Security & HIPAA Compliance

Senavida

Senavida is built for healthcare. Protecting the health information entrusted to our platform is central to how we operate. This page summarizes how we approach privacy and security and how we support our customers' HIPAA compliance. It is provided for information; the binding terms are set out in our Business Associate Agreement and services agreement.

Our role under HIPAA

Senavida provides a software platform that healthcare providers and practices use to deliver care and manage their work. When we create, receive, maintain, or transmit protected health information ("PHI") on a customer's behalf, we act as a **business associate** under HIPAA. The provider or practice remains the covered entity responsible for the patient relationship; Senavida handles PHI only to provide the services and only as permitted by our agreement with that customer.

Business Associate Agreements

We enter into a Business Associate Agreement (BAA) with every covered-entity customer before handling PHI on their behalf. The BAA defines how we may use and protect PHI, our breach-notification commitments, and our obligations to bind any subcontractors to equivalent terms. A BAA is part of customer onboarding and is available on request.

How we safeguard your data

We maintain an information security program designed to meet the HIPAA Security Rule, with administrative, physical, and technical safeguards that include:

- Encryption of data in transit and at rest;
- Role-based access controls and least-privilege access to PHI;
- Multi-factor authentication for access to systems that handle PHI;
- Audit logging and monitoring of access and activity;
- A secure software development lifecycle, change management, and vulnerability management;
- Regular risk assessments and documented policies and procedures; and
- Workforce confidentiality obligations and recurring HIPAA privacy and security training.

Subprocessors

We rely on a limited set of vetted infrastructure and service providers to operate the platform. Where these subprocessors handle PHI, they are bound by agreements at least as protective as our own obligations. For a current list of subprocessors send a request to support@senavida.com.

Breach notification

We maintain a documented process to detect, investigate, and respond to security incidents. If a reportable breach of unsecured PHI occurs, we notify the affected customer promptly and provide

the information they need to meet their own notification obligations, consistent with our agreements and HIPAA.

Shared responsibility

Security is a shared effort. Senavida secures the platform and the infrastructure it runs on. Customers are responsible for matters within their control — for example, managing their own user accounts and access, configuring the product appropriately, maintaining their Notice of Privacy Practices, and obtaining any required patient consents.

Contact

To request a BAA, ask a security question, or report a concern, contact us at support@senavida.com. For questions about your own health records, please contact your healthcare provider.