# Infrastructure & Security

*Senavida | Business Associate (HIPAA-regulated SaaS)*

**Policy title: Infrastructure & Security 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 Infrastructure & Security Policy (the "Policy") describes the technical and organizational controls **Senavida** (the "Organization," "we," "our," or "us") uses to protect its platform and the data it processes. Senavida runs on enterprise-grade infrastructure with continuous monitoring, automated threat detection, and regular security assessments, and follows industry best practices for secure software development and change management.

As a HIPAA business associate, Senavida is directly and fully subject to the HIPAA Security Rule (45 C.F.R. Part 164, Subpart C) and maintains a documented information security program covering administrative, physical, and technical safeguards for electronic Protected Health Information ("ePHI"). This Policy summarizes that program. It works alongside Senavida's *HIPAA Compliance — Privacy & PHI-Handling Policy* and *Data Privacy & Handling Policy*; where a Business Associate Agreement ("BAA") is more restrictive, the BAA governs.

This Policy applies to all Senavida production systems, supporting infrastructure, and personnel who build, operate, or support the platform.

## 2. Policy Statement

It is the policy of Senavida to protect the confidentiality, integrity, and availability of the platform and the data it processes through defense-in-depth; to encrypt data in transit and at rest; to restrict access by role and least privilege; to monitor continuously and respond quickly to threats; to build and change software securely; to maintain resilient, recoverable systems; and to hold its workforce and subprocessors accountable for security.

## 3. Key Definitions

- **ePHI:** Protected Health Information created, received, maintained, or transmitted in electronic form.
- **Least Privilege:** granting each user, system, or process only the access needed to perform its function, and no more.
- **Defense-in-Depth:** the use of multiple, layered safeguards so that the failure of any one control does not lead to compromise.
- **Subprocessor:** a third party engaged to process data or provide infrastructure on Senavida's behalf.

- **Production Environment:** the systems that store or process Customer Data and deliver the live platform to customers.

## 4. Security Governance

Senavida designates a Security Official responsible for developing, implementing, and maintaining the information security program. Security roles and responsibilities are defined, and security policies are documented, approved, and reviewed at least annually. Risk is managed through a documented risk analysis and risk management process that identifies threats and vulnerabilities to ePHI and drives remediation based on likelihood and impact.

## 5. Cloud Infrastructure and Hosting

Senavida's platform runs on enterprise-grade cloud infrastructure operated by established providers that maintain their own recognized security and compliance programs. Senavida enters into Business Associate Agreements or equivalent data-protection agreements with infrastructure providers that handle ePHI. Production infrastructure is provisioned through controlled, repeatable processes, and configuration is managed to enforce secure, consistent baselines. Production is logically separated from development and testing environments.

## 6. Network Security

Senavida applies layered network controls to limit exposure and contain risk:

- **Segmentation:** production systems are isolated and segmented so that access to one component does not grant access to others.
- **Perimeter controls:** firewalls and security groups restrict inbound and outbound traffic to what is required.
- **Encrypted transport:** external and internal service communications use current industry-standard transport encryption.
- **Boundary protection:** administrative interfaces are restricted, and public exposure of services is minimized.

## 7. Encryption and Key Management

Senavida encrypts ePHI and other sensitive data both in transit and at rest using strong, industry-standard algorithms. Data moving between users and the platform, and between platform components, is protected with current transport encryption; stored data is encrypted at rest. Encryption keys are managed under controlled procedures, with access to key material restricted and monitored, and keys rotated according to defined practices.

## 8. Identity and Access Management

Access to Senavida systems and data is governed by least privilege and role-based access control. Each user has a unique identity; shared accounts are avoided. Access to production systems and ePHI requires authentication, and privileged and remote access require multi-factor authentication. Access is granted through an approval process, reviewed periodically, and promptly revoked upon role change or separation. Authentication events and privileged actions are logged.

## 9. Continuous Monitoring and Threat Detection

Senavida monitors its environment continuously to detect and respond to security-relevant events:

- **Audit logging:** security-relevant events — access, administrative actions, and configuration changes — are logged and retained.
- **Automated threat detection:** monitoring and alerting identify anomalous or unauthorized activity for investigation.
- **Log integrity:** logs are protected against unauthorized alteration and reviewed as part of security operations.
- **Alerting and triage:** defined thresholds generate alerts that are triaged and escalated through the incident-response process.

## 10. Vulnerability and Patch Management

Senavida maintains a vulnerability management process that includes regular scanning of infrastructure and application components, tracking of identified issues, and remediation prioritized by severity within defined timeframes. Security patches for operating systems, dependencies, and platform components are applied on a risk-based schedule. Senavida conducts, and/or engages qualified third parties to conduct, periodic security assessments and penetration testing, and remediates findings through its risk management process.

## 11. Secure Software Development

Senavida follows industry best practices for secure software development throughout the development lifecycle:

- **Secure design and coding:** security requirements are considered in design, and developers follow secure coding practices to address common classes of vulnerabilities.
- **Code review:** changes are peer-reviewed before merging to production branches.
- **Automated checks:** testing and security tooling are integrated into the build and deployment pipeline.
- **Dependency management:** third-party components are inventoried and monitored for known vulnerabilities.
- **Environment separation:** development and testing use non-production data wherever practicable and are isolated from production.

## 12. Change and Release Management

Senavida maintains rigorous change management processes. Changes to production are documented, reviewed, tested, and approved before release, and are deployed through controlled, repeatable pipelines that support traceability and rollback. Emergency changes follow an expedited but documented path with retrospective review. These controls reduce the risk that changes introduce security weaknesses or service disruption.

## 13. Business Continuity, Backups, and Disaster Recovery

Senavida protects the availability and recoverability of the platform and ePHI. Data is backed up on a regular schedule, backups are encrypted, and restoration is tested periodically to verify recoverability. Senavida maintains a data-backup and disaster-recovery plan and a contingency plan consistent with the HIPAA Security Rule, with defined objectives for recovery, so that operations and data can be restored following a disruptive event.

## 14. Endpoint and Workforce Security

Workforce devices that access Senavida systems are subject to security requirements such as disk encryption, endpoint protection, screen locking, and timely patching. Access from workforce devices follows the same least-privilege and authentication requirements as other access. Workforce members receive security awareness training and are bound by acceptable-use and confidentiality obligations.

## 15. Physical Security

Production infrastructure is hosted in facilities operated by cloud providers that maintain robust physical and environmental controls, including restricted facility access, monitoring, and environmental protections. Senavida workforce members do not store ePHI on unmanaged local media, and physical materials containing sensitive data, if any, are secured and disposed of using methods that render data unrecoverable.

## 16. Incident Response

Senavida maintains an incident-response capability to identify, contain, investigate, and remediate security incidents. If an incident involves an acquisition, access, use, or disclosure of PHI not permitted by a BAA or HIPAA, Senavida 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. Lessons learned are used to strengthen controls.

## 17. Third-Party and Subprocessor Security

Before engaging a subprocessor that will access infrastructure or ePHI, Senavida evaluates its security posture and binds it, through a subcontractor BAA or equivalent agreement, to protections at least as strict as those Senavida is subject to. Senavida maintains a current inventory of subprocessors that support the platform and periodically reviews their security.

## 18. Security Assessments and Assurance

Senavida's security practices are reviewed and updated on a regular basis. This includes internal reviews, risk assessments, vulnerability scanning, and periodic independent testing, together with alignment to recognized industry frameworks as described in Senavida's *Compliance & Certifications* documentation. Findings are tracked to remediation.

## 19. Contact

Security questions, concerns, or vulnerability reports may be directed to Senavida's Security Official, Anthony Centi, at **support@senavida.com**.

## 20. Review and Revision

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