Data Privacy & Handling

Senavida | Business Associate (HIPAA-regulated SaaS)

Policy title: Data Privacy & Handling Policy

Organization role: Business Associate (HIPAA-regulated SaaS platform)

Policy owner: Augustine W. Walsh Jr, Founder

Effective date: June 24, 2026 **Version:** 1.0 **Next scheduled review:** 06/30/2027

Applies to: All Senavida workforce members, contractors, volunteers, and subcontractors who access, process, or support the platform.

1. Purpose and Scope

This Data Privacy & Handling Policy (the "Policy") describes how **Senavida** (the "Organization," "we," "our," or "us") collects, uses, protects, shares, retains, and disposes of the data entrusted to us. It reflects a single guiding principle: your data is yours. We handle it only to deliver and support our services, only as our agreements and applicable law permit, and always under safeguards designed to keep it confidential and secure.

Senavida operates a software-as-a-service platform that creates, receives, maintains, and/or transmits data — including Protected Health Information ("PHI") — on behalf of its customers. Where that data is PHI, our handling is also governed by our *HIPAA Compliance — Privacy & PHI-Handling Policy*, our Business Associate Agreements ("BAAs"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the HITECH Act and the HIPAA Omnibus Rule. This Policy complements, and does not replace, those documents; where a BAA or the HIPAA policy is more specific or more protective, that document governs.

This Policy applies to all data Senavida processes in any form — electronic, paper, or oral — and to every member of Senavida's workforce, its contractors, and its subcontractors. Where applicable state law, including Texas law, provides individuals greater protection, the more protective standard applies.

2. Policy Statement

It is the policy of Senavida to treat all customer and personal data as confidential and belonging to the customer and the individuals it concerns; to collect and use only the data necessary for a legitimate, disclosed purpose; to protect data with strong administrative, physical, and technical safeguards, including end-to-end encryption; to never sell personal information; to share data with third parties only with authorization or as law requires; to be transparent about our practices; and to support customers and individuals in exercising their rights over their data.

3. Key Definitions

- **Personal Data / Personal Information:** information that identifies, relates to, or could reasonably be linked to an identified or identifiable individual or household.

- **Protected Health Information (PHI):** individually identifiable health information, in any form, that Senavida creates, receives, maintains, or transmits on behalf of a customer.
- **Customer Data:** all data, including Personal Data and PHI, that a customer or its authorized users submit to, or that is generated within, the Senavida platform.
- **Processing:** any operation performed on data, including collection, access, use, storage, transmission, disclosure, retention, and deletion.
- **De-identified Data:** data from which identifiers have been removed such that it no longer identifies, and cannot reasonably be used to identify, an individual, consistent with 45 C.F.R. § 164.514.
- **Subprocessor:** a third party engaged by Senavida to process data on our behalf in support of the platform (for example, a hosting or infrastructure provider).

4. Data Ownership and Customer Control

Senavida does not own the Customer Data it processes. Customer Data belongs to, and is controlled by, the customer and the individuals it concerns. Senavida processes Customer Data solely to provide and support the contracted platform and services, and only as the applicable agreement, BAA, and law permit. Nothing in this Policy grants Senavida rights to Customer Data beyond what those documents expressly allow. Customers retain the ability to access, export, correct, and request deletion of their data as provided in their agreement and, for PHI, as described in our HIPAA policy.

5. Categories of Data We Handle

The specific data Senavida processes depends on how a customer configures and uses the platform. Typical categories include:

- **Account and contact data:** names, business email addresses, roles, and authentication credentials for authorized users.
- **Customer-submitted content:** records and information a customer or its users enter into or upload to the platform, which may include PHI.
- **Usage and log data:** technical records such as access logs, audit events, device and browser information, and diagnostic data used to secure, operate, and improve the service.
- **Support data:** information provided when a customer contacts us for assistance.

We do not seek to collect more data than the platform and the customer's configuration require.

6. Purpose Limitation and Lawful Basis

Senavida processes data only for the purposes for which it was provided: to deliver, maintain, secure, support, and improve the platform for our customers; to meet our contractual and legal obligations; and to protect the rights, safety, and property of our customers, their users, and Senavida. We do not process Customer Data for our own independent purposes, and we do not repurpose data for uses incompatible with why it was collected. Where PHI is involved, permitted uses and disclosures are limited to those set out in the applicable BAA and our HIPAA policy.

7. Data Minimization

We apply the principle of data minimization and, for PHI, the HIPAA minimum-necessary standard: we collect, use, disclose, and request only the data reasonably needed to accomplish the intended purpose. Workforce and system access to data is restricted by role and function, so individuals can reach only the data their responsibilities require.

8. No Sale of Personal Information

Senavida does not sell personal information, and we do not share it with third parties for their own marketing or independent commercial purposes. We do not exchange personal information for money or other valuable consideration. We do not use Customer Data or PHI to build advertising profiles. PHI is never sold and is never used for marketing except as expressly permitted by HIPAA and the applicable BAA.

9. Sharing and Disclosure of Data

Senavida discloses data only in limited, defined circumstances:

- **To the customer and its authorized users,** as part of providing the service.
- **To subprocessors** that support the platform, under written contracts that bind them to protections at least as strict as those in this Policy and, for PHI, under subcontractor BAAs (see Section 12).
- **With the customer's or individual's authorization,** where a specific disclosure has been directed or consented to.
- **As required by law,** such as to comply with a valid legal process, provided we assess each request and disclose only what is required.
- **To protect rights and safety,** where necessary to prevent harm, fraud, or abuse, consistent with law and the applicable agreement.

Outside these circumstances, Senavida does not share personal information or PHI with third parties without the customer's explicit consent.

10. Encryption and Data Protection

Senavida protects data with layered administrative, physical, and technical safeguards. Among them:

- **Encryption in transit:** data moving between users and the platform, and between platform components, is encrypted using current industry-standard transport protocols.
- **Encryption at rest:** stored data, including PHI, is encrypted using strong, industry-standard algorithms, with keys managed under controlled procedures.
- **Access controls:** role-based access control, unique user identity, and authentication requirements limit who can reach data.
- **Audit logging and monitoring:** access to and activity on the platform is logged and monitored to detect and investigate unauthorized or unusual activity.

These measures are described more fully in Senavida's *Infrastructure & Security* documentation and Information Security Policy.

11. Data Retention and Disposal

Senavida retains Customer Data for as long as needed to provide the service and to meet legal, regulatory, and contractual obligations. On termination or expiration of an agreement, Senavida returns or securely destroys Customer Data, including PHI, as the agreement or BAA directs, except where retention is required by law. Documentation required by HIPAA is retained for at least six (6) years, or longer where state law or a BAA requires. Disposal is carried out using methods designed to render data unreadable and unrecoverable.

12. Subprocessors

Before allowing any subprocessor to process data on Senavida's behalf, we obtain written assurances — through a data-processing or subcontractor Business Associate Agreement — that the subprocessor will

apply protections at least as strict as those we are bound by under our agreements and HIPAA. Senavida maintains a current inventory of subprocessors that handle Customer Data and PHI and remains responsible for their compliance in support of the platform.

13. Supporting Individual Rights

Individuals exercise their privacy rights through the customer (the covered entity or controller), not through Senavida directly. As a business associate and processor, Senavida supports its customers in honoring those rights. The table below summarizes our supporting role:

Right	Senavida's supporting role
Access / portability	Make the relevant data available to the customer (or, if delegated, the individual) so a request can be fulfilled, and support export in a usable format.
Correction / amendment	Incorporate corrections or amendments the customer directs into the data Senavida maintains.
Deletion	Delete or return data at the customer's direction, subject to legal retention requirements.
Accounting of disclosures	Maintain and provide information about disclosures Senavida makes, so the customer can respond to a request.
Restrictions / confidential communications	Honor restrictions and alternative-communication arrangements the customer has agreed to, where they affect data Senavida handles.

Senavida routes any privacy request it receives directly from an individual to the relevant customer for handling, unless an agreement or BAA assigns that responsibility to Senavida.

14. Transparency

Senavida is committed to transparent data-handling practices. We describe the data we process and how we protect it in our Trust Center, our agreements, and this Policy. We notify affected customers of material changes to how we handle data, and we respond to reasonable questions about our practices.

15. Data Incident and Breach Handling

If Senavida discovers an acquisition, access, use, or disclosure of data not permitted by its agreement, BAA, or HIPAA, it follows its *Breach Reporting & Process* procedure to assess the incident and notify the affected customer (and, where delegated, others) within required timeframes. That procedure is incorporated into this Policy by reference.

16. Workforce Training and Accountability

All workforce members receive training on this Policy and related privacy and security procedures shortly after joining, when material changes occur, and periodically thereafter; training is documented and records are retained. Workforce members who fail to comply are subject to disciplinary action up to and including termination. Senavida will not retaliate against any person for reporting a concern, filing a complaint, or participating in an investigation.

17. Contact

Questions, requests, or concerns about this Policy or Senavida's data-handling practices may be directed to Senavida's Privacy and Security Officer, Anthony Centi, at **support@senavida.com**.

18. Review and Revision

This Policy is reviewed at least annually and revised as needed to reflect changes in law, regulation, customer agreements, or Senavida's operations.