This HIPAA Security Compliant Checklist is provided to you by:

www.HIPAAHQ.com

1.0 – Introduction to the HIPAA Security Rule Compliance Checklist

If your organization works with ePHI (electronic protected health information), the U.S. government mandates that certain precautions must be taken to ensure the safety of sensitive data. The penalties for not complying with these legal requirements set forth by HIPAA can be severe: criminal charges, up to $1.5 million in fines, and liability in civil suits. As such, it is of paramount importance that all entities covered by HIPAA's stipulations engage in periodic compliance checks.

In this article, we will briefly outline all the requirements your organization must satisfy to be considered compliant to the Act.

The purpose of this checklist is to present HIPAA's dense, and oftentimes, confusing requirements in more accessible language.

Keep in mind that, unlike the highly specific legal language used in the Act, layman explanations are more legally ambiguous. As such, do not treat this article as an exact, one-to-one translation of the legal stipulations.

What this checklist CAN do for your organization: expand an employee's/subcontractor's understanding of HIPAA requirements, provide security officers with a general guideline for the policies and procedures that must be covered in compliance reports, and act as a launching point for a new compliance plan.

What this checklist CANNOT do for your organization: replace the proper legal due diligence required for true HIPAA compliance.

2.0 – HIPAA Administrative Safeguards Checklist

The backbone of a covered entity's internal policies, HIPAA's administrative safeguards require your organization to establish procedures that ensure security measures are adequately planned, developed, implemented, maintained, and managed. There are a total of 9 administrative safeguard standards, each of which has one or more implementation requirement(s).

To be compliant with HIPAA's administrative safeguard requirements, ensure that your organization has implemented the following standards:

2.1 – Security Management

This standard requires your organization to implement policies for the detection, prevention, and containment of security violations.

□ Have you conducted a comprehensive risk assessment of potential vulnerabilities to confidentiality, integrity, and availability of ePHI?

□ Do you have policies for sanctioning employees who fail to comply with proper security procedures?

□ Have you implemented procedures to review activity of systems where ePHI is stored (audit logs/access logs/security incident reports)?

2.2 – Assigned Security Responsibility

□ Have you identified a security official to be responsible for developing and implementing security policies and procedures?

2.3 – Work Force Security

This standard is meant to ensure that your organization has procedures in place to grant access to ePHI when it is appropriate.

□ Do you have policies in place for authorizing and supervising employees/subcontractors who work with ePHI?

□ Have you established clearance procedures on how a worker's access to is granted or denied ePHI?

□ Do you have a clear procedure for terminating a workforce member's access to ePHI?

2.4 – Information Access Management

□ If your organization is a subsidiary/part of a larger organization, do you have procedures that prevent the larger organization(s) from accessing ePHI?

□ Are clear policies in place describing how, when, and where access to ePHI can be granted?

□ Have you instituted procedures to consistently document and review a user's access to ePHI?

2.5 – Security Awareness and Training

- □ Do you publish periodic security updates and reminders for your workforce?

- □ Are there policies in place to ensure that your workstations, servers, and digital systems have adequate protections from malicious software?

- □ Have you implemented monitoring procedures for user logins and suspicious activity?

- □ Have you established strict policies for the creation, modification, and protection of secure passwords?

2.6 – Security Incident Procedures

- □ Does your organization have procedures in place for responding to security incidents, mitigating their effects, and documenting them?

2.7 – Contingency Plan

In case of emergencies (like fire, natural disasters, system malfunctions, etc.) your organization must have codified contingency plans to ensure the safety of ePHI.

- □ Do you have a data backup plan for retrieving exact copies of lost or damaged ePHI?

- □ Have you implemented data restoration procedures?

- □ Does your organization have procedures in place that would allow processes critical to the security of ePHI to continue in the event of an emergency?

- □ Do you conduct periodic testing and revisions of contingency plans?

- □ Have you conducted an assessment to determine the data and applications that are critical to your contingency plans?

2.8 – Evaluation

- □ Does your organization conduct periodic evaluations of established policies and procedures to ensure that they continue to adequately protect ePHI?

2.9 – Business Associate Contracts

A Business Associate is anyone who handles ePHI on your organization's behalf (email providers, server hosts, messaging services, clearinghouses etc.).

□ Are your business associates compliant to HIPAA standards?

□ Have you documented the relevant safety assurances through a written contract (Business Associates Agreement)?

3.0 – HIPAA Physical Safeguards Checklist

The second category of HIPAA's Security Rule outlines all the required measures a covered entity must enact to ensure that physical access to ePHI is limited only to appropriate personnel.

3.1 – Facility Access Controls

□ Do you have procedures in place to grant appropriate personnel (e.g. data recovery specialists) access to your facilities in the event of an emergency?

□ Has your organization enacted policies and procedures to protect the facility and its equipment from unauthorized access, tampering, and theft?

□ Have you implemented procedures for validating a person's right to access your facilities, workstations, and software?

□ Are policies in place to ensure that all repairs and modifications of physical security components (doors, locks, etc.) are carefully documented?

3.2 – Workstation Use

□ Have you established clear policies and procedures that outline the manner in which workstations must be used to ensure the safety of ePHI?

3.3 – Workstation Security

□ Do you have physical safeguards in place to ensure that only authorized personnel have access to workstations with ePHI?

3.4 – Device and Media Controls

□ Has your organization established clear procedures for safely disposing of ePHI and/or the hardware it is stored on?

□ Have you implemented policies requiring complete removal of ePHI from storage mediums (hard drives, flash storage, etc.) before they can be reused?

□ Does your organization document the movement of digital media containing ePHI?

□ Have you established procedures to safely backup ePHI prior to the movement of the hardware it is stored on?

4.0 – HIPAA Technical Safeguards Checklist

The last section of HIPAA's Security Rule outlines required policies and procedures for safeguarding ePHI through technology. Although exact technological solutions are not specified, they should adequately address any security risks discovered in the assessment referred to in section 2.1 of this checklist, and comply with established system review procedures outlined in the same section.

4.1 – Access Control

□ Does your organization assign unique usernames/number identifiers to all workforce members who have access to ePHI?

□ Are there procedures in place to ensure that the appropriate individuals can access ePHI in the event of an emergency?

□ Are users automatically logged out of systems containing ePHI after a set time of inactivity?

□ Has your organization implemented policies for encryption/decryption to prevent unauthorized entities from accessing ePHI?

4.2 – Audit Control

□ Has your organization implemented reasonable audit controls (software/hardware/procedural) to record and assess the activity of systems containing ePHI?

4.3 – Integrity Control

□ Have you implemented technical processes (check-sum verification, digital signatures, etc.) to verify that ePHI is not being altered in an unauthorized manner?

4.4 – Person or Entity Authentication

□ As per the risk assessment, has your organization implemented adequate methods for ensuring that individuals trying to access ePHI are who they say they are?

4.5 – Transmission Security

□ Has your organization implemented adequate solutions (e.g. network communication protocols) to ensure that transmitted ePHI cannot be modified without detection?

□ As per the risk assessment, is your organization encrypting ePHI when it is necessary for the security and integrity of the data?

5.0 – Final Considerations

Recognizing that a wide range of organizations store, transmit, and use ePHI, HIPAA's Security Rule is intentionally vague at times; there is no single solution that covers every possibility. The language of the Act is clear in other ways—the onus of determining adequate protections is on the covered entity.

Depending on the unique structure of your organization, you may not necessarily need to follow every stipulation outlined in the Act. Or conversely, you may be legally required to take measures not specifically mentioned in HIPAA. This will be determined by the results of your risk assessment.

As such, there are a few more considerations you should make to ensure your organization is compliant to HIPAA:

□ Where applicable, were all vital assessments conducted by contractors/businesses with adequate security expertise?

□ If certain stipulations were deemed inapplicable to your organization, have you adequately demonstrated this in your compliance documentation?

□ Has all relevant compliance information (policies, procedures, assessment results, security reports, audit reports, etc.) been adequately documented?

□ Does your organization periodically reassess its HIPAA compliance?

- □ Has a HIPAA lawyer assessed your organization’s compliance reports?