



Anxya Tech Private Limited · CIN U62099PN2024PTC230490

Data Processing & Business Associate Agreements

Prepared by Anxya Health, Legal & Compliance
Generated 02 Oct 2026

Data Processing & Business Associate Agreements

Data Processing & Business Associate Agreements

Anxya Tech Private Limited — CIN: U62099PN2024PTC230490 — Pune, Maharashtra, India ·
privacy@anxya.health

Effective: 1 June 2026

This document sets out the standard data-protection terms Anxya Health offers to enterprise customers (pharma, hospital, payer, provider and similar) who process personal or health data through the Service. It comprises Part A — Data Processing Agreement (DPA) and Part B — HIPAA Business Associate Agreement (BAA). A negotiated, countersigned copy is executed per customer — email privacy@anxya.health.

Part A — Data Processing Agreement (DPA)

This DPA forms part of the agreement between the customer ("Controller") and Anxya Tech Private Limited ("Processor") and reflects GDPR Article 28 and the India DPDP Act, 2023.

1. Roles & subject matter. The Controller determines the purposes and means of processing; the Processor processes personal data only to provide the Service and on the Controller's documented instructions. Duration follows the underlying subscription.
2. Nature & purpose. Hosting, generating, storing and returning outputs from Controller data (including uploaded documents and queries) via the Service and its AI sub-processors, solely to deliver the requested functionality.
3. Categories of data & data subjects. Account users and any personal data the Controller submits (e.g., patient, employee or research-subject data). The Controller is responsible for the lawful basis of any special-category / health data it submits.
4. Sub-processors. The Controller authorises the sub-processors listed in the Anxya Privacy Policy (cloud/hosting, AI model providers, email and payment providers). The Processor imposes data-protection terms on each, remains liable for their performance, and will give notice of material changes with a right to object.
5. Security (Art. 32). Encryption in transit, hashed credentials, access controls, de-identification for research cohorts, logging and least-privilege administration appropriate to the risk.
6. Data-subject requests & assistance. The Processor will assist the Controller with data-subject rights, DPIAs and prior consultations by appropriate technical and organisational measures.
7. Personal-data breach. The Processor will notify the Controller without undue delay after becoming aware of a personal-data breach affecting Controller data, with information reasonably available.
8. International transfers. Where data leaves its region, the Processor relies on Standard Contractual Clauses, adequacy decisions or equivalent safeguards.
9. Return & deletion. On termination, the Processor will delete or return Controller personal data within a commercially reasonable period, subject to legal retention, and delete residual copies on backup rotation.
10. Audits. The Processor will make available information necessary to demonstrate compliance and allow for reasonable audits, on notice and subject to confidentiality.

Part B — HIPAA Business Associate Agreement (BAA)

Applies where the customer is a HIPAA Covered Entity (or Business Associate) and Protected Health Information ("PHI") is processed. Anxya acts as Business Associate.

1. Permitted uses & disclosures. The Business Associate may use or disclose PHI only to perform the Service, as permitted by this BAA, or as required by law, and will not use PHI for any purpose the Covered Entity could not.
2. Safeguards. Administrative, physical and technical safeguards consistent with the HIPAA Security Rule to protect electronic PHI.
3. Reporting. The Business Associate will report any impermissible use/disclosure, Security Incident, and Breach of Unsecured PHI without unreasonable delay.
4. Subcontractors. Subcontractors that handle PHI agree to the same restrictions and conditions.
5. Individual rights. The Business Associate will make PHI available for access, amendment and an accounting of disclosures per 45 CFR §§164.524, 164.526 and 164.528.
6. Return or destruction. On termination, PHI is returned or destroyed where feasible; where not feasible, protections continue for as long as PHI is retained.
7. Governing terms. This BAA supplements the DPA and the main agreement. For PHI conflicts, this BAA controls.

Note. This is a standard template for review; a signed, negotiated agreement is executed per customer. Anxya Health holds no organizational certifications (no SOC 2, no ISO/IEC 42001); these agreements describe contractual data-protection commitments, not a certification.

Signed for the Controller/Covered Entity: Date:

Signed for Anxya Tech Private Limited: Date: