HIPAA Breach Reporting & Process

Senavida | Business Associate (HIPAA-regulated SaaS)

Procedure title: HIPAA Breach Reporting & Process

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

Procedure owner: Anthony Centi, Co-Founder/Security Officer

Effective date: 06/24/2026 **Version:** 1.0 **Next scheduled review:** 09/30/2026

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

1. Purpose and Scope

This procedure establishes how **Senavida** (the "Organization"), in its role as a **business associate**, identifies, investigates, documents, and reports breaches of unsecured PHI in accordance with the HIPAA Breach Notification Rule (45 C.F.R. §§ 164.400–414, and specifically § 164.410 governing business associates), the HITECH Act, applicable state law, and the Organization's Business Associate Agreements ("BAAs").

Senavida's primary breach obligation is to notify the affected **customer** — the covered entity or business associate on whose behalf Senavida holds the PHI — promptly and with the information that customer needs. The customer is generally responsible for notifying affected individuals, the Secretary of HHS, and the media, unless a BAA delegates some or all of those notifications to Senavida. This procedure applies to PHI in any form and to all members of Senavida's workforce and its subcontractors.

2. Key Definitions

- **Breach:** the acquisition, access, use, or disclosure of PHI not permitted by the Privacy Rule that compromises the security or privacy of the PHI. An impermissible use or disclosure is **presumed** to be a breach unless a low probability of compromise is demonstrated through the risk assessment in Section 5.
- **Unsecured PHI:** PHI not rendered unusable, unreadable, or indecipherable to unauthorized persons through encryption or destruction consistent with HHS guidance. Properly encrypted or destroyed PHI is not "unsecured."
- **Security incident:** an attempted or successful unauthorized access, use, disclosure, modification, or destruction of information, or interference with system operations. Not every incident is a breach, but every incident involving PHI is assessed under this procedure.
- **Discovery:** a breach is treated as discovered on the first day it is known, or by reasonable diligence would have been known, to any Senavida workforce member or agent other than the person who committed it.
- **Customer:** the covered entity or business associate for whom Senavida processes PHI and to whom Senavida must report breaches.

3. Breach Determination and Exceptions

An impermissible use or disclosure of unsecured PHI is presumed to be a breach. The presumption does not apply, and reporting is not required, where one of the following exceptions is met and documented:

1. **Good-faith, unintentional access by workforce.** Unintentional acquisition, access, or use of PHI by a workforce member or person acting under Senavida's authority, in good faith and within scope, and not further used or disclosed impermissibly.
2. **Inadvertent disclosure between authorized persons.** Inadvertent disclosure between persons authorized to access PHI at Senavida (or at the customer or another business associate within the same arrangement), where the PHI is not further used or disclosed impermissibly.
3. **Good-faith belief information could not be retained.** A disclosure where Senavida has a good-faith belief that the unauthorized recipient could not reasonably have retained the PHI.

If no exception applies, Senavida performs the risk assessment in Section 5 to determine whether the incident is a reportable breach.

4. Discovery and Internal Escalation

Reporting deadlines run from the date of discovery, so prompt internal escalation is essential:

1. **Report immediately.** Any workforce member who becomes aware of a suspected or actual breach or security incident reports it to the Privacy / Security Officer without delay, and in any event within 72 hours of becoming aware.
2. **Contain.** Take immediate steps to stop and contain the incident (isolate affected systems, revoke compromised access, recover data) while preserving evidence.
3. **Open a record.** The Privacy / Security Officer opens an incident record capturing the date of discovery, what occurred, the PHI involved, the affected customer(s), and the individuals likely affected.
4. **Investigate.** Determine whether an impermissible use or disclosure occurred, which customer(s) and individuals are affected, and whether any exception in Section 3 applies.

> **How to report internally:** Contact the Privacy / Security Officer at anthony@senavida.com. Reports may be made confidentially; retaliation for good-faith reporting is prohibited.

5. Risk Assessment (Four-Factor Analysis)

Unless an exception applies or the PHI was secured, Senavida conducts and documents a risk assessment of whether there is a low probability that the PHI was compromised, considering at least these four factors. (A BAA may instead assign the breach determination to the customer; if so, Senavida provides the facts and supports that determination.)

1. **Nature and extent of the PHI.** The identifiers involved and the likelihood of re-identification.
2. **The unauthorized recipient.** Who used or received the PHI, and whether that person has an independent duty to protect it.
3. **Whether the PHI was actually acquired or viewed.** As opposed to a mere opportunity for access.

4. **Extent of mitigation.** The degree to which the risk has been mitigated (e.g., recovery of data or written assurances of destruction).

If Senavida cannot demonstrate a low probability of compromise, the incident is a reportable breach and Section 6 applies. The assessment and its conclusion are documented and retained.

6. Notification to the Affected Customer (Primary Obligation)

On determining that a reportable breach of unsecured PHI has occurred, Senavida notifies the affected customer:

- **Timing under HIPAA:** without unreasonable delay and no later than 60 calendar days after discovery (§ 164.410).
- **Timing under the BAA:** most BAAs require notice far sooner. Senavida will notify the customer within 72 hours of discovery, or sooner if the BAA so requires. The stricter timeframe always controls.

To the extent known at the time, and supplemented as the investigation continues, the notice to the customer includes:

- The identification of each individual whose PHI was, or is reasonably believed to have been, accessed, acquired, used, or disclosed;
- A description of what happened, including the date of the breach and the date of discovery;
- A description of the types of PHI involved (e.g., name, Social Security number, diagnosis, account number) without including the PHI itself;
- Any steps the individuals should take to protect themselves; and
- What Senavida is doing to investigate, mitigate harm, and prevent recurrence, and a point of contact for the customer.

Senavida cooperates with the customer to provide any further information the customer needs to meet its own notification obligations.

7. Downstream Notifications (Customer Responsibility Unless Delegated)

Notifying affected individuals, the Secretary of HHS, and — for larger breaches — the media is generally the covered entity's responsibility. Senavida performs these notifications only where a BAA expressly delegates them. The reference table below summarizes those downstream obligations so the responsibilities are clear in either case:

Recipient	Trigger	Deadline (from discovery)
Affected individuals	Any reportable breach	Without unreasonable delay; ≤ 60 days
Media outlets	Breach affecting 500+ residents of one State/jurisdiction	Without unreasonable delay; ≤ 60 days
HHS (OCR) — large	Breach affecting 500+	Without unreasonable delay; ≤ 60 days
HHS (OCR) — small	Breach affecting fewer than 500	Annually; ≤ 60 days after year-end (by ~March 1)

8. Subcontractor Breaches

Subcontractor business associates must report breaches of unsecured PHI to Senavida without unreasonable delay and no later than the timeframe set in their subcontractor BAA (and in any event ≤ 60 days after discovery). On receiving such a report, Senavida assesses the incident under this procedure and reports up the chain to the affected customer within Senavida's own deadlines.

9. Law Enforcement Delay

If a law enforcement official states that notification would impede a criminal investigation or cause damage to national security, Senavida delays notification for the period specified in a written statement, or, if the statement is oral, documents it and delays no more than 30 days unless a written statement is provided within that period. Senavida coordinates any such delay with the affected customer.

10. Mitigation

To the extent practicable, Senavida mitigates any harmful effect of an impermissible use or disclosure of PHI that it knows about, including recovering or securing PHI, obtaining assurances of destruction, correcting access controls, and implementing corrective actions to prevent recurrence. Senavida coordinates mitigation and any individual-facing remedies (such as credit monitoring) with the affected customer.

11. Documentation, Retention, and Burden of Proof

Senavida bears the burden of demonstrating that required notifications were made or that an impermissible use or disclosure did not constitute a reportable breach. For every incident, Senavida documents and retains: the incident report and investigation findings; the four-factor risk assessment and its conclusion; copies of notifications to customers (and others, if delegated) with proof of timing; and any exception relied upon. Records are retained at least six (6) years, or longer if a BAA or state law requires.

12. Roles and Responsibilities

Role	Responsibility
All workforce members	Recognize and immediately report suspected or known incidents involving PHI.
Privacy / Security Officer	Lead the investigation, conduct and document the risk assessment, determine reportability, and notify affected customers within required deadlines.
Engineering / Security	Contain and remediate technical incidents; preserve logs and evidence; support forensic analysis.
Leadership / Counsel	Approve customer and any delegated external notifications; manage legal and regulatory risk; authorize mitigation resources.
Subcontractors	Report breaches to Senavida within the subcontractor BAA timeframe and provide supporting information.

13. State Law and Other Obligations

A single incident may trigger obligations beyond HIPAA and beyond the BAA. Senavida coordinates with affected customers to assess applicable state breach-notification laws, which may impose shorter deadlines or notice to state agencies.

14. Training and Process Testing

Workforce members are trained to recognize and report incidents involving PHI as part of HIPAA privacy and security training. Senavida periodically tests this process (for example, through tabletop exercises) to confirm that escalation, assessment, and customer notification can be completed within BAA and regulatory deadlines.

15. Review and Revision

This procedure is reviewed at least annually and updated to reflect changes in law, regulation, customer BAAs, or operations, including any final rule modifying the HIPAA Security or Breach Notification requirements.

Quick-reference: who Senavida notifies, and when

Recipient	Trigger	Deadline (from discovery)
Customer (primary)	Any reportable breach of PHI Senavida holds	Per BAA (often 24–72 hrs); ≤ 60 days under HIPAA
Affected individuals	Only if BAA delegates this to Senavida	Without unreasonable delay; ≤ 60 days
HHS / media	Only if BAA delegates this to Senavida	Per the downstream table in Section 7
Senavida (inbound)	Breach discovered by a subcontractor	Per subcontractor BAA; ≤ 60 days

Approval

Augustine W. Walsh Jr. – Founder

Signature: Signed by: Augustine Walsh Jr. 8467CFC016A34CD... Date: 6/24/2026