

Business Associate Agreement

Kestra Labs LLC • Last Updated: March 1, 2026

Availability: The BAA is available on the Zero Trust tier only. Contact sales@kestralabs.com to execute.

1. Purpose

This Business Associate Agreement ("BAA") is required when Customer is a Covered Entity or Business Associate under HIPAA and uses the Service to process Protected Health Information ("PHI"). Kestra Labs agrees to be designated as a Business Associate.

2. Permitted Uses

Kestra Labs may use or disclose PHI solely for: performing its obligations under the Service Agreement, and as required by law. Kestra Labs will not use or disclose PHI for marketing, sell PHI, or use PHI for any purpose not expressly permitted.

3. Safeguards

Kestra Labs implements administrative, physical, and technical safeguards appropriate to protect PHI including: Zero Trust tier mTLS (PHI credentials never stored in our infrastructure), PII redaction engine configured to detect and mask PHI fields (patient names, MRNs, dates of birth), AES-256 encryption at rest with customer-managed keys, TLS 1.3 encryption in transit, and access controls limiting Kestra Labs personnel access to PHI to those with a demonstrated need.

4. Breach Notification

Kestra Labs will report any Breach of Unsecured PHI to Customer without unreasonable delay and no later than 30 calendar days after discovery. Report will include: identification of each individual affected (if known), description of the breach, types of PHI involved, and remediation steps taken.

5. Subcontractors

Kestra Labs will ensure that any subcontractor that creates, receives, maintains, or transmits PHI on behalf of Kestra Labs agrees to substantially similar restrictions as contained in this BAA.

6. Audit and Access

Kestra Labs will make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of HHS for purposes of determining Customer's compliance with HIPAA. Kestra Labs will provide access to PHI within 10 business days of a written request.

7. Termination

Upon termination, Kestra Labs will return or destroy all PHI received from Customer or created on Customer's behalf. If return or destruction is not feasible, Kestra Labs will extend the protections of this BAA to the remaining PHI and limit further uses and disclosures to those purposes that make return or destruction infeasible.