HEALTH TECH
DEFENDERS

HIPAA CHECKLIST

This checklist includes general questions about the measures your organization should have in place to assert HIPAA compliance. It is not to be considered as legal advice. Completing this checklist successfully does not certify that you or your organization are HIPAA compliant.

Version:
1.1 (11/14/23)

Sponsored by:
Health Tech Defenders

HIPAA Compliance Checklist

Utilize this checklist for a self-assessment of HIPAA (Health Insurance Portability and Accountability Act) compliance within your organization. The HHS Office for Civil Rights has identified the following components as vital aspects of a robust HIPAA compliance program.

ROLES / RESPONSIBILITIES ASSIGNMENT

HIPAA compliance involves various roles and responsibilities within a healthcare organization to ensure the protection of patients' health information. *Note: The specific roles and their scope may vary depending on the size and complexity of the organization.*

☐ **Privacy Officer:** The Privacy Officer is responsible for developing and implementing privacy policies and procedures, conducting staff training, and ensuring that patient information is used and disclosed in accordance with HIPAA regulations.

☐ **Security Officer:** The Security Officer oversees the organization's efforts to safeguard electronic protected health information (ePHI). This includes implementing security policies, conducting risk assessments, and ensuring the security of electronic systems and data.

☐ **Compliance Officer:** The Compliance Officer is responsible for overseeing the organization's overall compliance with HIPAA and other healthcare regulations. This includes monitoring and auditing for compliance and addressing any identified issues.

POLICIES AND PROCEDURES

The Policies and Procedures section of your checklist serves as the foundation for HIPAA compliance within your organization. This section ensures that employees have clear guidance on HIPAA requirements, security measures, incident response protocols, and privacy practices, promoting a consistent and secure environment for PHI across all facets of your organization.

☐ **HIPAA Privacy Rule Policies and Procedures:** Policies and procedures that govern how protected health information is handled, shared, and protected in compliance with the HIPAA Privacy Rule. It includes guidelines on patient rights, minimum necessary access, and proper uses and disclosures of health information.

☐ **HIPAA Security Rule Policies and Procedures:** Policies and procedures that address the protection of electronic protected health information (ePHI) as required by the HIPAA Security Rule. It includes measures to safeguard ePHI through risk assessments, access controls, and incident response protocols.

☐ **HIPAA Breach Notification Rule Policies and Procedures:** Policies and procedures related to the identification, assessment, and notification of breaches of protected health information as required by the HIPAA Breach Notification Rule. It guides organizations on how to respond to security incidents and notify affected parties and regulatory authorities when necessary.

REQUIRED ANNUAL AUDITS / ASSESSMENTS

HIPAA (Health Insurance Portability and Accountability Act) requires covered entities and business associates to conduct various annual audits and assessments to ensure compliance with the law. These audits are essential to safeguard the privacy and security of protected health information (PHI).

☐ **Security Risk Assessment:** Covered entities and business associates must conduct an annual security risk assessment to identify vulnerabilities and risks to electronic protected health information (ePHI). This assessment helps in implementing safeguards to protect ePHI.

☐ **Privacy Rule Compliance Assessment:** Organizations need to assess their compliance with the HIPAA Privacy Rule annually. This involves reviewing privacy policies, procedures, and practices related to the use and disclosure of PHI.

☐ **Security Rule Compliance Assessment:** Similar to the Privacy Rule assessment, organizations must conduct an annual review of their compliance with the HIPAA Security Rule. This includes evaluating the implementation of security safeguards to protect ePHI.

☐ **Asset and Device Assessment:** An asset and device assessment is a process that involves the identification, tracking, and evaluation of all electronic devices and assets within an organization that store, process, or transmit protected health information (PHI).

☐ **Physical Site Assessment:** A physical site assessment involves the evaluation of the physical security measures and practices in place at healthcare facilities or locations where PHI is handled, stored, or accessed.

☐ **Gap Assessment:** A gap assessment involves the process of documenting all deficiencies identified in the previous assessments with the goal of pinpointing areas where an organization falls short of compliance.

REMEDIATION PLANS

This section reviews the creation and documenting of action items aimed at addressing deficiencies and gaps identified through the above listed assessments. This critical step involves developing specific strategies to bring the organization into compliance.

☐ **Document Remediation Plans:** Create comprehensive records of all remediation actions, including a description of the issue, responsible parties, action steps, timelines, allocated resources, and monitoring procedures, to track and ensure the successful resolution of identified deficiencies.

☐ **Review Remediation Plans:** Collaborate with relevant stakeholders to verify that the remediation plans encompass and adequately address all identified deficiencies, ensuring alignment with organizational goals for compliance and data security.

☐ **Retain Remediation Plans:** Safely archive and store all documented remediation plans, for at least 6 years, in a secure and accessible repository, maintaining a historical record of actions taken to address identified deficiencies for future reference, compliance audits, and reporting.

STAFF TRAINING

This section of your HIPAA checklist focuses on ensuring that all employees and workforce members receive comprehensive training on HIPAA regulations and the organization's privacy and security policies.

☐ **Policies and Procedures Training:** training employees on the organization's HIPAA policies and procedures, ensuring that they are aware of and understand the guidelines for handling protected health information (PHI).

☐ **HIPAA Awareness Training:** provide a broad understanding of the Health Insurance Portability and Accountability Act, its importance, and the organization's commitment to PHI protection. It is intended for all employees, regardless of their role.

☐ **HIPAA Security Training:** Specialized training program that delves into the technical and operational aspects of protecting electronic protected health information (ePHI).

VENDORS AND BUSINESS ASSOCIATES

This section of the checklist focuses on the critical aspect of managing external relationships in compliance with HIPAA. It emphasizes the need for proper documentation and agreements with both Business Associates and non-Business Associate vendors, ensuring that all parties handling protected health information (PHI) uphold the necessary privacy and security standards required by HIPAA.

☐ **Business Associate Agreements for each Business Associate:** A BAA is a legally binding contract that outlines the responsibilities and obligations regarding protected health information (PHI) between your organization and your Business Associates.

☐ **Performed Due Diligence on Business Associates:** Verify that your Business Associates have their own robust policies and procedures in place to protect PHI, and that they understand their responsibilities as per the BAA.

☐ **Confidentiality Agreements with non-Business Associate Vendors:** This checklist item pertains to the use of Confidentiality Agreements with vendors that may have access to sensitive information but do not meet the criteria of a Business Associate as defined by HIPAA.

BREACHES

This section addresses the essential elements of breach management and response in the context of HIPAA compliance. It focuses on an organization's ability to effectively investigate, report, and address security incidents and breaches involving protected health information (PHI).

☐ **Ability to Track and Manage the Investigation of All Incidents:** A robust system and process in place for tracking, documenting, and managing the investigation of all incidents and breaches.

☐ **Ability to Provide Required Reporting of Minor and Meaningful Breaches or Incidents: A** structured reporting mechanism that enables the organization to differentiate between minor incidents and meaningful breaches. It ensures that the organization can comply with HIPAA's reporting requirements, notifying affected individuals, regulatory authorities, and other stakeholders as necessary.

☐ **Staff Can Anonymously Report an Incident:** A mechanism that allows staff to report security incidents or breaches anonymously, which can encourage early reporting and improve overall incident response and prevention efforts.