# HIPAA Compliance

Anything Helps is committed to full compliance with the Health Insurance Portability and Accountability Act (HIPAA) of 1996. This policy establishes national standards for the protection, privacy, and security of Protected Health Information (PHI) in all formats—electronic (ePHI), paper, and verbal. It is regulated by the Department of Health and Human Services (HHS) and enforced by the Office for Civil Rights (OCR). This policy applies to all employees, independent contractors, business associates, and volunteers who handle, store, or transmit PHI on behalf of the organization.

---



---

## Definitions

- HIPAA: A federal law mandating the protection and confidential handling of an individual's health information.
- Protected Health Information (PHI): Information about an individual's health status, provision of health care, or payment for health care that can be linked to a specific individual.
- ePHI: Electronic Protected Health Information.
- Covered Entity: Any organization or individual who provides treatment, payment, and health care operations.
- Business Associate: An individual or entity that performs functions involving the use or disclosure of PHI on behalf of the organization.
- Workforce Members: Employees, independent contractors, and volunteers who provide services on behalf of the organization.
- Minimum Necessary Standard: The principle that workforce members should access only the minimal amount of PHI necessary to complete their job duties

### HIPAA Rules and Regulations

To ensure compliance, Anything Helps follows these core HIPAA regulations:

- HIPAA Privacy Rule: Sets standards for protecting individuals' PHI, including the right to access, restrict, and control the disclosure of their information.
- HIPAA Security Rule: Establishes physical, technical, and administrative safeguards for maintaining, transmitting, and handling ePHI.
- HIPAA Breach Notification Rule: Defines the required response and notification process in case of a breach involving PHI or ePHI.
- HIPAA Omnibus Rule: Extends HIPAA regulations to business associates, requiring Business Associate Agreements (BAAs) to define their responsibilities in protecting PHI.

### Client Rights Under HIPAA

HIPAA grants clients specific rights regarding their PHI, which must be communicated and respected by the organization:

- Right to Access: Clients can request and obtain a copy of their PHI, which must be provided within 30 days, with secure electronic access if requested.
- Right to Amend: Clients may request corrections to their PHI if they believe it is inaccurate or incomplete. The organization must respond within 60 days.
- Right to Request Restrictions: Clients may ask for restrictions on how their PHI is used or disclosed. Any agreed-upon restrictions must be documented.
- Right to Confidential Communications: Clients may request communications by alternative means, and the organization must accommodate reasonable requests.

## Safeguarding PHI

### Administrative Safeguards

- Access Controls: PHI access is restricted based on job responsibilities. Role-based access control (RBAC) ensures that individuals only access the minimum necessary information.
- Business Associate Agreements (BAAs): Before PHI is shared with business associates, a BAA must be signed, outlining their responsibilities in protecting the PHI. The Privacy Officer manages the execution and annual review of all BAAs.
- Contingency Planning: A contingency plan is in place to protect PHI during emergencies, including system failures or natural disasters. Regular data backups and disaster recovery procedures are included.
- Non-Disclosure Agreements (NDAs): Before sharing information with non-employees, an NDA must be signed by both an officer within the organization and the non-employee.

### Physical Safeguards

- Device Security: Mobile devices (laptops, phones, tablets) that store or access PHI must be encrypted and protected by multi-factor authentication (MFA). Devices must not be left in unsecured locations.
- Workstation Security: Employees working remotely must secure their workstations, using privacy screens and avoiding public Wi-Fi.
- Media and Device Disposal: Devices storing PHI must be securely wiped before disposal or physically destroyed if they cannot be wiped clean.

### Technical Safeguards

- Encryption: All ePHI must be encrypted both in transit and at rest to prevent unauthorized access.
- Audit Logs: Systems handling ePHI must generate audit logs that track access and activity, with regular reviews to identify unauthorized access or suspicious activity.
- Automatic Locking: Workstations accessing ePHI must have automatic locking features enabled to prevent unauthorized access during inactivity.

### Data Sharing and Secure Transmission

- Authorized Access: PHI should only be shared with authorized personnel who have a legitimate need for access.
- Secure Transmission: PHI must not be sent via unencrypted email, text, or other unsecured methods. HIPAA-compliant systems must be used to transmit PHI.
- Verification of Identity: Before responding to external inquiries, always verify the requestor's identity and their right to access the information.
- Documentation of Disclosures: All PHI disclosures must be documented, including the recipient, date of disclosure, and purpose, in accordance with HIPAA requirements.

### Training and Recordkeeping

- Initial Training: All new workforce members must complete HIPAA training during onboarding, covering the organization's policies, procedures, and the Privacy and Security Rules.
- Annual Refresher Training: Employees, contractors, and volunteers must complete annual refresher training, which includes updates to policies, real-world examples of HIPAA breaches, and role-specific guidance.
- Specialized Training: Employees handling large volumes of PHI or managing IT infrastructure must receive specialized training on data encryption, risk mitigation, and security incident handling.
- Recordkeeping: The Privacy Officer will maintain detailed records of all training sessions, including participant names, dates, and signed attestations. All training records must be retained for a minimum of six years.

## Risk Management

### Risk Assessment and Mitigation

- Annual Risk Assessment: The Privacy Officer, with IT staff, will conduct an annual risk assessment covering administrative, physical, and technical safeguards.
- Scope of Assessment: The risk assessment will identify vulnerabilities related to unauthorized access, encryption weaknesses, physical security, and external threats.
- Risk Evaluation: Risks will be categorized based on their likelihood and potential impact on PHI.
- Risk Management Plans: The Privacy Officer will create a Risk Management Plan outlining the following:
  - Prioritized List of Risks: Based on likelihood and impact.
  - Specific Corrective Actions: Tailored to each risk identified.
  - Designated Staff Responsibilities: Assign personnel to implement corrective actions.
  - Deadlines: Set timeframes for completing mitigation measures.

### Corrective Measures

- Technical Risks: Address technical issues, such as weak encryption, by upgrading encryption protocols, enhancing network security, or installing security patches.
- Administrative Risks: For training gaps, schedule additional training sessions and update training materials.
- Physical Risks: Safeguard mobile device use in public spaces with privacy screens or stricter device policies.
- Monitoring and Review: The Privacy Officer will monitor risk mitigation actions regularly, reviewing progress at intervals and updating the Risk Management Plan as necessary.

### Sanctions

- Civil and Criminal Penalties: HIPAA violations may result in civil fines ranging from $100 to $50,000 per violation, depending on the severity, or criminal penalties for intentional violations.
- Internal Enforcement: Employees or contractors found in violation of HIPAA policies will be subject to disciplinary actions, including retraining, suspension, or termination.
- Resolution Agreements: In cases of significant non-compliance, OCR may impose a resolution agreement requiring specific corrective actions, such as workforce training or regular audits.

### Auditing

- Continuous Monitoring: The Privacy Officer will implement a continuous monitoring program to track HIPAA compliance through regular audits and reviews of access logs and system activity.
- Continuous Improvement: Policies, procedures, and training programs will be updated based on the findings from audits and risk assessments to adapt to emerging risks.
- Engagement with Third-Party Experts: The organization will engage external HIPAA compliance experts or legal counsel as needed for independent audits or complex incident investigations.
- Annual Risk Assessment: The Privacy Officer, in collaboration with IT staff, will conduct a comprehensive risk assessment at least once per year, or whenever there are significant changes in operations, technology, or staffing. The risk assessment will cover administrative, physical, and technical safeguards, identifying vulnerabilities related to the following:
  - Unauthorized access to PHI
  - Weaknesses in encryption, MFA, or access controls
  - Vulnerabilities in physical security, such as the use of mobile devices in public spaces
  - Gaps in employee training or knowledge
  - External threats, such as cyberattacks and phishing attempts

Risk Evaluation: The Privacy Officer will categorize risks based on their degree:

- Likelihood: How likely is the risk to occur?
- Impact: What is the potential impact on PHI?

Documentation: Each risk identified must be documented, including:

- Risk description
- Potential threat
- Likelihood and impact
- Current mitigation measures in place

Reporting: The results of the risk assessment will be presented to senior management for review, along with recommendations for further action.

---

**References:** **Business Associate Agreements** | **Audit Log** | **HIPAA Training**

**Previous:** HMIS Security Standards