Health Insurance Portability & Accountability Act

Policy Owner(s): Compliance Department, Human Resources

Effective Date: August 9, 2016 | **Revised Date:** May 1, 2026

1. Policy Objective

Heartspring is committed to safeguarding the privacy and security of Protected Health Information (PHI) in compliance with the Health Insurance Portability and Accountability Act (HIPAA), the HITECH Act, and applicable federal and state laws. Heartspring maintains appropriate administrative, physical, and technical safeguards to protect PHI from unauthorized access, use, or disclosure, and requires all workforce members and Business Associates to comply with its HIPAA policies and procedures and to report any suspected or known privacy or security incidents promptly.

2. Scope

This policy applies to all Heartspring workforce members, contracted service providers, students, volunteers, and Business Associates, and governs all PHI, in any form or medium, created or maintained by or on behalf of Heartspring.

3. Policy Statement

Heartspring is committed to protecting the privacy, confidentiality, and security of Protected Health Information (PHI) related to our clients, students, and their families in accordance with the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and applicable federal and state laws. Heartspring collects, uses, maintains, and discloses PHI only as permitted or required by law and implements appropriate administrative, physical, and technical safeguards to protect such information. All workforce members, volunteers, students, contractors, visitors, and Business Associates are required to maintain the confidentiality of PHI and comply with Heartspring's privacy and security policies and procedures. Clients, students, and their families may expect that information related to care and services received at Heartspring will be handled confidentially and disclosed only in accordance with applicable laws and authorized purposes.

Protected Health Information (PHI) includes verbal, written, and electronic information that identifies an individual and relates to an individual's past, present, or future physical or mental health, the provision of healthcare, or payment for healthcare. PHI may exist within individual records or be included in aggregated data, reports, or other documentation generated by Heartspring and is subject to appropriate privacy and security protections regardless of form or format.
Heartspring adheres to the HIPAA Minimum Necessary standard by limiting the collection, use, and disclosure of PHI to the minimum amount necessary to accomplish the intended purpose, except where the minimum necessary standard does not apply, including disclosures for treatment. Workforce members may be exposed to sensitive and personal information in the course of their duties and are required to protect the confidentiality of PHI at all times in accordance with Heartspring policies and applicable law.
Heartspring maintains organizational oversight to support compliance with HIPAA requirements. Human Resources is responsible for maintaining documentation of workforce acknowledgement of applicable HIPAA policies, and the Compliance Department is responsible for overseeing Business Associate relationships, including the execution and maintenance of Business Associate Agreements (BAAs), in accordance with regulatory requirements.

3.1 Security Officer and Privacy Officer Roles

In accordance with HIPAA requirements, Heartspring designates the area leader of the Information Technology/Business Intelligence (IT/BI) department as the HIPAA Security Officer, responsible for overseeing the development, implementation, and maintenance of administrative, technical, and physical safeguards to protect electronic protected health information (ePHI). The Compliance area leader serves as the HIPAA Privacy Officer and is responsible for overseeing compliance with HIPAA Privacy Rule requirements, including the development and enforcement of privacy policies, workforce training, complaint investigation, and breach response related to protected health information (PHI).

3.2 Business Associates

Business Associates may engage subcontractors to perform functions or activities involving Protected Health Information (PHI) on behalf of Heartspring only as permitted by applicable law and contractual requirements. Business Associates are responsible for ensuring that any subcontractor who creates, receives, maintains, or transmits PHI on Heartspring's behalf agrees in writing to comply with HIPAA requirements through a written subcontractor business associate agreement. Business Associates remain fully responsible for the acts and omissions of their subcontractors with respect to HIPAA compliance.

3.3 Technology

- Heartspring employees are required to take reasonable steps to prevent inadvertent disclosure of PHI through unsecured technology.

- Heartspring issued desktop and laptop computers must be set to screen saver lock automatically after 5 minutes of inactivity. This setting is set up by the IT department on all new devices and should not be overridden.
- Employees who access the Heartspring Virtual Private Network (VPN) or Electronic Medical Record (EMR) system remotely are required to exit out of those programs after each use and to lock down the device when not in use. VPN and EMR access will only be installed on Heartspring-issued devices by the IT department.
- Employees who access their Heartspring email and/or Outlook calendar on a personal cell phone, tablet, or other mobile devices must protect said device(s) with a passcode, swipe code, or biometric authentication.
- The iPods/iPads used for data collection by direct care professional staff have a time lock set and will lock down, requiring the entry of a passcode, after a set amount of time. Staff are prohibited from changing or disabling the lock down settings.
- Heartspring utilizes approved email encryption tools to protect PHI transmitted electronically, in accordance with applicable security standards.

3.4 Breach

Workforce members must promptly report any suspected or confirmed unauthorized access, use, or disclosure of PHI to the Compliance Director. All reports will be investigated, and required notifications, mitigation, and corrective actions will be completed in accordance with applicable law.
Reports may be made without fear of retaliation, and workforce members are not required to determine whether an incident constitutes a breach prior to reporting.
Any Heartspring workforce member who becomes aware of a suspected or confirmed unauthorized access, use, or disclosure of Protected Health Information (PHI) must report the incident immediately upon discovery to the Heartspring Compliance Director, Privacy Officer, or Security Officer. Workforce members are required to report suspected incidents and are not responsible for determining whether an incident constitutes a reportable breach.
Upon receipt of an incident report, the Compliance Director will conduct a documented investigation and risk assessment in accordance with applicable law to determine whether a breach has occurred. If a reportable breach is confirmed, Heartspring will notify affected individuals without unreasonable delay and in no case later than sixty (60) days following discovery of the breach.
Breaches involving fewer than 500 individuals will be documented and reported to the U.S. Department of Health and Human Services Office for Civil Rights no later than sixty (60) days after the end of the calendar year in which the breach occurred. Larger breaches will be reported in accordance with regulatory requirements.

4. Policy Violations

Penalties

HIPAA violations are classified into four tiers based on the level of knowledge, intent, and corrective action taken: Tier 1 – No Knowledge; Tier 2 – Reasonable Cause; Tier 3 – Willful Neglect that is corrected within the required timeframe; and Tier 4 – Willful Neglect that is not corrected. Enforcement actions and civil monetary penalties are assessed in accordance with the applicable tier and increase with the level of accountability.

Any Heartspring workforce member, including employees, practicum students, interns, and volunteers, who violates this policy or applicable HIPAA requirements will be subject to appropriate disciplinary action, up to and including termination of employment or affiliation, in accordance with Heartspring's disciplinary standards and applicable law. Violations may also subject the individual to civil or criminal penalties as provided by law.

Any contract worker, consultant, vendor personnel, or other non-employee individual acting on behalf of Heartspring who violates this policy or applicable HIPAA requirements may be subject to corrective action, up to and including termination of the contractual relationship, revocation of access to Heartspring facilities or systems, and other remedies available under contract or applicable law. Violations may also subject the individual or contracting entity to civil or criminal penalties as provided by law.

5. Definitions

- Business Associates **-** entities that create, receive, maintain or transmit electronically protected health information on the covered entities' behalf which assist in healthcare operations and have direct access to the protected health information of Heartspring clients.
- Covered Entity – an entity that must follow HIPAA regulations
- HIPAA - Health Insurance Portability and Accountability Act of 1996 - Mandate that privacy practices be integrated into daily operations
- PHI – Protected Health Information, individually identifiable health information created or received by a healthcare provider, health plan, employer, or healthcare clearing house and that relates to the past, present or future mental or physical health of the individual: provision of healthcare to the individual; or payment for the provision of healthcare to the individual, which is transmitted or maintained in any form or medium.

6. Forms or Related Policies

Not Applicable

7. Applicable Laws/Regulations

CARF Medical Rehabilitation Standard 1.E.3
Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Health Information Technology for Economic and Clinical Health Act (HITECH)

REVISION RECORD

DATE	VERSION	REVISION DESCRIPTION
11/7/2022	v.1.1	Reviewed. No changes.
3/31/2025	v.2	Updated policy owners. Changes to Sections 3, 3.1, 3.3 and 5. List of HHS Identifiers for PHI updated.
5/1/2026	v.3	Updated language throughout to align with OCR Regulations, Changes to Sections 1, 2, 3, and 4.