CHECKLIST

HIPAA Compliance Checklist

51 items covering administrative, physical, and technical safeguards plus breach notification, business associate management, and privacy rule requirements.

Published by
Compliance Enablers LLP

Last Updated
March 2026

Pages
~13 pages

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) establishes national standards for protecting sensitive patient health information. Compliance is mandatory for covered entities (healthcare providers, health plans, and healthcare clearinghouses) and their business associates.

This checklist provides a comprehensive, actionable framework for assessing and maintaining HIPAA compliance. Use it as a self-assessment tool, an audit preparation guide, or a foundation for building your compliance program. Each item includes a brief explanation to help you understand the requirement and verify your organization's compliance status.

How to Use This Checklist: Review each item, mark its status (Complete, In Progress, or Not Started), and document evidence for completed items. Items marked In Progress or Not Started should be added to a remediation plan with assigned owners and target completion dates.

Administrative Safeguards (45 CFR 164.308)

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

- ☐ **1. Designated Security Officer** Appoint a Security Officer responsible for the development and implementation of the security policies and procedures required by the HIPAA Security Rule. This individual must have the authority and resources to fulfill this role effectively. Document the appointment, including the officer's name, title, and responsibilities.
- ☐ **2. Designated Privacy Officer** Appoint a Privacy Officer responsible for the development and implementation of the privacy policies and procedures required by the HIPAA Privacy Rule. This may be the same person as the Security Officer or a separate individual. Document the appointment formally.
- ☐ **3. Comprehensive Risk Assessment** Conduct a thorough, documented risk assessment that identifies all reasonably anticipated threats and vulnerabilities to the confidentiality, integrity, and availability of ePHI. The risk assessment should cover all systems that create, receive, maintain, or transmit ePHI. Update the risk assessment at least annually or whenever significant changes occur in the environment.
- ☐ **4. Risk Management Plan** Based on the risk assessment findings, develop and implement a risk management plan that reduces identified risks to reasonable and appropriate levels. Document each identified risk, the selected risk treatment (mitigate, accept, transfer, avoid), and the specific controls implemented. Track remediation activities to completion.
- ☐ **5. Workforce Security Procedures** Implement procedures to ensure that all workforce members have appropriate access to ePHI based on their roles, and to prevent unauthorized workforce members from obtaining access. This includes procedures for authorizing access, establishing access levels, and terminating access when employment or responsibilities change.
- ☐ **6. Security Awareness and Training Program** Provide regular security awareness training to all workforce members, including employees, volunteers, trainees, and contractors. Training should cover password management, phishing awareness, workstation security, reporting of security incidents, and proper handling of ePHI. Document training completion for all workforce members. Conduct training at hire and at least annually thereafter.
- ☐ **7. Security Incident Procedures** Develop and implement policies and procedures to identify, report, respond to, and mitigate security incidents involving ePHI. Define what constitutes a security incident, establish reporting channels, assign investigation responsibilities, and document incident response activities and outcomes.
- ☐ **8. Contingency Plan** Establish a contingency plan that includes: (a) a data backup plan to create and maintain retrievable exact copies of ePHI, (b) a disaster recovery plan to restore any loss of data, and (c) an emergency mode operations plan to enable continuation of critical business processes while the system is being restored. Test the contingency plan at least annually.
- ☐ **9. Periodic Evaluations** Perform periodic technical and non-technical evaluations to assess the extent to which security policies and procedures meet the requirements of the Security Rule. Evaluations should be conducted in response to environmental or operational changes and at least annually. Document evaluation results and any identified deficiencies.
- ☐ **10. Sanction Policy** Develop and apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures. Sanctions should be documented and applied consistently. Communicate the

sanction policy to all workforce members so they understand the consequences of non-compliance.

- [ ] **11. Information System Activity Review** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. Define the frequency of review (daily, weekly, or monthly, depending on the risk level), who performs the review, and how findings are documented and addressed.
- [ ] **12. Access Authorization and Management** Implement policies and procedures for granting access to ePHI based on the principle of least privilege. Define the process for requesting access, approving access, modifying access when roles change, and revoking access upon termination. Maintain records of access authorizations and conduct periodic access reviews to verify that access levels remain appropriate.

Physical Safeguards (45 CFR 164.310)

Physical safeguards are the physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

- [ ] **13. Facility Access Controls** Implement policies and procedures to limit physical access to facilities where ePHI is stored or accessible. This includes access control systems (badge readers, key locks, biometric controls), visitor management procedures (sign-in logs, escorts), and access authorization lists. Maintain records of facility access and review them periodically.
- [ ] **14. Workstation Use Policies** Define the proper functions to be performed, the manner in which they are to be performed, and the physical attributes of the surroundings for workstations that access ePHI. Address screen positioning to prevent unauthorized viewing, automatic screen lock requirements, clean desk policies, and restrictions on the use of personal devices to access ePHI.
- [ ] **15. Workstation Security** Implement physical safeguards for all workstations that access ePHI to restrict access to authorized users. This includes positioning workstations in secure areas, using cable locks for portable devices, implementing privacy screens, and ensuring that workstations in public or shared areas are secured when unattended.
- [ ] **16. Device and Media Controls — Disposal** Implement policies and procedures to address the final disposition of ePHI and the hardware or electronic media on which it is stored. Ensure that ePHI is securely destroyed before devices are disposed of, recycled, or donated. Use methods appropriate to the media type — secure wiping, degaussing, or physical destruction. Maintain disposal records.
- [ ] **17. Device and Media Controls — Re-use** Implement procedures for removal of ePHI from electronic media before the media is made available for re-use. Verify that all ePHI has been effectively removed before reassigning hardware to another user or repurposing storage media. Document the sanitization process and verification.
- [ ] **18. Device and Media Controls — Accountability and Movement** Maintain records of the movements of hardware and electronic media that contain ePHI, and identify any person responsible for such items. Track devices throughout their lifecycle — from procurement through deployment, movement, and disposal. Implement procedures for the receipt and removal of hardware and media that contain ePHI within and from the facility.

Technical Safeguards (45 CFR 164.312)

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

- [ ] **19. Unique User Identification** Assign a unique identifier (user ID) to each workforce member who accesses ePHI. Shared accounts and generic user IDs should be eliminated. Unique identification enables accurate audit logging, accountability, and access management. Document the user identification standard and ensure all systems comply.
- [ ] **20. Emergency Access Procedures** Establish procedures for obtaining necessary ePHI during an emergency. Define what constitutes an emergency, who is authorized to use emergency access procedures, how emergency access is activated, and how emergency access events are logged and reviewed after the fact. Test emergency access procedures periodically.
- [ ] **21. Automatic Logoff** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. Configure automatic logoff on all systems that access ePHI. The timeout period should be risk-appropriate — typically 15 minutes or less for clinical workstations and 30 minutes or less for administrative systems.
- [ ] **22. Encryption of ePHI at Rest** Implement a mechanism to encrypt ePHI stored on electronic media. Use encryption algorithms that meet NIST standards (e.g., AES-256). Encryption at rest protects ePHI in the event of physical theft or unauthorized access to storage media. If encryption is not implemented, document the rationale

and equivalent alternative measures.

- [ ] **23. Audit Controls** Implement hardware, software, and procedural mechanisms that record and examine activity in information systems that contain or use ePHI. Configure audit logging on all systems that process ePHI. Logs should capture user access, data modifications, authentication events, and administrative actions. Retain logs for a minimum of six years.
- [ ] **24. Integrity Controls** Implement policies and procedures to protect ePHI from improper alteration or destruction. Deploy mechanisms to verify that ePHI has not been altered or destroyed in an unauthorized manner. This includes file integrity monitoring, checksums, digital signatures, and database integrity controls.
- [ ] **25. Authentication** Implement procedures to verify that a person or entity seeking access to ePHI is who they claim to be. Deploy multi-factor authentication (MFA) for all remote access to ePHI and for privileged accounts. Implement strong password policies (minimum length, complexity, expiration) and account lockout procedures for failed authentication attempts.
- [ ] **26. Transmission Security — Encryption in Transit** Implement security measures to protect ePHI transmitted over electronic communications networks. Use TLS 1.2 or higher for all web-based access to ePHI. Encrypt email communications containing ePHI. Use encrypted VPN connections for remote access. Verify that encryption is applied end-to-end, not just at the perimeter.
- [ ] **27. Transmission Security — Integrity Controls** Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection. Use mechanisms such as message authentication codes, digital signatures, or checksums to verify the integrity of ePHI during transmission.

Breach Notification Rule (45 CFR 164.400-414)

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

- [ ] **28. Breach Notification Policy** Develop a comprehensive breach notification policy that defines what constitutes a breach, the risk assessment process for determining whether notification is required, notification timelines, and responsible parties. The policy should address both the covered entity's obligations and the obligations of business associates to report breaches.
- [ ] **29. Breach Risk Assessment Process** Establish a documented process for assessing whether an impermissible use or disclosure of PHI constitutes a breach requiring notification. The assessment should consider: (a) the nature and extent of PHI involved, (b) the unauthorized person who used or received the PHI, (c) whether the PHI was actually acquired or viewed, and (d) the extent to which the risk to the PHI has been mitigated.
- [ ] **30. Individual Notification Procedures** Implement procedures to notify affected individuals within 60 days of discovering a breach. Notification must include: a description of the breach, the types of information involved, steps individuals should take to protect themselves, what the organization is doing to investigate and mitigate harm, and contact information for questions. Maintain templates for breach notification letters.
- [ ] **31. HHS Notification Procedures** Implement procedures to notify the Secretary of HHS of breaches. Breaches affecting 500 or more individuals must be reported within 60 days of discovery. Breaches affecting fewer than 500 individuals must be reported annually. Maintain records of all breach notifications submitted.
- [ ] **32. Breach Documentation and Log** Maintain a log of all breaches and suspected breaches, including those that do not require notification. Document the investigation process, risk assessment results, notification decisions, and any corrective actions taken. Retain breach documentation for a minimum of six years.

Business Associate Management (45 CFR 164.308(b), 164.314)

Organizations must manage the compliance of business associates — entities that create, receive, maintain, or transmit PHI on behalf of the covered entity.

- [ ] **33. Business Associate Inventory** Maintain a complete, current inventory of all business associates — organizations or individuals that perform functions or activities on behalf of your organization that involve the use or disclosure of PHI. Include the type of PHI shared, the purpose of the relationship, and the primary contact. Review the inventory at least annually.
- [ ] **34. Business Associate Agreements (BAAs)** Execute a written Business Associate Agreement with every business associate before sharing PHI. The BAA must specify the permitted uses and disclosures of PHI, require the business associate to implement appropriate safeguards, require reporting of breaches, and ensure return or

destruction of PHI upon termination. Review and update BAAs when relationships or services change.

- [ ] **35. Business Associate Risk Assessment** Conduct risk assessments of business associates to evaluate their ability to safeguard PHI. Assess their security posture, compliance programs, incident history, and financial stability. Determine the level of risk associated with each business associate relationship and implement risk-appropriate oversight.
- [ ] **36. Ongoing Business Associate Monitoring** Implement procedures to monitor business associate compliance on an ongoing basis. This may include periodic compliance attestations, security questionnaire reviews, SOC 2 report reviews, or on-site assessments. Increase monitoring frequency for high-risk business associates.
- [ ] **37. Subcontractor Management** Ensure that business associates extend HIPAA requirements to their subcontractors through downstream BAAs. Verify that business associates have procedures to manage their subcontractors' compliance. The chain of accountability must extend to every entity that touches PHI.
- [ ] **38. BAA Termination Procedures** Establish procedures for terminating business associate relationships when compliance concerns cannot be resolved. Include provisions for the return or destruction of PHI upon termination, verification that PHI has been returned or destroyed, and documentation of the termination process.

Privacy Rule Requirements (45 CFR 164.500-534)

The Privacy Rule establishes national standards for the protection of individually identifiable health information and grants individuals rights over their health information.

- [ ] **39. Notice of Privacy Practices (NPP)** Develop, distribute, and maintain a Notice of Privacy Practices that describes how PHI may be used and disclosed, individuals' rights regarding their PHI, the organization's legal duties, and who to contact for more information or to file a complaint. Provide the NPP to patients at the first point of service and make it available on request and on the organization's website.
- [ ] **40. Minimum Necessary Standard** Implement policies and procedures that limit the use, disclosure, and request of PHI to the minimum amount necessary to accomplish the intended purpose. Define role-based access to PHI based on job function and need-to-know. The minimum necessary standard does not apply to disclosures to or requests by healthcare providers for treatment purposes.
- [ ] **41. Individual Rights — Access** Implement procedures to grant individuals access to their PHI within 30 days of a request (one 30-day extension is permitted). Individuals have the right to inspect and obtain copies of their PHI in the designated record set. Provide PHI in the format requested by the individual if readily producible.
- [ ] **42. Individual Rights — Amendment** Implement procedures to allow individuals to request amendments to their PHI. The organization must act on amendment requests within 60 days (one 30-day extension is permitted). If the amendment is denied, provide a written denial with the reason and the individual's right to submit a statement of disagreement.
- [ ] **43. Individual Rights — Accounting of Disclosures** Implement procedures to provide individuals with an accounting of disclosures of their PHI made in the six years prior to the request. The accounting must include the date of disclosure, the name of the entity or person who received the PHI, a brief description of the PHI disclosed, and the purpose of the disclosure.
- [ ] **44. Authorization Requirements** Implement policies and procedures governing the use and disclosure of PHI that require individual authorization. Ensure that authorization forms include all required elements: a description of the information to be used or disclosed, the purpose, the expiration date, and the individual's right to revoke authorization. Maintain signed authorization forms.
- [ ] **45. Uses and Disclosures for Marketing and Fundraising** Implement policies that ensure PHI is not used for marketing purposes without individual authorization, except for limited exceptions (face-to-face communications and promotional gifts of nominal value). If PHI is used for fundraising, provide individuals with a clear opportunity to opt out.
- [ ] **46. De-Identification Standards** If the organization uses de-identified health information, ensure that de-identification is performed in accordance with the HIPAA de-identification standards — either the Expert Determination method (statistical/scientific analysis) or the Safe Harbor method (removal of 18 specified identifiers). Document the de-identification method used.

Documentation Requirements (45 CFR 164.316)

HIPAA requires that certain policies, procedures, and actions be documented and retained.

- [ ] **47. Policy and Procedure Documentation** Maintain written policies and procedures that implement the standards, implementation specifications, and other requirements of the Security Rule. Policies must be reviewed and updated periodically in response to environmental or operational changes. Ensure policies are accessible to all workforce members responsible for implementing them.
- [ ] **48. Documentation Retention** Retain all HIPAA-required documentation for a minimum of six years from the date of its creation or the date when it was last in effect, whichever is later. This includes policies, procedures, risk assessments, training records, BAAs, breach notifications, and other compliance documentation.
- [ ] **49. Policy Review and Update Schedule** Establish a formal schedule for reviewing and updating all HIPAA-related policies and procedures. At minimum, conduct annual reviews. Additionally, review policies whenever there are changes to regulations, the organization's operations, technology, or the threat environment. Document review dates and any changes made.
- [ ] **50. Training Documentation** Maintain records of all HIPAA training provided to workforce members. Documentation should include the training content, date of training, names of attendees, and training completion status. Retain training records for six years.
- [ ] **51. Compliance Program Documentation** Document the overall HIPAA compliance program, including the governance structure, compliance officer responsibilities, risk management approach, audit schedule, and continuous monitoring processes. This documentation should provide a comprehensive view of how the organization achieves and maintains HIPAA compliance.

Compliance Status Summary

Use this summary to track your organization's overall compliance posture.

Category	Total Items	Complete	In Progress	Not Started
Administrative Safeguards	12	___	___	___
Physical Safeguards	6	___	___	___
Technical Safeguards	9	___	___	___
Breach Notification	5	___	___	___
Business Associate Management	6	___	___	___
Privacy Rule Requirements	8	___	___	___
Documentation Requirements	5	___	___	___
Total	51	___	___	___

Next Steps

1. **Conduct a baseline assessment** using this checklist to identify your current compliance status.
2. **Prioritize gaps** based on risk level and regulatory exposure.
3. **Develop a remediation plan** with assigned owners, target dates, and resource requirements.
4. **Implement controls** systematically, starting with the highest-risk gaps.
5. **Document everything** — HIPAA compliance depends on demonstrable, documented compliance activities.
6. **Monitor continuously** — compliance is not a one-time achievement but an ongoing program.
7. **Leverage a GRC platform** to centralize compliance tracking, automate evidence collection, and maintain continuous compliance visibility.

This resource is provided by Compliance Enablers — the unified GRC platform with 27 modules, 261+ compliance frameworks, and built-in security awareness training. Learn more at complianceenablers.com

Ready to Transform Your Compliance Program?

27 modules • 261+ frameworks • 157 templates • 40+ integrations • AI-powered • From $999/yr

Schedule a Demo

Start Free Trial