AUGMENTIVE BUSINESS 7 SOLUTIONS PVT. LTD.

COMPLIANCE CHECKLISTS

HIPAA Compliance Checklist

Complete checklist for ensuring HIPAA compliance when outsourcing medical records, coding, and billing functions.

Executive Summary

HIPAA compliance is mandatory for all organizations that handle Protected Health Information (PHI). This checklist provides a comprehensive framework for ensuring your outsourcing arrangements — including medical coding, billing, and records management — meet all HIPAA requirements under the Privacy Rule, Security Rule, and Breach Notification Rule.

$1.9M	18	60 Days	6 Years
Average HIPAA violation fine	PHI identifiers to protect	Breach notification deadline	Minimum records retention

HIPAA Overview

The Three HIPAA Rules

HIPAA (Health Insurance Portability and Accountability Act) consists of three main rules that govern how Protected Health Information must be handled:

- Privacy Rule: Establishes national standards for protecting individuals' medical records and other PHI. Sets limits on who can access PHI and under what circumstances.
- Security Rule: Establishes national standards to protect electronic PHI (ePHI) that is created, received, used, or maintained by covered entities. Requires administrative, physical, and technical safeguards.
- Breach Notification Rule: Requires covered entities and business associates to notify affected individuals, HHS, and in some cases the media, when there is a breach of unsecured PHI.

Who Must Comply?

- Covered Entities: Healthcare providers, health plans, and healthcare clearinghouses that transmit PHI electronically
- Business Associates: Any entity that performs functions or activities on behalf of a covered entity that involve PHI (includes offshore vendors, BPO companies, coders, billers)
- Subcontractors: Business associates that create, receive, maintain, or transmit PHI on behalf of another business associate

> **Critical Reminder**
> All outsourcing vendors who access PHI — including offshore medical coders, billers, transcriptionists, and data entry staff — are Business Associates under HIPAA and must sign a Business Associate Agreement (BAA).

The 18 PHI Identifiers

The following 18 identifiers must be protected under HIPAA. Any information that includes one or more of these is considered PHI:

#	Identifier	Examples
1	Names	Patient full name, initials
2	Geographic Data	Street address, city, county, zip code, state
3	Dates	Birth dates, admission/discharge dates, death dates, ages over 89
4	Phone Numbers	Home, work, cell phone numbers
5	Fax Numbers	Any fax number associated with an individual
6	Email Addresses	Personal or work email addresses
7	Social Security Numbers	Full or partial SSNs
8	Medical Record Numbers	Any unique identifier from a healthcare facility
9	Health Plan Beneficiary Numbers	Insurance member/plan numbers
10	Account Numbers	Financial account numbers linked to an individual
11	Certificate/License Numbers	Professional or state-issued license numbers
12	Vehicle Identifiers	VINs, license plate numbers
13	Device Identifiers	Serial numbers, unique device identifiers
14	URLs	Web addresses that identify an individual
15	IP Addresses	Internet Protocol addresses
16	Biometric Identifiers	Fingerprints, voice prints, retinal scans
17	Full-Face Photographs	Photos and comparable images
18	Unique Identifying Numbers	Any unique code or characteristic

Administrative Safeguards Checklist

Administrative safeguards are the policies, procedures, and actions to manage the implementation of security measures. Verify all items below:

Security Management Process

- ✓ Conduct and document annual risk analysis of all ePHI
- ✓ Implement security measures to reduce risks to reasonable levels
- ✓ Apply appropriate sanctions against workforce members who violate policies
- ✓ Regularly review information activity on systems that contain ePHI
- ✓ Document all security management activities

Workforce Security

- ✓ Implement procedures for granting access to ePHI based on role
- ✓ Ensure all workforce members have only the minimum necessary access
- ✓ Document authorization and supervision procedures for PHI access
- ✓ Implement procedures for terminating access when employment ends
- ✓ Maintain records of all workforce clearance decisions

Contingency Planning

- ✓ Establish data backup plans for all ePHI
- ✓ Create and test disaster recovery procedures
- ✓ Document emergency mode operation procedures
- ✓ Conduct annual testing and revision of contingency plans
- ✓ Establish criticality analysis for data and systems

Training & Awareness

- ✓ Provide security awareness training to all workforce members at hire
- ✓ Conduct annual HIPAA refresher training for all staff
- ✓ Train staff on how to recognize phishing and social engineering
- ✓ Document all training completion records
- ✓ Test staff knowledge with simulated phishing exercises
- ✓ Maintain attendance records for all HIPAA training sessions

Physical Safeguards Checklist

Facility Access Controls

- ✓ Implement procedures to control physical access to electronic information systems
- ✓ Document procedures for authorizing access to facilities
- ✓ Maintain activity logs of physical access to data centers/server rooms
- ✓ Implement procedures to protect PHI from unauthorized physical access
- ✓ Conduct regular security audits of physical access controls

Workstation Security

- ✓ Define and document appropriate workstation use policies
- ✓ Implement physical safeguards for all workstations with ePHI access
- ✓ Require automatic screen locks after maximum 15 minutes of inactivity
- ✓ Prohibit viewing of ePHI on screens visible to unauthorized individuals
- ✓ Ensure clean desk policy — no PHI left unattended

Device and Media Controls

- ✓ Implement procedures for final disposal of ePHI media (NIST 800-88)
- ✓ Document procedures for removal of ePHI from devices before reuse
- ✓ Maintain records of hardware and electronic media movements
- ✓ Implement encryption on all mobile devices and laptops
- ✓ Conduct hardware asset inventory quarterly

Technical Safeguards Checklist

Access Control

- ✓ Assign unique user IDs to each workforce member — no shared logins
- ✓ Implement emergency access procedures for urgent situations
- ✓ Encrypt all ePHI stored on servers, laptops, and removable media
- ✓ Implement automatic logoff after period of inactivity
- ✓ Enable audit controls on all systems containing ePHI
- ✓ Implement role-based access control (RBAC) for all systems

Transmission Security

- ✓ Encrypt all ePHI transmitted over open networks (TLS 1.2+)
- ✓ Implement network controls to prevent unauthorized PHI transmission
- ✓ Monitor all data transmissions containing PHI
- ✓ Prohibit transmission of PHI via unencrypted email
- ✓ Use secure file transfer protocols (SFTP, FTPS) for PHI transfer
- ✓ Document all data transmission policies and procedures

Audit Controls

- ✓ Implement hardware, software, and procedural mechanisms to record system activity
- ✓ Conduct regular reviews of audit logs
- ✓ Retain audit logs for minimum 6 years
- ✓ Alert security team on suspicious access patterns
- ✓ Conduct quarterly access reviews for all PHI systems

Business Associate Agreement (BAA) Checklist

Every vendor, contractor, or outsourcing partner who touches PHI must have a signed BAA. Verify the following for all business associates:

- ✓ BAA is signed before any PHI is shared with the vendor
- ✓ BAA specifies permitted uses and disclosures of PHI
- ✓ BAA requires appropriate safeguards to protect PHI
- ✓ BAA includes breach notification obligations (within 60 days)
- ✓ BAA prohibits impermissible uses or disclosures
- ✓ BAA requires return or destruction of PHI upon contract termination
- ✓ BAA is reviewed and updated at least every 3 years
- ✓ BAA covers offshore subcontractors if applicable
- ✓ Vendor's own subcontractors have signed BAAs
- ✓ BAA specifies minimum necessary standard applies

Breach Notification Requirements

What Constitutes a Breach?

A breach is an impermissible use or disclosure of PHI that compromises its security or privacy. Exceptions include: unintentional access by an authorized person, inadvertent disclosure between authorized persons, and good-faith belief that recipient could not retain PHI.

Notification Timeline

Notification To	Timing	Method
Affected Individuals	Within 60 days of discovery	Written notice, media if 10+ returned addresses
HHS Secretary	Within 60 days (500+ affected) or annual report (under 500)	HHS Breach Notification Portal
Media (State)	Within 60 days if 500+ residents of state affected	Prominent media outlets
Business Associates to Covered Entity	Without unreasonable delay, within 60 days	Per BAA terms

Vendor Assessment Checklist

Use this checklist when evaluating any new outsourcing vendor who will access PHI:

Due Diligence

- ✓ Request and review vendor's HIPAA compliance documentation
- ✓ Verify vendor's most recent risk assessment
- ✓ Review vendor's data breach history and incident response
- ✓ Check for any OCR investigations or settlements
- ✓ Verify vendor carries cyber liability insurance ($1M+ recommended)
- ✓ Review vendor's employee background check procedures
- ✓ Assess vendor's staff HIPAA training program
- ✓ Verify vendor's data center physical security certifications (SOC 2)

Technical Assessment

- ✓ Review vendor's encryption standards for stored and transmitted data
- ✓ Verify vendor's access control and authentication mechanisms
- ✓ Assess vendor's logging and monitoring capabilities
- ✓ Review vendor's vulnerability scanning and patch management
- ✓ Verify vendor's network segmentation for PHI environments
- ✓ Assess vendor's disaster recovery and business continuity plans
- ✓ Review vendor's penetration testing history

HIPAA Penalty Reference

Violation Category	Minimum Penalty	Maximum Penalty	Annual Cap
Did not know	$100 per violation	$50,000 per violation	$25,000
Reasonable cause	$1,000 per violation	$50,000 per violation	$100,000
Willful neglect – corrected	$10,000 per violation	$50,000 per violation	$250,000
Willful neglect – not corrected	$50,000 per violation	$50,000 per violation	$1,500,000

Action Plan Template

Use this 90-day action plan to close compliance gaps identified in this checklist:

Priority	Action Item	Owner	Target Date	Status
P1 – Critical	Sign BAAs with all current PHI vendors	Legal/Compliance	30 days	
P1 – Critical	Conduct formal Risk Analysis	IT Security	30 days	
P1 – Critical	Implement encryption on all mobile devices	IT	14 days	
P2 – High	Deliver HIPAA training to all staff	HR	45 days	
P2 – High	Review and update all PHI access permissions	IT Security	45 days	
P2 – High	Implement audit logging on PHI systems	IT	45 days	
P3 – Medium	Conduct physical security audit	Facilities	60 days	
P3 – Medium	Update workforce termination procedures	HR	60 days	
P3 – Medium	Develop breach notification procedures	Legal	60 days	
P4 – Low	Schedule annual compliance review	Compliance	90 days	

About AB7 Solutions

AB7 Solutions provides HIPAA-compliant staffing for medical coding, billing, and clinical documentation with BAAs, staff training, and SOC 2-aligned security controls. Contact us at hello@ab7solutions.com to discuss your healthcare outsourcing needs.