HIPAA Compliance Checklist

For Healthcare Practices, Insurance Agencies & HR Departments

Self-Assessment Edition · 2026

This checklist is designed to help healthcare practices, insurance agencies, third-party administrators, and HR departments conduct a rapid self-assessment of their HIPAA compliance posture. Work through each section, check the items your organization has addressed, and use the scoring guide at the end to identify priority gaps.

How to use this checklist: Review each item with your compliance lead or operations team. Check the box if your organization has fully addressed the item. Leave it unchecked if it is partial, undocumented, or not yet in place.

1 Privacy Rule Fundamentals

- ☐ A current, written Notice of Privacy Practices (NPP) is in place and distributed to patients/members at first service.
  Must be updated any time privacy practices change. Last review date should be documented.
- ☐ The NPP is posted prominently at your physical location and on your website (if applicable).
- ☐ Patients/members have been given the opportunity to acknowledge receipt of the NPP.
  Signed acknowledgment forms or documented attempts to obtain acknowledgment are required.
- ☐ Minimum Necessary standard is applied — staff only access PHI required for their specific role.
  Role-based access controls and documented access policies satisfy this requirement.
- ☐ Patients/members have a process to request access to, amend, or restrict their PHI.
  Responses to access requests must be provided within 30 days under the HIPAA Right of Access Rule.

2 Security Rule — Administrative Safeguards

- ☐ A current, documented Security Risk Analysis (SRA) has been conducted within the past 12 months.
  The SRA is the #1 cited deficiency in HHS audits. It must be documented, not just performed.
- ☐ A Risk Management Plan addressing identified vulnerabilities from the SRA is in place and actively followed.
- ☐ A designated HIPAA Security Officer has been assigned and their responsibilities are documented.
- ☐ Workforce HIPAA training has been completed within the past 12 months and records are maintained.
  Training must cover both Privacy and Security rules. Completion records are required.
- ☐ Sanctions for HIPAA violations are documented in policy and have been communicated to all staff.

3 Security Rule — Technical & Physical Safeguards

- [ ] Unique user IDs are assigned to every individual accessing electronic PHI (ePHI). Shared logins are not permitted.
- [ ] Automatic logoff is enabled on all workstations and devices that access ePHI.
  Recommended timeout is 15 minutes or less of inactivity.
- [ ] ePHI is encrypted at rest and in transit on all devices including laptops, mobile phones, and removable media.
  Encryption is an addressable specification — if not implemented, the decision must be documented and justified
- [ ] Physical access to areas where PHI is stored or accessed is restricted and monitored.
  Includes server rooms, filing areas, reception, and workstations visible to non-staff.
- [ ] A process exists to dispose of PHI securely — shredding paper records and wiping/destroying digital media.
  Vendor contracts for shredding or digital destruction should include HIPAA compliance language.

4 Business Associate Agreements (BAAs)

- [ ] A current inventory of all Business Associates (vendors who access PHI on your behalf) has been documented.
- [ ] Executed BAAs are on file for every Business Associate — including cloud storage, billing services, EHR vendors, and IT support.
  A BAA must be signed before PHI is shared. Verbal agreements do not satisfy this requirement.
- [ ] BAAs are reviewed and renewed when vendor contracts renew or when services change materially.
- [ ] Subcontractor BAAs have been obtained from Business Associates who engage their own subcontractors with PHI access.
  Your BA is responsible for this, but you should confirm it is in place.

5 Breach Notification Readiness

- [ ] A documented Breach Notification Policy and Procedure is in place that covers discovery, risk assessment, and reporting timelines.
  Covered entities must notify affected individuals within 60 days. HHS must be notified; media notification required for breaches affecting 500+ individuals.
- [ ] Staff know how to recognize and report a potential PHI breach internally.
  Internal reporting channels should be clearly communicated in training.
- [ ] A breach log is maintained documenting all potential and confirmed breaches and their disposition.

Your Score	
18–22 Checked	Strong compliance posture. Maintain documentation and schedule annual reviews.
12–17 Checked	Moderate risk. Prioritize unchecked items immediately, especially BAAs and training.
Below 12	High risk. Consider engaging a compliance specialist before your next audit.

Ready to close compliance gaps?

BCO provides hands-on HIPAA compliance support, documentation review, workforce training coordination, and audit preparation so you can focus on serving your clients with confidence.

Schedule a free 30-minute discovery call: beatyco.com · info@beatyco.com