

HIPAA-Compliant Data Security Policy

"Safeguarding Sensitive Health Data Through Robust Security Measures"



Satwic Inc.

177 E Colorado Blvd, Suite 200, Pasadena, CA 91105

(818)230-2181

September 2026

Contents

1. Purpose and Scope.....	3
2. Definitions.....	3
• PHI (Protected Health Information):.....	3
• ePHI:.....	3
• Business Associate:.....	3
3. Roles and Responsibilities.....	3
4. Privacy Rule Framework.....	4
5. Administrative Safeguards.....	4
5. Physical Safeguards.....	5
6. Technical Safeguards.....	5
7. Incident Response and Breach Notification.....	6
8. Workforce Training and Sanctions.....	6
9. Policy Review and Updates.....	7
11. Written Policies and Workforce Training.....	7
12. Safeguards for Electronic PHI.....	7
13. Encryption of ePHI.....	7
14. Use of Workforce Only.....	8
15. Documentation, Logging, and Audit Compliance.....	8
16. California Confidentiality of Medical Information Act (CMIA) Addendum	8
17. GDPR Addendum — Special-Category Health Data.....	9
18. FTC Health Breach Notification Rule Addendum.....	9
Acknowledgment and Agreement.....	10

1. Purpose and Scope

The purpose of this policy is to define security measures to protect ePHI from unauthorized access, use, disclosure, alteration, or destruction. This policy applies to all systems, networks, devices, and personnel involved in handling ePHI.

This policy also governs the use and disclosure of Protected Health Information (PHI) generally, not only in electronic form, and incorporates the Privacy Rule obligations described in the new Privacy Rule Framework section below.

2. Definitions

- **PHI (Protected Health Information):** Any information that relates to the past, present, or future physical or mental health of an individual and that identifies the individual.
- **ePHI:** PHI that is created, received, maintained, or transmitted in electronic form.
- **Business Associate:** An entity that performs functions or activities on behalf of a covered entity that involves the use or disclosure of PHI.
- **Minimum Necessary:** The principle that, when using, disclosing, or requesting PHI, workforce members must limit the PHI involved to the minimum amount reasonably necessary to accomplish the intended purpose, except where an exception under 45 CFR §164.502(b)(2) applies (e.g., disclosures to the individual, or disclosures required by law).
- **Privacy Officer:** The individual designated under 45 CFR §164.530(a) with overall responsibility for developing and implementing this policy's Privacy Rule provisions, including individual rights requests and the Notice of Privacy Practices.

3. Roles and Responsibilities

- **Security Officer:** Oversees the implementation of this policy, coordinates security efforts, and serves as the contact for all security-related matters.
- **Workforce Members:** Must follow this policy, complete HIPAA training, and report any suspected security incidents.
- **Privacy Officer:** Oversees compliance with the HIPAA Privacy Rule, including the Notice of Privacy Practices, minimum necessary determinations, and processing of individual rights requests (access, amendment, accounting of disclosures, restriction). May be the same individual as the Security Officer if both roles are formally documented and adequately resourced

4. Privacy Rule Framework

Notice of Privacy Practices (NPP): Where Satwic or a client operates as a HIPAA covered entity, an NPP describing permitted uses and disclosures of PHI, and how individuals may exercise their rights, shall be developed, distributed at first service delivery, and made available upon request (45 CFR §164.520).

Right of Access: Individuals may request access to their PHI in a designated record set. Requests shall be fulfilled within 30 days (with one 30-day extension permitted with written notice) (45 CFR §164.524).

Right to Amend: Individuals may request amendment of PHI they believe is inaccurate or incomplete. Requests shall be acted upon within 60 days, with a documented process for acceptance, denial, and appeal (45 CFR §164.526).

Right to an Accounting of Disclosures: Individuals may request a list of certain disclosures of their PHI made in the preceding six years. A log of such disclosures shall be maintained (45 CFR §164.528).

Right to Request Restrictions and Confidential Communications: Individuals may request restrictions on use or disclosure of PHI, and confidential communications at alternate locations or by alternate means. Requests shall be honored except where restrictions are not required by law (45 CFR §164.522).

Minimum Necessary Standard: The minimum necessary standard applies to all routine and non-routine uses, disclosures, and requests for PHI made by workforce members, not solely to technical system access controls.

5. Administrative Safeguards

- Conduct periodic risk analyses and document findings.
- Develop and maintain a risk management plan to address identified vulnerabilities.
- Implement workforce security and access authorization procedures. Provide HIPAA security training to all workforce members.
- Establish contingency plans, including data backup, disaster recovery, and emergency operations.
- Execute Business Associate Agreements with all subcontractors handling PHI.
- Business Associate Agreements must include, at minimum: permitted and required uses of PHI, a prohibition on further unauthorized use or

disclosure, subcontractor flow-down obligations, breach/security-incident reporting duties to Satwic, return or destruction of PHI upon termination, and audit/inspection rights (45 CFR §164.504(e)).

- Annual risk analyses shall follow the methodology described in NIST SP 800-66 and be benchmarked against the HHS Office for Civil Rights (OCR) Audit Protocol.

5. Physical Safeguards

- Restrict facility access to authorized personnel only.
- Implement workstation security measures, including automatic logoff and privacy screens.
- Maintain an inventory of hardware and devices used to store or access ePHI.
- Sanitize or securely dispose of media and devices before reuse or disposal.

6. Technical Safeguards

- Assign unique user IDs and implement strong authentication controls.
- "Strong authentication controls" is defined to require multi-factor authentication (MFA) for all workforce access — remote, on-site, and administrative — to any system that creates, receives, maintains, or transmits ePHI, consistent with HHS's proposed 2025 update to the Security Rule (proposed 45 CFR §164.312(d)).
- Use role-based access controls to limit access to the minimum necessary. Encrypt ePHI at rest and in transit using industry-standard encryption (e.g., AES-256).
- Maintain audit logs and regularly review system activity. Implement automatic logoff and intrusion detection measures.
- Mobile and BYOD devices accessing ePHI must be enrolled in mobile device management (MDM), support remote wipe, and store ePHI only within an approved encrypted container, consistent with Satwic's Mobile Devices & BYOD Policy (45 CFR §164.310(d)).

7. Incident Response and Breach Notification

- Report any suspected security incidents or breaches immediately to the Security Officer.
- Investigate incidents promptly and document findings.
- Upon discovery of a suspected breach, the Security Officer shall complete a documented four-factor risk assessment (nature/extent of PHI involved, unauthorized recipient, whether PHI was actually acquired/viewed, and extent of mitigation) to determine reportability. Where a reportable breach is confirmed: affected individuals shall be notified without unreasonable delay and no later than 60 calendar days after discovery; HHS shall be notified within 60 days of the end of the calendar year for breaches affecting fewer than 500 individuals, or without unreasonable delay (and no later than 60 days) for breaches affecting 500 or more individuals; and prominent media outlets shall be notified for breaches affecting 500 or more residents of a state or jurisdiction (45 CFR §§164.402–414).
- Security Incident Log: All suspected security incidents — including those that do not meet the threshold for a reportable breach — shall be logged, tracked, and reviewed quarterly, distinct from the breach register (45 CFR §164.308(a)(6)).

8. Workforce Training and Sanctions

- Provide initial and ongoing HIPAA training to all workforce members.
- Maintain training records for at least six years.
- Disciplinary action for non-compliance shall follow a documented, graduated sanctions schedule: (1) verbal warning and retraining for a first, low-severity violation; (2) written warning for a repeated or moderate-severity violation; (3) suspension pending investigation for a serious or willful violation; (4) termination of employment or contract for gross negligence, willful misconduct, or repeated violations after prior discipline. Sanctions shall be documented in the workforce member's personnel file and reported to the Security Officer and Privacy Officer (45 CFR §164.308(a)(1)(ii)(C)).

9. Policy Review and Updates

- This policy will be reviewed at least annually or when there are material changes in operations, regulations, or technology.
- Updates will be documented and communicated to all workforce members.

11. Written Policies and Workforce Training

- The Company maintains written policies and procedures to comply with HIPAA Security and Privacy Rules.
- All workforce members shall receive HIPAA training upon hire and annually thereafter.
- Training completion shall be documented and retained for a minimum of six (6) years.

12. Safeguards for Electronic PHI

- The Company shall maintain administrative, physical, and technical safeguards to reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI as required under 45 CFR §164.308, §164.310, and §164.312.
- Policies, procedures, and documentation shall be maintained in accordance with 45 CFR §164.316.

13. Encryption of ePHI

- All ePHI transmitted electronically shall be encrypted using secure transport protocols (e.g., TLS/SSL for email or HTTPS).
- All files containing ePHI stored or transmitted shall be encrypted at rest using industry-standard encryption (e.g., AES-256).
- All portable media or devices containing ePHI must be encrypted.

14. Use of Workforce Only

- Except as expressly authorized in writing by the Company, only employees of Satwic shall perform services involving access to PHI.

- PHI shall not be disclosed to independent contractors or agents without prior written authorization from the Company and execution of a Business Associate Agreement, if applicable.

15. Documentation, Logging, and Audit Compliance

- The Company shall maintain documentation of security policies, procedures, risk analyses, workforce training records, system access logs, and incident response records.
- Such records shall be retained for at least six (6) years.
- The Company shall cooperate and comply with audits, inspections, or investigations conducted by HHS or applicable state agencies regarding compliance with HIPAA security requirements.
- Where PHI is de-identified for analytics, reporting, or research, de-identification shall follow either the Safe Harbor method or the Expert Determination method described in 45 CFR §164.514, and the method used shall be documented.

16. California Confidentiality of Medical Information Act (CMIA) Addendum

In addition to HIPAA, Satwic, as a California-headquartered company, is subject to the California Confidentiality of Medical Information Act (Cal. Civ. Code §56 et seq.), which in some respects imposes broader obligations than HIPAA — including a broader definition of "medical information," restrictions on disclosure by employers who receive employee medical information, and a private right of action for unauthorized disclosure. Where CMIA imposes a more protective standard than HIPAA, the more protective CMIA standard shall control for California residents' medical information.

17. GDPR Addendum — Special-Category Health Data

Where Satwic or a client processes health data relating to individuals located in the European Union or European Economic Area, such data constitutes a special category of personal data under GDPR Article 9 and requires an explicit lawful basis for processing (e.g., explicit consent, or necessity for the provision of health

care). A Data Protection Impact Assessment (DPIA) shall be conducted before initiating any new large-scale processing of health data. In the event of a breach involving such data, the relevant supervisory authority shall be notified within 72 hours of becoming aware of the breach, and affected individuals shall be notified without undue delay where the breach is likely to result in a high risk to their rights and freedoms (GDPR Art. 33–34).

18. FTC Health Breach Notification Rule Addendum

Where Satwic develops, operates, or supports a product or service that handles individually identifiable health information but does not qualify as a HIPAA covered entity or business associate for that data (e.g., a direct-to-consumer health application), the FTC Health Breach Notification Rule (16 CFR Part 318) applies. Any breach of security involving such unsecured data shall be treated as a reportable event to the FTC and affected individuals, following the Rule's notification timelines, independent of and in addition to any HIPAA notification obligations that may also apply.

Acknowledgment and Agreement

I acknowledge that I have read, understood, and agree to comply with the policies and procedures outlined in this HIPAA-Compliant Data Security Policy document. I understand that violation of these policies may result in disciplinary action, up to and including termination of employment or contract, and may carry legal consequences.

Signature

Printed Name

Date