HIPAA Compliance Checklist

Improper safeguards can result in a HIPAA violation and a severe fine when the standards and requirements of the HIPAA Security Rule are not followed correctly. Companies may need to involve their IT Service Provider to implement appropriate security measures to avoid HIPAA violations.

Visual Edge IT can help you navigate HIPAA requirements and establish necessary compliance measures for your technology environment. Here is a HIPAA Compliance Checklist to get you started.

TECHNICAL SAFEGUARDS

☑ 1. Access Control

Implementing technical policies and procedures that allow only authorized users to access ePHI. This means using unique IDs so that each user will have a centrally-controlled, unique username
and PIN code.

☑ 2. Audit Controls

Detailed logs are needed to track all ePHI access attempts and to monitor how ePHI data is manipulated.

☑ 3. Integrity Controls

Authenticates attempts to alter or destroy ePHI data through unauthorized access.

☑ 4. Transmission Security

Implement tools that have functionality to encrypt messages when they are sent beyond an internal firewall server and decrypt messages when they are received.

PHYSICAL SAFEGUARDS

☑ 5. Facility Access & Control

Establishes who has physical access to the location where ePHI data is stored and includes ways to prevent unauthorized physical access, tampering and theft.

☑ 6. Workstation & Positioning Policies

Policies must be created to restrict the use of workstations that have access to ePHI, protect the surrounding area and define how functions are to be performed on the workstations.

☑ 7. Mobile Device Policies & Procedures

If ePHI can be accessed from mobile devices, policies must be in place to identify how ePHI is removed from the devices if the user leaves the organization or the device is re-used, lost, sold, etc.

☑ 8. Hardware Inventory

Inventory of all hardware must be maintained along with a record of movements for each item. Before equipment is moved, a copy of the ePHI must be made.

ADMINISTRATIVE SAFEGUARDS

☑ 9. Risk Assessment & Analysis

Create an ongoing process that locates areas in which ePHI is being used and evaluate ways in which breaches of ePHI may occur.

☑ 10. Risk Management Policy

Conduct evaluations at regular intervals to identify and minimize risks to a reasonable and appropriate level.

☑ 11. Security Personnel

Someone must be responsible for developing and implementing the organization's security policies and procedures.

☑ 12. Restricting Access

Controls must be in place to ensure that ePHI is not accessed by unauthorized users including employees and subcontractors. Authorized access should only be given based on the employee's role. Written agreements need to be signed with partners who have access to ePHI.

☑ 13. Workforce Training & Management

Document employee training on all ePHI access policies and how to recognize potential cyber security risks such as phishing and hacking.

☑ 14. Evaluation & Testing

Regular evaluation and testing of the contingency plan or all key software.

VISUAL EDGE IT