Compliance & Certifications

Senavida | Business Associate (HIPAA-regulated SaaS)

Policy title: Compliance & Certifications 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 Compliance & Certifications Policy (the "Policy") describes how **Senavida** (the "Organization," "we," "our," or "us") governs its compliance program and aligns its security and privacy practices with applicable laws, regulations, and industry frameworks. Senavida is committed to maintaining a high standard of compliance, and our practices are regularly reviewed and updated to keep pace with evolving regulations and industry standards.

As a HIPAA business associate operating a software-as-a-service platform, Senavida is directly subject to the HIPAA Security Rule, the Breach Notification Rule, and the business-associate provisions of the Privacy Rule, in addition to the terms of each Business Associate Agreement ("BAA"). This Policy works alongside Senavida's *HIPAA Compliance — Privacy & PHI-Handling Policy*, *Data Privacy & Handling Policy*, and *Infrastructure & Security* documentation.

Note on certification status: this Policy describes the frameworks Senavida aligns with and its compliance approach. Where a specific attestation, certification, or audit report is referenced, its current status should be confirmed against Senavida's live records before being represented to a customer. Placeholder status entries below are provided for the Organization to complete and maintain.

2. Policy Statement

It is the policy of Senavida to meet its legal and contractual obligations; to align its controls with recognized security and privacy frameworks; to assess and manage risk on an ongoing basis; to maintain accurate documentation and evidence of its controls; to hold subprocessors to equivalent standards; to train its workforce; and to continuously improve its compliance posture as laws, regulations, and industry expectations evolve.

3. Compliance Governance

Senavida's compliance program is owned by the Founder and administered by the designated Privacy and Security Officer, who is responsible for developing, implementing, and maintaining the program and for receiving compliance-related questions and reports. The Officer coordinates risk assessments, policy maintenance, control monitoring, audit activity, and remediation, and reports on the program's status to leadership.

4. Regulatory Framework

Senavida identifies and tracks the laws and regulations applicable to its role and its customers, and designs its controls to meet them. Core obligations include:

- **HIPAA / HITECH:** the HIPAA Security Rule, Breach Notification Rule, and business-associate provisions of the Privacy Rule, as amended by the HITECH Act and the HIPAA Omnibus Rule.
- **State privacy and breach-notification laws:** applicable state requirements, including Texas law; where state law is more protective, the more protective standard governs.
- **Contractual obligations:** the terms of each customer BAA and service agreement, which may impose additional or more specific requirements.

Senavida monitors regulatory developments and updates its policies and controls as obligations change.

5. Industry Frameworks and Standards

Beyond legal requirements, Senavida aligns its controls with recognized industry frameworks to provide customers with well-understood assurance. The table below lists the frameworks Senavida references and a status field for the Organization to maintain. Status values may include, for example: *Aligned*, *In progress*, *Audit scheduled*, or *Attestation available*.

Framework / standard	Relevance to Senavida	Status
HIPAA Security Rule	Baseline regulatory requirement for safeguarding ePHI as a business associate.	**Directly subject**
SOC 2 (Trust Services Criteria)	Independent assurance over security, availability, and confidentiality controls.	*[To be completed]*
ISO / IEC 27001	Framework for an information security management system (ISMS).	*[To be completed]*
NIST frameworks (e.g., CSF / SP 800-53)	Reference for risk-based control selection and security program maturity.	Referenced
HITRUST CSF	Healthcare-oriented control framework mapping to HIPAA and other standards.	*[To be completed]*

Senavida represents its certification and attestation status accurately and only claims a certification once it has been formally achieved and is current. Customers may request available reports, summaries, or evidence, subject to confidentiality terms.

6. Business Associate Agreements

Senavida enters into a Business Associate Agreement with every customer that is a covered entity or business associate before creating, receiving, maintaining, or transmitting PHI on that customer's behalf. Each BAA defines and limits permitted uses and disclosures, sets breach-reporting timeframes, and addresses return or destruction of PHI on termination. Where a BAA is more restrictive than Senavida's policies, the BAA controls. Senavida likewise binds its subprocessors through subcontractor BAAs to protections at least as strict.

7. Risk Management and Assessment

Senavida maintains a documented risk analysis and risk management process. Risks to the confidentiality, integrity, and availability of ePHI and other data are identified, evaluated by likelihood and impact, and addressed through prioritized remediation. Risk assessments are performed periodically and when significant changes occur, and results inform the compliance program and control roadmap.

8. Policies, Documentation, and Evidence

Senavida maintains a documented set of privacy and security policies and procedures, and retains the records, activities, and designations HIPAA requires. Documentation is kept for at least six (6) years from the date of creation or the date last in effect, whichever is later, and longer where state law or a BAA requires. Senavida retains evidence of control operation — such as logs, training records, review records, and assessment results — to support audits and customer due diligence.

9. Vendor and Subprocessor Risk Management

Senavida evaluates the security and compliance posture of subprocessors before engagement and periodically thereafter. Subprocessors that handle PHI are bound by subcontractor BAAs and are expected to maintain their own recognized security and compliance programs. Senavida maintains a current inventory of subprocessors and remains accountable for their compliance in support of the platform.

10. Audits, Monitoring, and Continuous Improvement

Senavida's controls are monitored on an ongoing basis and assessed through internal reviews and, where applicable, independent assessments such as penetration testing and third-party audits. Findings are tracked to remediation. Senavida treats compliance as a continuous process: as regulations and industry frameworks evolve, Senavida updates its controls, policies, and roadmap accordingly.

11. Workforce Training and Awareness

All workforce members receive training on Senavida's privacy, security, and compliance obligations 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, and Senavida will not retaliate against anyone for raising a concern, filing a complaint, or participating in an investigation.

12. Breach and Incident Compliance

If Senavida discovers an acquisition, access, use, or disclosure of PHI not permitted by a 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 and supports Senavida's obligations under the Breach Notification Rule and applicable state law.

13. Customer Assurance and Trust Center

Senavida supports customer due diligence through its Trust Center, which provides its compliance and security documentation, and by responding to reasonable security and compliance inquiries, questionnaires, and requests for available reports, subject to confidentiality terms. This Policy and the accompanying Trust Center materials are intended to give customers a clear, accurate view of Senavida's compliance posture.

14. Contact

Compliance questions, requests for documentation, or reports may be directed to Senavida's Privacy and Security Officer, Anthony Centi, at **support@senavida.com**.

15. Review and Revision

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