, VITHOS will provide an appropriate notice and obtain it through a clear affirmative action.

2. DEFINITIONS

Unless the context requires otherwise, the following expressions bear the meanings set out below.

2.1 "**APPLICABLE LAW**" means all statutes, rules, regulations, directions and legally binding requirements applicable to VITHOS from time to time, including, to the extent in force, **The Digital Personal Data Protection Act, 2023**, **The Digital Personal Data Protection Rules, 2025, The Information Technology Act, 2000 and rules made under it, applicable directions of The Indian Computer Emergency Response Team ("CERT-In"), Applicable Consumer Protection Laws**, requirements governing **The Ayushman Bharat Digital Mission ("ABDM"),** where applicable to VITHOS's participation in that ecosystem; and any amendment or replacement of the foregoing.

2.2 "**CHILD**" means an individual who has not completed eighteen (18) years of age, or such other age as may be prescribed under Applicable Law.

2.3 "**CONSENT**" has the meaning given to it under Applicable Law and, where the DPDP Act applies, means consent that is free, specific, informed, unconditional and unambiguous, signified through clear affirmative action for the Processing of Personal Data for a specified purpose.

2.4 "**DATA PRINCIPAL**" means the individual to whom the Personal Data relates, and includes such other persons recognised as acting on behalf of a Data Principal under Applicable Law.

2.5 "**DATA PROCESSOR**" means any person or entity that Processes Personal Data on behalf of VITHOS.

2.6 "**PERSONAL DATA**" means any data about an individual who is identifiable by or in relation to such data.

2.7 "**PERSONAL DATA BREACH**" means any unauthorised Processing of Personal Data, or any accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to Personal Data, that compromises its confidentiality, integrity or availability.

2.8 "**PROCESSING**" means a wholly or partly automated operation, or set of operations, performed on digital Personal Data, including collection, storage, use, sharing, disclosure and erasure.

2.9 "**USER**" means an individual who accesses, registers with or uses the Platform.

3. SCOPE AND APPLICABILITY

3.1 This Privacy Policy applies to Personal Data Processed by VITHOS in connection with, count registration and administration, use of the VITHOS mobile application and website, storage and management of health records for family member or dependant profiles, subscription and billing (where introduced), communications with VITHOS, the technical operation and security of the Platform, and any other Service expressly brought within this Policy.

3.2 This Privacy Policy applies to Personal Data collected in digital form, and to Personal Data collected in non-digital form and subsequently digitised, to the extent governed by Applicable Law.

4. PERSONAL DATA COLLECTED BY VITHOS

VITHOS seeks to collect only such Personal Data as is reasonably necessary for the purposes disclosed to the User. Depending on how a User uses the Platform, VITHOS may Process the following categories of Personal Data.

4.1 Account and Identity Information

- Full name, email address and mobile number;
- Account or User identifier and authentication information, including password credentials stored in cryptographically hashed form, and
- Name and email address received from Google, Apple or another authentication provider, where the User chooses to sign in through it.

4.2 Health and Medical Information

Where voluntarily uploaded, entered or otherwise provided by the User, VITHOS may Process laboratory and diagnostic reports, prescriptions, doctor's notes, medical reports,

scans, medication and allergy information, medical history and treatment related notes, hospital or healthcare provider documents, health records relating to authorised family member profiles, and any other health related document or information the User chooses to store on the Platform. VITHOS recognises the particularly confidential nature of health information and applies safeguards appropriate to its nature, volume and associated risk.

4.3 Camera and Photo Gallery Access

4.3.1 VITHOS requests access to a User's device camera and/or photo gallery strictly to allow the User to scan, capture or upload medical records and related documents to the Platform.

4.3.2 VITHOS does not access, browse or collect photographs or media on the User's device that are unrelated to this specific scan, capture or upload action. By actively using this functionality, the User consents to VITHOS accessing the camera and/or photo gallery solely to the extent necessary to complete that action.

4.4 Family Member and Dependant Information

Where a User creates a family member or dependant profile, VITHOS may Process that individual's name, age or date of birth, relationship to the account holder, and health, medication, allergy and other information voluntarily entered in connection with the profile. A User must not provide another individual's Personal Data unless the User has the authority or lawful basis to do so.

4.5 Technical and Device Information

VITHOS may automatically collect technical information necessary to operate, diagnose and secure the Platform, including IP address, device type, operating system, browser information, application version, session and timestamp data, authentication events, and crash, diagnostic and security logs. Such information will not intentionally include the substantive contents of health records, except where technically necessary for a feature expressly requested by the User.

4.6 Approximate Location

VITHOS may infer approximate city level location from a User's IP address where reasonably required for security, diagnostics or fraud prevention. VITHOS does not collect precise GPS location unless separately disclosed and consented to.

4.7 Subscription and Transaction Information

4.7.1 As of the date of this Privacy Policy, VITHOS does not offer any paid subscription, in-app purchase or other payment functionality, and does not collect or Process any payment, billing or transaction information.

4.7.2 If VITHOS introduces paid functionality, this Privacy Policy will be updated before launch to describe the transaction information Processed, the manner in which payment credentials are handled, and whether such credentials are collected directly by a payment gateway or service provider under its own privacy and security framework.

4.8 Communications

Where a User contacts VITHOS, VITHOS may Process the User's name and contact information together with the substance of the support request, grievance, privacy request, complaint or feedback provided.

5. DATA VITHOS DOES NOT INTEND TO COLLECT

Unless a specific feature expressly requires otherwise and an appropriate notice and Consent mechanism is provided, VITHOS does not intend to access or collect, the User's device contact list, microphone recordings, photographs or media on the User's device unrelated to the scan, capture or upload of medical records described in Clause 4.3, data from unrelated applications installed on the device; or precise GPS location.

6. SOURCES OF PERSONAL DATA

6.1 Directly from the User information entered during registration, health records uploaded, profile information and communications.

6.2 Automatically through the Platform, technical, device, diagnostic, security and usage information.

6.3 From authentication providers, where the User elects to sign in using Google, Apple or a similar service.

6.4 From another authorised User, where that User lawfully manages a family member's or dependant's information through an authorised profile. By uploading or entering another individual's Personal Data in connection with such a profile, the uploading User represents and authorises VITHOS to Process that information for the purposes of this Privacy Policy this representation is VITHOS's basis for accepting the upload, as

described in Clause 11. Where the Platform allows a family-member or dependant profile to be independently accessed by that individual, VITHOS restricts access to that profile to the individual concerned, VITHOS does not otherwise independently verify the uploading User's authority.

6.5 From service providers, to the limited extent necessary for payments, authentication, cybersecurity, support or other Services.

7. PURPOSES OF PROCESSING

VITHOS Processes Personal Data only for the following specified purposes:

- Account creation, authentication and administration,
- Storage, organisation and management of health records, including export where such functionality is made available,
- Management of family-member and dependant health profiles,
- Synchronisation of information across a User's authorised devices,
- Security, authentication and prevention of unauthorised access or misuse,
- Transactional communications, including authentication messages, password resets, login alerts and security notifications,
- Technical operations error diagnosis, crash investigation, performance and security monitoring,
- Customer support and handling of grievances and rights requests,
- Administration of paid subscriptions, if and when introduced, and related billing, accounting and tax compliance;
- Optional product updates or promotional communications, where the User has opted in or as otherwise permitted under Applicable Law, and
- AI-enabled extraction and mapping of information from uploaded medical records into structured form templates, as described in Clause 24.

8. CONSENT AND LAWFUL PROCESSING

8.1 Where Consent is the applicable basis for Processing, VITHOS obtains Consent before Processing Personal Data for the specified purpose.

8.2 Consent is sought through clear affirmative action and, where Applicable Law requires it, is never inferred merely from inactivity, silence or a User's failure to deselect a pre-selected option.

8.3 At or before seeking Consent, VITHOS provides an appropriate notice covering, where applicable the Personal Data proposed to be Processed, the specified purpose, the Service enabled by that Processing, how Consent may be withdrawn, how rights may be exercised, VITHOS's grievance-redressal mechanism, and the mechanism for approaching the Data Protection Board of India.

8.4 VITHOS does not make Consent conditional on the collection of Personal Data not necessary for the specified Service, except where Applicable Law permits.

8.5 Where VITHOS proposes to Process Personal Data for a materially different purpose, it will provide notice and obtain fresh Consent where required.

8.6 Nothing in this Privacy Policy prevents VITHOS from Processing Personal Data without Consent where such Processing falls within a legitimate use, or another circumstance expressly permitted under Applicable Law.

9. WITHDRAWAL OF CONSENT

9.1 Where Processing is based on Consent, the User may withdraw it at any time, including, where applicable, through the Platform's Settings.

9.2 Withdrawal does not affect the lawfulness of Processing carried out before it took effect.

9.3 Following withdrawal, VITHOS will cease the relevant Processing and cause its Data Processors to do the same and erase the affected Personal Data, unless continued retention or Processing is required or authorised under Applicable Law.

9.4 Where withdrawal prevents VITHOS from providing a Service that necessarily requires the affected Personal Data, VITHOS may discontinue that Service after informing the User of the consequence.

10. HEALTH DATA SPECIFIC COMMITMENTS

Unless VITHOS subsequently introduces a feature governed by a separate, compliant notice and lawful basis:

10.1 VITHOS will not sell Users' health records.

10.2 VITHOS will not disclose Users' health records to advertisers or data brokers for targeted advertising.

10.3 VITHOS will not disclose Users' health records to employers, pharmaceutical companies or insurers for their independent commercial exploitation.

10.4 VITHOS does not provide the substantive contents of Users' health records to any third-party AI provider for that provider's own general purpose or model training purposes. As explained in Clause 24, VITHOS's AI-enabled record extraction feature does not involve any such training, this is a contractual position under VITHOS's current arrangements with its AI providers, not merely an intention.

10.5 VITHOS will not use health records for targeted advertising.

10.6 Any materially new Processing of health records including additional AI analysis, automated profiling or third-party health-data integrations beyond that described in Clause 24 will be subject to an appropriate privacy assessment, notice and Consent, where required under Applicable Law.

11. FAMILY MEMBER INFORMATION

11.1 VITHOS permits an account holder to store health information relating to family members only where the account holder has appropriate authority to provide and manage that information.

11.2 By uploading Personal Data relating to another adult, the User represents that they have obtained the necessary permission, or otherwise have a lawful basis, to provide that information to VITHOS. VITHOS treats the upload itself as this representation and authorisation, as described in Clause 6.4.

11.3 VITHOS may request reasonable evidence of authority where a dispute, rights request or complaint concerns Personal Data stored by another User.

11.4 The ability to technically upload another person's information does not amount to a representation by VITHOS that the User has legal authority to do so.

12. CHILDREN'S PERSONAL DATA

12.1 A VITHOS account may only be created by a person who has completed eighteen (18) years of age.

12.2 An adult User may, where lawfully authorised, create or manage a health profile relating to a Child.

12.3 Where Applicable Law requires verifiable parental Consent, VITHOS will implement appropriate technical and organisational measures to verify that the individual identifying as the Child's parent or lawful guardian is an adult with legal authority to provide that Consent.

12.4 VITHOS will not undertake Processing of a Child's Personal Data that is likely to cause a detrimental effect on the Child's well-being.

12.5 VITHOS will not track or behaviourally monitor Children, or direct targeted advertising at them, except to the extent expressly permitted or exempted under Applicable Law.

12.6 Where VITHOS becomes aware that a Child's Personal Data has been collected without the authorisation Applicable Law requires, VITHOS may restrict its Processing and take appropriate steps to erase it.

13. SHARING OF PERSONAL DATA

VITHOS does not sell Personal Data. It may nevertheless be disclosed in the limited circumstances below.

13.1 Data Processors

VITHOS may engage Data Processors and service providers for cloud infrastructure and hosting, encrypted backups, email delivery, authentication, payment processing (if introduced), customer support, cybersecurity, application monitoring and error diagnostics, privacy-compatible analytics as described in Clause 23, and AI-enabled record extraction and mapping as described in Clause 24. VITHOS enters into appropriate contractual arrangements with its Data Processors requiring them to Process Personal Data only for authorised purposes and subject to appropriate confidentiality and security safeguards, to the extent such arrangements can reasonably be put in place at VITHOS's current stage, and remains responsible for Processing undertaken on its behalf to the extent required under Applicable Law.

13.2 User-Directed Sharing

Where the Platform permits a User to share records with another person, healthcare professional or family member, VITHOS discloses the information the User selects in accordance with the User's instructions. The User is responsible for confirming the identity and authority of the intended recipient before sharing health records.

13.3 Legal Disclosure

VITHOS may disclose Personal Data where required under Applicable Law, an order of a competent court, a lawful governmental or regulatory direction, a lawful law-enforcement request, or applicable cybersecurity reporting requirements. Where legally permitted and appropriate, VITHOS may notify affected Users before or after such disclosure.

13.4 Corporate Transactions

Personal Data may be disclosed in connection with a bona fide merger, acquisition, restructuring, investment, financing, insolvency or sale of VITHOS or substantially all of its relevant business assets, subject to appropriate confidentiality, purpose-limitation and Applicable Law requirements.

14. DATA RESIDENCY AND INTERNATIONAL TRANSFERS

14.1 Based on VITHOS's presently stated architecture, Personal Data stored through the Platform is hosted on infrastructure located within India.

14.2 VITHOS will verify whether any service provider, support provider, authentication provider, analytics provider or other Data Processor accesses or Processes Personal Data from outside India before representing that no cross-border Processing whatsoever occurs.

14.3 VITHOS uses third-party AI providers Mistral, based in the European Union, and OpenAI, based in the United States to extract, analyse and map information from uploaded medical records, as described in Clause 24. This involves a transfer of Personal Data to those jurisdictions, carried out under data-processing agreements with each provider. Under the DPDP Act, cross-border transfer of Personal Data is permitted by default and restricted only to countries the Central Government specifically notifies, as of the date of this Privacy Policy, neither the European Union nor the United States is subject to such a restriction. VITHOS will update this Clause if that position changes, or if its arrangements with these providers change.

14.4 Any transfer of Personal Data outside India will otherwise be undertaken only in accordance with the DPDP Act, the DPDP Rules and any restriction imposed by the Central Government.

14.5 If VITHOS materially changes its data residency practices, affected Users will be given appropriate notice, and Consent will be obtained where Applicable Law requires it.

15. INFORMATION SECURITY

15.1 VITHOS implements reasonable security safeguards designed to protect Personal Data against Personal Data Breaches, unauthorised Processing, disclosure, acquisition, alteration, destruction and loss of access.

15.2 Based on VITHOS's currently represented technical architecture, these safeguards include, encryption of health records both at rest and in transit using AES-256, the latter implemented via TLS 1.3, restricted production system access with multi factor authentication, access logging and access controls, encrypted backups, vulnerability scanning, and monitoring of relevant security events.

15.3 Access to Personal Data is restricted, so far as reasonably practicable, to authorised personnel and service providers with a legitimate need for it.

15.4 VITHOS implements appropriate contractual and organisational measures with its Data Processors, and maintains logs and records required for cybersecurity, incident detection, investigation and compliance.

15.5 No electronic system can be guaranteed to be absolutely secure, and nothing in this Privacy Policy constitutes a guarantee that a Personal Data Breach can never occur.

16. PERSONAL DATA BREACH

16.1 VITHOS maintains an incident response mechanism designed to detect, contain, assess, investigate, remediate and document Personal Data Breaches, taking reasonable steps to contain the incident, assess its nature and scope, identify affected Data Principals where reasonably practicable, investigate the cause, remediate identified vulnerabilities, and comply with applicable notification requirements.

16.2 Where required under the DPDP Act and DPDP Rules, VITHOS will notify affected Data Principals of a Personal Data Breach in the manner Applicable Law prescribes, including a description and nature of the breach, its extent and timing, likely consequences, mitigation measures taken, steps the individual may take, and VITHOS's contact details for related enquiries.

16.3 VITHOS will notify the Data Protection Board of India of Personal Data Breaches within the timeframe Applicable Law prescribes, and will separately comply with cyber incident reporting obligations under the Information Technology Act, CERT-In directions and other Applicable Law.

17. DATA RETENTION

17.1 VITHOS does not retain Personal Data indefinitely merely because it has been collected.

17.2 Personal Data is ordinarily retained only for as long as the specified purpose continues to be served, the User maintains an active account for which the data remains necessary, retention is required under Applicable Law, or retention is necessary for security, fraud prevention, or the establishment, exercise or defence of legal claims.

17.3 Once the specified purpose is no longer served and retention is not required by Applicable Law, VITHOS erases the relevant Personal Data and causes its Data Processors to do the same.

18. DELETION OF INDIVIDUAL HEALTH RECORDS

18.1 Users may delete individual reports through functionality provided within the Platform.

18.2 Based on VITHOS's currently stated deletion architecture, a deleted report ceases to appear in the User's vault immediately, is intended to be removed from active servers within approximately twenty-four (24) hours, and residual encrypted backup copies are intended to be overwritten or deleted within ninety (90) days in each case subject to lawful retention requirements and technical backup cycles.

19. ACCOUNT DELETION

19.1 Users may request deletion of their VITHOS account and associated Personal Data and health records through the applicable account settings or by contacting VITHOS.

19.2 Following a valid request, the account is deactivated, Personal Data is ordinarily removed from active systems within thirty (30) days, and residual data in encrypted backups is ordinarily overwritten or removed within ninety (90) days, information VITHOS is legally required to retain may continue to be retained solely for that purpose.

19.3 VITHOS may retain a limited record of the deletion request reasonably necessary to demonstrate compliance for a documented retention period, and invoices, tax and accounting records may be retained for the period Applicable Law prescribes, notwithstanding deletion of the User's health-record vault. Personal Data retained solely for a statutory requirement will not be used for an unrelated commercial purpose.

20. DATA EXPORT

20.1 As of the date of this Privacy Policy, VITHOS does not support export of a User's stored health records or other Personal Data. VITHOS does support complete deletion of a User's account and associated Personal Data, as described in Clause 19.

20.2 If VITHOS introduces export functionality, this Clause will be updated to describe its scope, format, any limitations (such as expiry of temporary download links), and the User's responsibility for securing exported information once it leaves VITHOS's control. Until then, a User who wishes to obtain a copy of their Personal Data may submit a request under Clause 22, and VITHOS will respond in accordance with Applicable Law and its grievance-redressal mechanism.

21. RIGHTS OF DATA PRINCIPALS

Subject to the commencement, applicability, limitations and exceptions under the DPDP Act and DPDP Rules, a Data Principal may exercise the rights below. As noted in Clause 1.5, VITHOS is still building the technical and organisational mechanisms needed to give full effect to these rights, the current status of a specific mechanism, such as data export, is described in the relevant Clause.

- Right to access information about Personal Data VITHOS Processes,
- Right to correction of inaccurate or misleading Personal Data,
- Right to completion of incomplete Personal Data, and to updating Personal Data where appropriate,
- Right to erasure of Personal Data previously provided, except where retention is necessary for the specified purpose or required by Applicable Law presently given effect through the account-deletion mechanism at Clause 19,
- Right to withdraw Consent, where Processing is based on Consent,
- Right to grievance redressal regarding VITHOS's performance of its obligations or a Data Principal's exercise of their rights,

- Right to nominate another individual to exercise these rights in the event of the Data Principal's death or incapacity, in accordance with Applicable Law, and
- Right to approach the Data Protection Board of India, where applicable, after exhausting VITHOS's grievance-redressal mechanism to the extent Applicable Law requires.

22. EXERCISING YOUR RIGHTS

22.1 A User may submit a privacy request by emailing privacy@vithos.in. VITHOS does not, as of the date of this Privacy Policy, offer a dedicated in-app rights-request form; if one is introduced, this Clause will be updated accordingly.

22.2 VITHOS may undertake reasonable identity verification before disclosing, correcting, updating or erasing Personal Data, and may require evidence of authority where a request concerns another person's Personal Data.

22.3 VITHOS will respond to and process valid requests within the timeframe Applicable Law and its published grievance-redressal mechanism prescribe, and may refuse or limit a request only to the extent Applicable Law permits.

23. COOKIES, SDKs AND ANALYTICS

23.1 The VITHOS website and Platform may use cookies, SDKs or equivalent technologies necessary for authentication, session management, security, fraud prevention, User preferences, diagnostics and service performance.

23.2 VITHOS does not run analytics tools on the substantive contents of Users' health records or other sensitive Personal Data, and will not knowingly transmit such content to advertising or general analytics providers unless that Processing has been specifically disclosed and lawfully authorised.

23.3 VITHOS collects analytics limited to aggregate User behaviour on the Platform such as feature usage and navigation patterns to improve the Platform. VITHOS displays a Consent notice for this at the start of a User's use of the Platform, and a User may withdraw that Consent at any time through Settings.

23.4 VITHOS does not use advertising cookies, cross-site tracking technologies or advertising identifiers, and does not serve advertisements within the Platform. If VITHOS introduces any such technology, an appropriate consent-management

mechanism will be implemented before deployment, where Applicable Law requires it, and this Policy will be updated accordingly.

24. ARTIFICIAL INTELLIGENCE AND AUTOMATED PROCESSING

24.1 VITHOS uses third-party AI tools Mistral and OpenAI to extract, analyse and dynamically map information from Users' uploaded medical records into structured form templates within the Platform, so that Users can view and organise their health records.

24.2 VITHOS accesses these tools through commercial API arrangements that contractually prohibit Mistral and OpenAI from using data submitted through the API to train their general-purpose models. Information sent to VITHOS's AI providers for the purpose in Clause 24.1 is Processed solely to deliver that feature to the User, is not used by those providers to train models made available to other customers or the public, and is not used by VITHOS for any independent model training.

24.3 If VITHOS introduces further AI-enabled analysis, summarisation, recommendation, profiling or similar Processing beyond that described in Clause 24.1, it will assess the Processing before deployment and put in place an appropriate lawful basis, privacy notice, Consent where required, purpose limitation, data minimisation, security safeguards and appropriate controls over the relevant third-party AI provider.

25. THIRD-PARTY SERVICES

25.1 The Platform may integrate with third-party authentication, communications, AI or other technology providers.

25.2 Where such a third party acts solely as VITHOS's Data Processor, VITHOS imposes appropriate contractual Processing restrictions, where a third party independently determines the purposes and means of Processing, its activities may additionally be governed by its own privacy notice, which Users should review before providing Personal Data to it directly.

26. DATA PRINCIPAL RESPONSIBILITIES

Users are expected to comply with Applicable Law, provide authentic information and not impersonate another person or provide false particulars, provide another person's Personal Data only where lawfully authorised, maintain the confidentiality of their

account credentials and notify VITHOS promptly of suspected unauthorised access, and exercise their statutory rights responsibly and in accordance with Applicable Law.

27. PRIVACY BY DESIGN

VITHOS endeavours to structure its Processing activities around specified and lawful purposes, data minimisation and purpose limitation, appropriate Consent management, restricted access and confidentiality, reasonable security safeguards, retention limitation, mechanisms for correction and erasure, appropriate oversight of its Data Processors, breach-response preparedness, and accountability for Processing undertaken on its behalf.

28. CHANGES TO THIS PRIVACY POLICY

28.1 VITHOS may amend this Privacy Policy from time to time to reflect changes to the Platform, new features, changes in Processing activities or Applicable Law, regulatory guidance, cybersecurity requirements, changes in VITHOS's service-provider architecture, or VITHOS's incorporation as a formal legal entity. A revised Policy will carry an updated "Last Updated" date.

28.2 Where a change materially affects the Processing of Personal Data, VITHOS will provide appropriate notice by email, in-app notification, website notice or another reasonable means, and will obtain fresh Consent before commencing any new Processing purpose that requires it. Mere continued use of the Platform does not substitute for Consent where Applicable Law requires it.

29. DISCONTINUATION OF VITHOS

29.1 If VITHOS permanently discontinues the Platform, it will, where reasonably practicable, legally permissible and technically feasible, give Users appropriate notice and an opportunity to obtain a copy of their stored health records.

29.2 Following discontinuation, Personal Data will be erased once no longer necessary for the specified purpose, unless retention is required under Applicable Law, and will not become an unrestricted business asset merely because VITHOS ceases operations.

30. GRIEVANCE REDRESSAL

30.1 VITHOS maintains an accessible mechanism through which Data Principals may raise complaints about the Processing of Personal Data, the exercise of privacy rights,

withdrawal of Consent, deletion, security incidents, unauthorised Processing, or any alleged failure by VITHOS to comply with Applicable Law. As of the date of this Privacy Policy, this mechanism operates by email and telephone; VITHOS does not yet offer a dedicated in-app complaint form.

30.2 Complaints may be submitted to the Privacy / Grievance Contact:

Name: Aditya Ghai
Email: privacy@vithos.in
Telephone: +91 70003 25890

30.3 VITHOS will respond to grievances within the period Applicable Law and its published grievance-redressal mechanism prescribe. Where the DPDP Act and applicable Rules permit, a Data Principal who remains dissatisfied after exhausting this mechanism may approach the Data Protection Board of India.

31. DATA PROTECTION OFFICER

31.1 VITHOS will appoint a Data Protection Officer where such appointment becomes mandatory, including if VITHOS is notified as a Significant Data Fiduciary under the DPDP Act, and will publish that officer's business contact information to the extent Applicable Law requires.

31.2 Until a Data Protection Officer is legally required, the privacy/grievance contact identified in Clause 30 serves as the contact point for privacy-related communications.

32. GOVERNMENT AND REGULATORY REQUESTS

32.1 VITHOS may receive lawful requests, notices, orders or directions from courts, regulatory authorities, CERT-In, law-enforcement bodies or governmental authorities, and will disclose Personal Data pursuant to such a request only where disclosure is required or permitted under Applicable Law.

32.2 Where legally permissible, VITHOS may scrutinise, seek clarification of, or challenge a request that appears invalid, excessive or beyond the requesting authority's lawful jurisdiction, and is not required to notify a User of a governmental request where notification is prohibited by Applicable Law or a lawful direction.

33. ABDM AND DIGITAL HEALTH ECOSYSTEM INTEGRATION

33.1 Nothing in this Privacy Policy should be read as representing that VITHOS is presently registered, certified or approved as an ABDM Health Information Provider, Health Information User, Personal Health Record application or other ABDM participant, unless that status has actually been obtained.

33.2 If VITHOS integrates with ABHA, ABDM or another component of the National Digital Health Ecosystem, it will implement the additional consent, security, interoperability, audit and privacy requirements applicable to that integration, and will update this Privacy Policy and relevant consent notices before or alongside deployment where the integration materially changes VITHOS's Processing activities.

34. LANGUAGE AND ACCESSIBILITY OF PRIVACY NOTICES

VITHOS provides privacy and Consent notices in clear and plain language and, where Applicable Law requires it, will offer Data Principals the option to access the applicable notice in English or a language specified in the Eighth Schedule to the Constitution of India. VITHOS maintains appropriate mechanisms enabling Users to access information about withdrawal of Consent, exercise of statutory rights, grievance redressal, and complaints to the Data Protection Board of India.

35. CONTACT INFORMATION

For questions, privacy requests or complaints concerning this Privacy Policy or VITHOS's Processing of Personal Data, please contact:

VITHOS, published on the Google Play Store as "Vithos Labs"
Full legal entity name: _____
Website: www.vithos.in
Contact Person: Aditya Ghai
General Support: support@vithos.in
Privacy: privacy@vithos.in
Telephone: +91 70003 25890

36. GOVERNING LAW

This Privacy Policy and VITHOS's Processing of Personal Data are governed by the laws of India. Nothing in this Privacy Policy excludes, restricts or waives any statutory right of a Data Principal, or any obligation imposed on VITHOS that cannot lawfully be excluded, restricted or waived.

37. SEVERABILITY

If any provision of this Privacy Policy is found to be unlawful, invalid or unenforceable under Applicable Law, that provision will, to the extent possible, be interpreted or modified to give effect to its lawful purpose, and the remaining provisions will continue in full force and effect.

38. PRIVACY POLICY VERSION

Version: 1.0
Effective Date: 14/08/2026
Last Updated: 14/08/2026

© [2026] VITHOS (Vithos Labs). All rights reserved.