HCAB
Home Care Agency Blueprint
Building Successful Home Care Businesses

HIPAA Compliance Toolkit

Privacy and Security for Home Care Agencies

Complete Toolkit

www.homecareagencyblueprint.com

HIPAA Overview for Home Care Agencies

The Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996 to protect patients' medical records and other personal health information. For home care agencies, HIPAA compliance is not optional - it is a federal requirement that carries significant penalties for violations.

Why HIPAA Matters for Home Care

Home care providers have unique access to patients' homes and personal information. This intimate care environment creates additional privacy responsibilities that office-based healthcare providers may not face.

The Three Main HIPAA Rules

Rule	Purpose	Key Requirements
Privacy Rule	Protects the privacy of individually identifiable health information	Limits use and disclosure of PHI; provides patient rights
Security Rule	Sets standards for protecting electronic PHI (ePHI)	Administrative, physical, and technical safeguards
Breach Notification Rule	Requires notification following a breach of unsecured PHI	Notify individuals, HHS, and sometimes media

Penalties for Non-Compliance

HIPAA Violation Penalties (Updated 2024)

- **Tier 1 (Unknowing):** $137 - $68,928 per violation
- **Tier 2 (Reasonable Cause):** $1,379 - $68,928 per violation
- **Tier 3 (Willful Neglect - Corrected):** $13,785 - $68,928 per violation
- **Tier 4 (Willful Neglect - Not Corrected):** $68,928 - $2,067,813 per violation
- **Criminal Penalties:** Up to $250,000 and 10 years imprisonment

Who Must Comply with HIPAA

HIPAA applies to two categories of organizations:

Covered Entities

- Healthcare providers who transmit health information electronically (including most home care agencies)
- Health plans (insurance companies, HMOs, Medicare, Medicaid)
- Healthcare clearinghouses

Business Associates

- Billing companies
- EHR/EMR vendors
- Cloud storage providers
- IT service providers
- Shredding companies
- Consultants who access PHI

> **Home Care Agency Tip**
>
> If your agency bills Medicare, Medicaid, or private insurance electronically, you are a covered entity under HIPAA. Even if you only accept private pay, following HIPAA guidelines is a best practice that protects both your clients and your business.

Key HIPAA Terms and Definitions

Understanding HIPAA terminology is essential for compliance. Below are the key terms every home care agency staff member should know:

Term	Definition
Protected Health Information (PHI)	Any individually identifiable health information held or transmitted by a covered entity. Includes past, present, or future physical/mental health conditions, healthcare provided, or payment for healthcare.
Electronic PHI (ePHI)	PHI that is created, stored, transmitted, or received in electronic form.
Covered Entity	A health plan, healthcare clearinghouse, or healthcare provider who transmits health information electronically.
Business Associate	A person or organization that performs functions involving PHI on behalf of a covered entity.
Minimum Necessary	The principle that only the minimum amount of PHI needed to accomplish a task should be used or disclosed.
Authorization	A detailed, written permission signed by the patient allowing specific uses or disclosures of PHI.
Breach	Unauthorized acquisition, access, use, or disclosure of PHI that compromises its security or privacy.
De-identified Information	Health information that does not identify an individual and cannot reasonably be used to identify an individual.

The 18 PHI Identifiers

HIPAA identifies 18 types of information that can identify an individual when associated with health information:

1. Names
2. Geographic data (smaller than state)
3. Dates (except year) related to individual
4. Phone numbers
5. Fax numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
1. Account numbers
2. Certificate/license numbers
3. Vehicle identifiers and serial numbers
4. Device identifiers and serial numbers
5. Web URLs
6. IP addresses
7. Biometric identifiers
8. Full-face photographs
9. Any other unique identifying number

Privacy Rule Essentials

The HIPAA Privacy Rule establishes national standards for the protection of individually identifiable health information. It applies to PHI in any form - electronic, paper, or oral.

Core Principles of the Privacy Rule

1. Use and Disclosure Limitations

PHI may only be used or disclosed in the following circumstances:

- **To the Individual:** Patients have the right to access their own PHI
- **Treatment, Payment, and Healthcare Operations (TPO):** No authorization required
- **With Authorization:** Patient must sign a valid authorization form
- **As Required by Law:** Court orders, public health reporting, etc.
- **To Prevent Serious Threat:** Imminent danger to health or safety

> **Treatment, Payment, and Operations (TPO)**
>
> **Treatment:** Providing, coordinating, or managing healthcare services (e.g., sharing care notes with a patient's physician)
>
> **Payment:** Activities related to obtaining reimbursement (e.g., submitting claims to insurance)
>
> **Operations:** Administrative and quality improvement activities (e.g., staff training, quality assessment)

2. Minimum Necessary Standard

When using, disclosing, or requesting PHI, you must make reasonable efforts to limit the information to the minimum necessary to accomplish the intended purpose.

> **Exceptions to Minimum Necessary**
>
> The minimum necessary standard does NOT apply to: disclosures to the patient, disclosures for treatment purposes, disclosures authorized by the patient, disclosures required by law, or disclosures to HHS for compliance investigations.

3. Notice of Privacy Practices

Covered entities must provide patients with a Notice of Privacy Practices (NPP) that describes:

- How PHI may be used and disclosed
- The patient's rights regarding their PHI
- The covered entity's duties to protect PHI
- How to file a complaint

Patient Rights Under the Privacy Rule

Right	Description	Response Time
Right to Access	Inspect and obtain a copy of their PHI	30 days (one 30-day extension allowed)
Right to Amend	Request corrections to their PHI	60 days (one 30-day extension allowed)
Right to Accounting	Receive a list of certain disclosures of their PHI	60 days (one 30-day extension allowed)
Right to Restrict	Request limitations on uses/ disclosures	Must agree to restrict if patient pays out of pocket
Right to Confidential Communications	Request communications by alternative means/locations	Must accommodate reasonable requests
Right to Notice	Receive the Notice of Privacy Practices	At first service delivery

Security Rule Requirements

The HIPAA Security Rule establishes standards specifically for protecting electronic PHI (ePHI). It requires covered entities to implement administrative, physical, and technical safeguards.

> **Security Rule Flexibility**
>
> The Security Rule is designed to be flexible and scalable. Small home care agencies do not need the same level of security infrastructure as large hospital systems. What matters is that your safeguards are reasonable and appropriate for your organization's size, complexity, and resources.

Administrative Safeguards

Administrative safeguards are policies and procedures designed to manage the selection, development, implementation, and maintenance of security measures.

Required Administrative Safeguards:

- [ ] **Security Management Process**
  Implement policies and procedures to prevent, detect, contain, and correct security violations. Includes risk analysis and risk management.

- [ ] **Assigned Security Responsibility**
  Designate a security official responsible for developing and implementing security policies.

- [ ] **Workforce Security**
  Ensure appropriate access to ePHI and prevent unauthorized access. Includes authorization, supervision, and termination procedures.

- [ ] **Information Access Management**
  Implement policies for authorizing access to ePHI consistent with the Privacy Rule.

- [ ] **Security Awareness and Training**
  Implement security awareness and training programs for all workforce members, including management.

- [ ] **Security Incident Procedures**
  Implement policies and procedures to address security incidents.

- [ ] **Contingency Plan**
  Establish procedures for responding to emergencies that damage systems containing ePHI.

- [ ] **Evaluation**
  Perform periodic technical and non-technical evaluations of security policies and procedures.

Physical Safeguards

Physical safeguards are physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment.

Required Physical Safeguards:

- [ ] **Facility Access Controls**
  Limit physical access to electronic information systems and facilities. Include contingency operations, facility security plan, access control, and maintenance records.

- [ ] **Workstation Use**
  Specify proper functions and physical attributes of workstations that access ePHI.

- [ ] **Workstation Security**
  Implement physical safeguards restricting access to workstations with ePHI access.

- [ ] **Device and Media Controls**
  Implement policies for disposal, media re-use, accountability, and data backup/storage of devices containing ePHI.

Technical Safeguards

Technical safeguards are the technology and related policies and procedures that protect ePHI and control access to it.

Required Technical Safeguards:

- [ ] **Access Control**

  Implement technical policies to allow only authorized persons to access ePHI. Includes unique user identification, emergency access procedure, automatic logoff, and encryption/decryption.

- [ ] **Audit Controls**

  Implement mechanisms to record and examine activity in systems containing ePHI.

- [ ] **Integrity**

  Implement policies to protect ePHI from improper alteration or destruction.

- [ ] **Person or Entity Authentication**

  Implement procedures to verify that a person or entity seeking access to ePHI is who they claim to be.

- [ ] **Transmission Security**

  Implement technical measures to guard against unauthorized access to ePHI transmitted over electronic networks.

Breach Notification Procedures

The HIPAA Breach Notification Rule requires covered entities to notify affected individuals, HHS, and in some cases the media, following a breach of unsecured PHI.

What Constitutes a Breach?

A breach is the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule that compromises the security or privacy of the PHI.

> **Presumption of Breach**
>
> Any impermissible use or disclosure is presumed to be a breach unless you can demonstrate through a risk assessment that there is a low probability the PHI has been compromised.

Exceptions to the Breach Definition:

1. **Unintentional acquisition** by a workforce member acting in good faith and within scope of authority
2. **Inadvertent disclosure** between authorized persons at the same covered entity or business associate
3. **Good faith belief** that the unauthorized person could not retain the information

Risk Assessment Factors

To determine if a breach occurred, assess at minimum:

Factor	Considerations
Nature and Extent of PHI	Types of identifiers involved, likelihood of re-identification, types of health information
Unauthorized Person	Who received the information? Are they obligated to protect PHI?
PHI Actually Acquired or Viewed	Was the information actually accessed, or just potentially accessible?

Mitigation Extent	What steps have been taken to reduce harm? Was information returned or destroyed?

Breach Response Timeline

Critical Deadlines

Individual Notification:	Within 60 days of discovery
HHS Notification (500+ individuals):	Within 60 days of discovery
HHS Notification (under 500):	Within 60 days of end of calendar year
Media Notification (500+ in one state):	Within 60 days of discovery

Individual Notification Requirements

Written notification to affected individuals must include:

- Brief description of what happened, including date of breach and date of discovery
- Types of unsecured PHI involved (e.g., names, SSN, diagnoses)
- Steps individuals should take to protect themselves
- Description of what you are doing to investigate, mitigate harm, and prevent future breaches
- Contact procedures (toll-free number, email, postal address)

Breach Response Steps

1. **Discover and Contain:** Immediately stop the breach and secure PHI
2. **Document:** Record all facts, dates, and individuals involved
3. **Assess:** Conduct risk assessment to determine if breach occurred
4. **Notify:** Notify affected individuals, HHS, and media if required
5. **Mitigate:** Take steps to reduce harm to affected individuals
6. **Prevent:** Implement measures to prevent similar breaches

NOTICE OF PRIVACY PRACTICES

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.

Our Pledge Regarding Your Health Information

We understand that your health information is personal and we are committed to protecting it. We create a record of the care and services you receive from us. We need this record to provide you with quality care and to comply with certain legal requirements.

This notice applies to all records of your care generated by our agency, whether made by agency personnel or your personal physician. Your personal physician may have different policies and a separate notice regarding the use and disclosure of your health information.

How We May Use and Disclose Health Information About You

For Treatment

We may use your health information to provide you with medical treatment or services. We may disclose health information about you to doctors, nurses, technicians, or other personnel who are involved in your care.

For Payment

We may use and disclose health information about you so that the treatment and services you receive may be billed and payment may be collected from you, an insurance company, or a third party.

For Health Care Operations

We may use and disclose health information about you for agency operations, including quality assessment, employee review, training, licensing, and conducting or arranging for other business activities.

As Required by Law

We will disclose health information about you when required to do so by federal, state, or local law.

To Avert a Serious Threat to Health or Safety

We may use and disclose health information about you when necessary to prevent a serious threat to your health and safety or the health and safety of the public or another person.

Your Rights Regarding Your Health Information

Right to Inspect and Copy: You have the right to inspect and obtain a copy of health information that may be used to make decisions about your care.

Right to Amend: If you believe that health information we have about you is incorrect or incomplete, you may ask us to amend the information.

Right to an Accounting of Disclosures: You have the right to request an accounting of certain disclosures we made of your health information.

Right to Request Restrictions: You have the right to request a restriction or limitation on the health information we use or disclose about you.

Right to Request Confidential Communications: You have the right to request that we communicate with you about health matters in a certain way or at a certain location.

Right to a Paper Copy of This Notice: You have the right to a paper copy of this notice at any time.

Changes to This Notice

We reserve the right to change this notice. We reserve the right to make the revised or changed notice effective for health information we already have about you as well as any information we receive in the future.

Complaints

If you believe your privacy rights have been violated, you may file a complaint with our agency or with the Secretary of the Department of Health and Human Services. To file a complaint with our agency, contact our Privacy Officer. You will not be penalized for filing a complaint.

Contact Information

Privacy Officer:

_____

Agency Name:

_____

Address:

_____

Phone:

_____

Effective Date: _____

ACKNOWLEDGMENT OF RECEIPT OF NOTICE OF PRIVACY PRACTICES

Patient/Client Acknowledgment Form

I acknowledge that I have received a copy of the Notice of Privacy Practices for:

Agency Name:

_____

The Notice of Privacy Practices describes how the agency may use and disclose my protected health information to carry out treatment, payment, or health care operations and for other purposes that are permitted or required by law.

I understand that I have the right to review the Notice of Privacy Practices before signing this acknowledgment. I understand that the agency reserves the right to change its Notice of Privacy Practices.

I understand that I may request a copy of the current Notice of Privacy Practices at any time.

_____ _____

Patient/Client Signature Date

Printed Name:

_____

FOR OFFICE USE ONLY - If Patient Unable or Refuses to Sign:

☐ Patient unable to sign due to medical condition

☐ Patient refused to sign

☐ Emergency circumstances prevented obtaining acknowledgment

☐ Other: _____

Staff Signature:

_____ Date: _____

AUTHORIZATION FOR DISCLOSURE OF PROTECTED HEALTH INFORMATION

HIPAA-Compliant Release Form

Section 1: Patient Information

Patient Name: _____

Medical Record Number: _____

Date of Birth: _____

Social Security Number (last 4): _____

Address: _____

Section 2: Authorization to Release Information

I authorize the following party to release my protected health information:

Name/Organization: _____

Address: _____

Phone/Fax: _____

Section 3: Information to be Released TO

Name/Organization: _____

Address: _____

Phone/Fax:

Section 4: Specific Information to be Released

I authorize the release of the following information (check all that apply):

- ☐ Complete Medical Record
- ☐ History and Physical
- ☐ Progress Notes
- ☐ Medication List
- ☐ Laboratory Results
- ☐ Care Plan
- ☐ Discharge Summary
- ☐ Billing Records
- ☐ Mental Health Records
- ☐ HIV/AIDS Information
- ☐ Other (specify): _____

Date Range of Records:

From _____ To _____

Section 5: Purpose of Disclosure

- ☐ Continued Care/Treatment
- ☐ Insurance/Payment
- ☐ Legal Purposes
- ☐ Personal Use
- ☐ Other: _____

Section 6: Expiration

This authorization will expire on (date or event): _____

If no date is specified, this authorization will expire one (1) year from the date signed.

Section 7: Patient Rights and Signature

I understand that:

- I may revoke this authorization at any time by submitting a written request, except to the extent that action has already been taken.
- I may refuse to sign this authorization and my refusal will not affect my ability to obtain treatment or payment.
- Information disclosed pursuant to this authorization may be subject to re-disclosure by the recipient and may no longer be protected by federal privacy regulations.
- I am entitled to a copy of this authorization after I sign it.

Patient/Legal Representative Signature

Date

Printed Name:

If signed by representative, relationship to patient:

BUSINESS ASSOCIATE AGREEMENT

HIPAA-Compliant Contract Template

This Business Associate Agreement ("Agreement") is entered into by and between:

COVERED ENTITY:

_____

_____

Name and Address

BUSINESS ASSOCIATE:

_____

_____

Name and Address

Effective Date: _____

RECITALS

WHEREAS, Covered Entity wishes to disclose certain information to Business Associate pursuant to the terms of this Agreement, some of which may constitute Protected Health Information ("PHI");

WHEREAS, Covered Entity and Business Associate intend to protect the privacy and provide for the security of PHI disclosed to Business Associate pursuant to this Agreement in compliance with HIPAA and the HITECH Act;

NOW, THEREFORE, in consideration of the mutual promises below and the exchange of information pursuant to this Agreement, the parties agree as follows:

Article 1: Definitions

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the HIPAA Rules.

Article 2: Obligations of Business Associate

Business Associate agrees to:

1. Not use or disclose PHI other than as permitted or required by this Agreement or as required by law;
2. Use appropriate safeguards and comply with the Security Rule to prevent unauthorized use or disclosure of PHI;
3. Report to Covered Entity any use or disclosure of PHI not provided for by this Agreement of which it becomes aware, including any security incident or breach;

4. Ensure that any subcontractors that create, receive, maintain, or transmit PHI agree to the same restrictions and conditions;
5. Make available PHI in accordance with the individual's rights under the Privacy Rule;
6. Make its internal practices, books, and records relating to PHI available to HHS for purposes of determining compliance;
7. Return or destroy all PHI received from Covered Entity upon termination of this Agreement.

Article 3: Permitted Uses and Disclosures

Business Associate may use or disclose PHI:

1. To perform functions, activities, or services for Covered Entity as specified in the underlying service agreement;
2. For the proper management and administration of Business Associate;
3. To provide data aggregation services relating to the healthcare operations of Covered Entity;
4. As required by law.

Article 4: Obligations of Covered Entity

Covered Entity shall:

1. Notify Business Associate of any limitations in its Notice of Privacy Practices;
2. Notify Business Associate of any changes in, or revocation of, authorization by an individual;
3. Notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to.

Article 5: Term and Termination

This Agreement shall be effective as of the Effective Date and shall terminate when all PHI provided by Covered Entity to Business Associate is destroyed or returned to Covered Entity.

Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall provide an opportunity for Business Associate to cure the breach. If Business Associate does not cure the breach within thirty (30) days, Covered Entity may terminate this Agreement.

Article 6: Miscellaneous

Amendment: This Agreement may not be modified except by written agreement signed by both parties.

Survival: The obligations of Business Associate under Article 2 shall survive the termination of this Agreement.

Interpretation: Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the parties to comply with HIPAA.

BUSINESS ASSOCIATE AGREEMENT

Signature Page

IN WITNESS WHEREOF, the parties have executed this Agreement as of the Effective Date.

COVERED ENTITY:

Organization Name:

_____

_____ _____

Authorized Signature Date

Printed Name: **Title:**

_____ _____

BUSINESS ASSOCIATE:

Organization Name:

_____

_____ _____

Authorized Signature Date

Printed Name: **Title:**

_____ _____

Important Notes:

- Keep signed copies on file for at least six (6) years
- Review and update annually or when services change
- Ensure all subcontractors sign similar agreements
- Consult with legal counsel before signing

BREACH INCIDENT REPORT

HIPAA Security Incident Documentation Form

IMPORTANT: Complete this form immediately upon discovery of a potential breach

This form must be completed within 24 hours of incident discovery and submitted to the Privacy Officer.

Section 1: Report Information

Report Completed By: _____

Date of Report: _____

Title/Position: _____

Contact Phone: _____

Section 2: Incident Details

Date Incident Occurred: _____

Date Incident Discovered: _____

Time Incident Occurred: _____

Time Incident Discovered: _____

Location of Incident:

_____

Type of Incident (check all that apply):

- ☐ Lost/stolen laptop or device
- ☐ Lost/stolen paper records
- ☐ Unauthorized access to records
- ☐ Email sent to wrong recipient
- ☐ Improper disposal of records
- ☐ Hacking/IT security incident
- ☐ Verbal disclosure
- ☐ Other: _____

Section 3: Description of Incident

Provide a detailed description of what occurred:

Section 4: PHI Involved

Number of individuals potentially affected:

_____

Types of PHI involved (check all that apply):

- ☐ Names
- ☐ Addresses
- ☐ Dates of birth
- ☐ Social Security numbers
- ☐ Medical record numbers
- ☐ Diagnosis/treatment information
- ☐ Financial/billing information
- ☐ Insurance information
- ☐ Medications
- ☐ Other: _____

Section 5: Individuals Involved

Employee(s) involved in incident:

_____

Unauthorized person(s) who received/accessed PHI:

_____

Section 6: Immediate Actions Taken

BREACH INCIDENT REPORT

Page 2 - Risk Assessment and Resolution

Section 7: Risk Assessment

Evaluate the following factors to determine breach probability:

1. Nature and extent of PHI involved:

☐ Low risk - Limited identifiers, no sensitive information

☐ Medium risk - Some identifiers, minimal clinical information

☐ High risk - SSN, financial info, or sensitive diagnoses included

2. Was PHI actually acquired or viewed?

☐ Yes - confirmed

☐ No - PHI was not accessed

☐ Unknown - cannot determine

3. Unauthorized person receiving PHI:

☐ Healthcare provider (bound by own HIPAA obligations)

☐ Business associate (BAA in place)

☐ General public/unknown party

4. Was information returned or destroyed?

☐ Yes - PHI has been returned/destroyed (attach confirmation)

☐ No

☐ Pending

Section 8: Breach Determination

Based on the risk assessment, this incident:

☐ **IS a reportable breach** - Notification required

☐ **IS NOT a reportable breach** - Low probability PHI was compromised

Determination made by:

_____ Date: _____

Section 9: Notification Actions (if breach determined)

☐ Individual notification letters sent - Date: _____

☐ HHS notified via breach portal - Date: _____

☐ Media notification (if 500+ affected) - Date: _____

Section 10: Corrective Actions

Describe steps taken to prevent similar incidents:

_____ _____

Privacy Officer Signature Date

EMPLOYEE CONFIDENTIALITY AGREEMENT

HIPAA and Protected Health Information

Employee Information

Employee Name: _____

Department: _____

Position/Title: _____

Date of Hire: _____

Confidentiality Agreement

As an employee of _____ ("the Agency"), I understand that I may have access to confidential information, including Protected Health Information (PHI) as defined by the Health Insurance Portability and Accountability Act (HIPAA).

I understand and agree to the following:

1. Definition of Confidential Information

Confidential information includes, but is not limited to:

- Patient/client names, addresses, phone numbers, and other identifying information
- Medical records, diagnoses, treatment plans, and care notes
- Financial and billing information
- Insurance information
- Social Security numbers
- Any other information that could identify a patient/client

2. Use of Confidential Information

I agree to:

- Access only the minimum necessary PHI needed to perform my job duties
- Never access records of patients/clients I am not assigned to care for
- Never access my own medical records or those of family members through the Agency's systems

- Never share login credentials or allow others to use my access
- Log off or lock computer screens when stepping away

3. Disclosure of Confidential Information

I agree to:

- Never discuss patient information in public areas or with unauthorized individuals
- Never post patient information on social media or share through personal email
- Never take photographs or recordings of patients without proper authorization
- Only disclose PHI as permitted by HIPAA and Agency policies

4. Protection of Confidential Information

I agree to:

- Keep paper records in secure locations
- Properly dispose of documents containing PHI (shredding)
- Report any suspected breaches or security incidents immediately
- Follow all Agency policies regarding information security

5. Duration of Obligation

I understand that my obligation to maintain confidentiality continues even after my employment with the Agency ends. I agree not to disclose any confidential information learned during my employment at any time in the future.

6. Consequences of Violation

I understand that violation of this agreement may result in:

- Disciplinary action, up to and including termination of employment
- Civil and/or criminal penalties under HIPAA
- Personal liability for damages

Acknowledgment and Signature

By signing below, I acknowledge that I have read and understand this Confidentiality Agreement. I agree to comply with all terms and conditions stated herein and with all Agency policies regarding confidentiality and HIPAA compliance.

Employee Signature

Date

Printed Name:

Witnessed by (Supervisor/HR):

Witness Signature

Date

HIPAA TRAINING ACKNOWLEDGMENT

Employee Training Completion Record

Employee Information

Employee Name: _____

Employee ID: _____

Position/Title: _____

Department: _____

Training Details

Training Date: _____

Trainer Name: _____

Training Duration: _____

Training Method: _____

Type of Training:

- ☐ Initial HIPAA Training (new employee)
- ☐ Annual HIPAA Refresher Training
- ☐ Policy/Procedure Update Training
- ☐ Remedial Training (following incident)

Topics Covered

I acknowledge that the training covered the following topics:

- ☐ What is HIPAA and why it matters
- ☐ Protected Health Information (PHI) definition
- ☐ The 18 PHI identifiers
- ☐ Privacy Rule requirements
- ☐ Security Rule requirements
- ☐ Minimum necessary standard
- ☐ Patient rights under HIPAA
- ☐ Permitted uses and disclosures
- ☐ Breach notification procedures
- ☐ How to report security incidents
- ☐ Penalties for HIPAA violations
- ☐ Agency-specific policies and procedures

Employee Acknowledgment

By signing below, I acknowledge and certify that:

1. I have completed HIPAA training as described above.
2. I understand my responsibilities to protect patient privacy and the security of health information.
3. I have had the opportunity to ask questions and receive clarification on HIPAA requirements.
4. I understand the consequences of violating HIPAA, including potential termination and legal penalties.
5. I agree to comply with all HIPAA regulations and Agency policies regarding protected health information.
6. I will immediately report any suspected privacy or security incidents to my supervisor or the Privacy Officer.

_____ _____

Employee Signature Date

Printed Name:

_____

FOR OFFICE USE ONLY

Recorded by: **Date entered:**

_____ _____

Next training due:

HIPAA Compliance Checklist

Use this comprehensive checklist to assess your agency's HIPAA compliance status. Review each item and document your compliance measures.

Administrative Requirements

- [ ] **Privacy Officer Designated**
  A specific individual is responsible for developing and implementing privacy policies.

- [ ] **Security Officer Designated**
  A specific individual is responsible for developing and implementing security policies. (May be same person as Privacy Officer)

- [ ] **Written Policies and Procedures**
  Documented HIPAA policies and procedures are in place and accessible to workforce.

- [ ] **Notice of Privacy Practices**
  NPP is developed, posted, and provided to all patients at first service.

- [ ] **Workforce Training**
  All workforce members receive HIPAA training upon hire and annually thereafter.

- [ ] **Confidentiality Agreements**
  All employees sign confidentiality agreements as part of onboarding.

- [ ] **Business Associate Agreements**
  BAAs are in place with all vendors who access PHI.

- [ ] **Risk Assessment Completed**
  Annual risk assessment identifies vulnerabilities and documents mitigation measures.

- [ ] **Incident Response Plan**
  Procedures for responding to security incidents and breaches are documented.

- [ ] **Sanctions Policy**
  Policy for disciplinary action against workforce members who violate HIPAA.

Physical Safeguards

- [ ] **Facility Access Controls**
  Office areas with PHI have appropriate access controls (locks, badges, etc.).

- [ ] **Workstation Security**
  Computer screens positioned away from public view; automatic screen locks enabled.

- [ ] **Paper Record Security**
  Paper records stored in locked cabinets; not left unattended.

- [ ] **Device Security**
  Mobile devices are encrypted; laptops secured when not in use.

- [ ] **Proper Disposal**
  Paper records shredded; electronic media properly wiped before disposal.

Technical Safeguards

- [ ] **Unique User Identification**
  Each user has unique login credentials; no shared accounts.

- [ ] **Strong Password Policy**
  Passwords meet complexity requirements; changed regularly.

- [ ] **Access Controls**
  Role-based access limits PHI access to job-related needs only.

- [ ] **Encryption**
  ePHI encrypted at rest and in transit (emails, file transfers).

- [ ] **Audit Logs**

  System logs track who accesses ePHI and when; logs reviewed regularly.

- [ ] **Anti-Malware Protection**

  Current antivirus/anti-malware on all systems; automatic updates enabled.

- [ ] **Data Backup**

  Regular backups performed; backups tested for restoration capability.

ANNUAL HIPAA AUDIT CHECKLIST

Internal Compliance Review Tool

Audit Information

Audit Period: _____

Audit Date: _____

Auditor Name: _____

Title/Position: _____

Audit Item	Compliant	Notes/Action Needed
Policy and Procedure Review		
HIPAA policies reviewed and updated within past year	☐	
Notice of Privacy Practices current and accurate	☐	
Policies accessible to all workforce members	☐	
Training and Awareness		
All employees completed annual HIPAA training	☐	
Training documentation on file for all employees	☐	
New hire training completed within 30 days of start	☐	
Business Associates		
List of all business associates current	☐	
BAAs in place for all vendors accessing PHI	☐	
BAAs reviewed and updated as needed	☐	

Risk Management	
Risk assessment performed within past year	☐
Identified risks have documented mitigation plans	☐
Security incidents logged and investigated	☐
Access Controls	
User access reviewed - terminated employees removed	☐
Access levels appropriate for job functions	☐
Password policy enforced	☐
Physical Security	
Office security adequate for PHI protection	☐
Paper records secured in locked storage	☐
Disposal procedures followed (shredding, wiping)	☐

Audit Summary

Total Items Reviewed:

_____

Items Compliant:

_____

Items Needing Action:

_____

Key Findings and Recommendations:

_____ _____

Auditor Signature Date

HIPAA RISK ASSESSMENT WORKSHEET

Security Risk Analysis Tool

About This Worksheet

The HIPAA Security Rule requires covered entities to conduct an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. Use this worksheet to document your risk assessment.

Assessment Information

Assessment Date: _____

Assessment Period: _____

Conducted By: _____

Next Assessment Due: _____

Step 1: ePHI Inventory

List all systems, applications, and locations where ePHI is created, received, maintained, or transmitted:

System/Application	Type of ePHI	Location

Step 2: Threat Identification

Identify potential threats to ePHI (check all that apply to your environment):

Human Threats:

- ☐ Unauthorized access by employees
- ☐ Unauthorized access by outsiders
- ☐ Social engineering/phishing
- ☐ Theft of devices
- ☐ Accidental disclosure

Technical Threats:

- ☐ Malware/ransomware
- ☐ System failure
- ☐ Network intrusion
- ☐ Data corruption
- ☐ Loss of data backup

Environmental Threats:

- ☐ Natural disaster (flood, fire, earthquake)
- ☐ Power failure
- ☐ Other: _____

Step 3: Vulnerability Assessment

For each identified threat, assess vulnerabilities:

Threat	Vulnerability	Likelihood (H/M/L)	Impact (H/M/L)	Risk Level

Risk Level: High = High likelihood + High impact; Medium = Mixed ratings; Low = Low likelihood + Low impact

HIPAA RISK ASSESSMENT WORKSHEET

Page 2 - Mitigation and Documentation

Step 4: Current Security Measures

Document existing safeguards already in place:

Administrative Safeguards:

Physical Safeguards:

Technical Safeguards:

Step 5: Risk Mitigation Plan

For each high and medium risk identified, document mitigation strategies:

Risk	Mitigation Strategy	Responsible Party	Target Date

Step 6: Summary and Certification

Overall Risk Assessment Summary:

High Risks Identified: _____

Low Risks Identified: _____

Medium Risks Identified: _____

Total Risks Requiring Action: _____

I certify that this risk assessment has been conducted in accordance with the requirements of the HIPAA Security Rule. The assessment accurately reflects the current state of ePHI security at this organization.

_____ _____

Security Officer Signature Date

Printed Name:

_____

Document Retention

HIPAA requires that risk assessments and related documentation be retained for a minimum of six (6) years from the date of creation or the date when it was last in effect, whichever is later.

Thank You

for choosing Home Care Agency Blueprint

Additional HIPAA Resources

Resource	Website
HHS Office for Civil Rights (OCR)	hhs.gov/hipaa
HIPAA Breach Portal	ocrportal.hhs.gov/ocr/breach
Security Rule Guidance	hhs.gov/hipaa/for-professionals/security
Privacy Rule Guidance	hhs.gov/hipaa/for-professionals/privacy
OCR Complaint Portal	hhs.gov/hipaa/filing-a-complaint

Need More Help?

Home Care Agency Blueprint offers additional resources and consulting services to help you build a compliant, successful home care agency:

- **State Licensing Guides** - Step-by-step licensing requirements for every state
- **Policy and Procedure Manuals** - Complete, customizable documentation
- **Caregiver Training Programs** - Comprehensive training materials
- **Business Plan Templates** - Investor-ready planning documents

- **One-on-One Consulting** - Expert guidance for your specific situation

Visit Us Online

homecareagencyblueprint.com

Questions? Contact us at support@homecareagencyblueprint.com