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 2025

Contents

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.

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.

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.

4. 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.

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.
- 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.

7. Incident Response and Breach Notification

- Report any suspected security incidents or breaches immediately to the Security Officer.
- Investigate incidents promptly and document findings.
- Notify affected covered entities of breaches in accordance with HIPAA Breach Notification Rule.

8. Workforce Training and Sanctions

- Provide initial and ongoing HIPAA training to all workforce members.
- Maintain training records for at least six years.
- Enforce disciplinary actions for non-compliance with this policy.

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.

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