Business Associate Agreement

This Business Associate Agreement ("BAA") is required for HIPAA-covered entities using Genos to process protected health information (PHI).

1. Definitions

For purposes of this Agreement, the following terms shall have the meanings set forth below:

- "Covered Entity" refers to the organization or individual practitioner that subscribes to Genos and is subject to the HIPAA Privacy and Security Rules.
- "Business Associate" refers to Genos ("Company"), which creates, receives, maintains, or transmits Protected Health Information on behalf of the Covered Entity.
- "Protected Health Information" (PHI) means any individually identifiable health information as defined under 45 CFR §160.103, transmitted or maintained in any form or medium by the Business Associate on behalf of the Covered Entity.
- "Electronic Protected Health Information" (ePHI) means PHI that is transmitted or maintained in electronic media.
- "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

2. Permitted Uses and Disclosures

The Business Associate may use or disclose PHI only as follows:

1. As necessary to perform services on behalf of the Covered Entity as described in the underlying service agreement, including but not limited to: data storage, data processing, clinical data encryption, and generation of AI-assisted clinical insights.
2. As required by law, including compliance with HIPAA regulations, court orders, or lawful subpoenas.
3. For the proper management and administration of the Business Associate, provided that any disclosure is required by law or the Business Associate obtains reasonable assurances from any third party that the information will be held confidentially.

The Business Associate shall not use or disclose PHI for any purpose other than those listed above or as otherwise required by law.

3. Safeguards

The Business Associate shall implement the following safeguards to protect PHI:

3.1 Administrative Safeguards

- Designate a Security Officer responsible for development and implementation of security policies.
- Conduct regular risk assessments to identify threats to ePHI confidentiality, integrity, and availability.
- Implement workforce training on privacy and security policies.
- Maintain written policies and procedures for HIPAA compliance.

3.2 Physical Safeguards

- Infrastructure hosted in SOC 2 Type II certified data centers (Supabase, Vercel, AWS).
- Physical access to servers controlled by infrastructure providers with documented access controls.

3.3 Technical Safeguards

- All ePHI encrypted at rest using AES-256-GCM with per-tenant encryption keys managed via envelope encryption.
- All data in transit encrypted using TLS 1.3 with forward secrecy.

- Role-based access controls (RBAC) enforced at both application and database levels.
- PostgreSQL Row-Level Security (RLS) policies enforce strict multi-tenant data isolation.
- Comprehensive audit logging of all ePHI access and modifications.
- Encryption key rotation capability without service interruption.

4. Breach Notification

1. The Business Associate shall report to the Covered Entity any use or disclosure of PHI not provided for in this Agreement of which the Business Associate becomes aware, including any Security Incident or Breach of Unsecured PHI.
2. Notification of a Breach shall be provided to the Covered Entity without unreasonable delay and in no case later than thirty (30) calendar days after discovery of the Breach.
3. The notification shall include, to the extent possible: identification of affected individuals, description of the Breach, steps taken to investigate and mitigate, and contact information for a representative.
4. The Business Associate shall cooperate with the Covered Entity in the investigation of any Breach and in the fulfillment of the Covered Entity's obligations under HIPAA Breach Notification Rules.

5. Termination

1. Term. This Agreement shall remain in effect for the duration of the underlying service agreement between the parties.
2. Termination for Cause. Either party may terminate this Agreement if it determines that the other party has violated a material term. The non-breaching party shall provide written notice and allow thirty (30) days to cure.
3. Obligations on Termination. Upon termination, the Business Associate shall return or destroy all PHI, or extend protections if return/destruction is not feasible.
4. Data Export. Prior to termination, the Covered Entity may request a complete export of their data. The Business Associate shall provide the export in a standard, machine-readable format within thirty (30) business days.

To execute this BAA, please contact us at legal@genos.app with your organization name and the name of the authorized signatory.