PROTECTED HARBOR

HIPAA COMPLIANCE CHECKLIST

Here is a checklist to assist your company in adhering to HIPAA compliance and regulations.

Between **2009** and **2020**, the HHS' Office for Civil Rights received **3,705** reports of healthcare data breaches involving 500 or more records.

A total of **268,189,693** healthcare records have been lost, stolen, exposed, or improperly disclosed as a result of these breaches.

This represents more than **81.72%** of the United States population. Most of these breaches could have been prevented if HIPAA compliances had been ensured.

AUDITS AND ASSESSMENTS

- Internal audits, security assessments, and privacy audits should be performed regularly to ensure data security.
- Using the NIST, determine which of the HIPAA Rule SP 800-66, Revision 1 mandatory yearly audits and assessments apply to your organization.
- Conduct the necessary audits and evaluations, analyze the results, and record any issues or inadequacies.
- To address those flaws and weaknesses, create and document detailed repair plans.
- Implement the plans, evaluate the results, and revise the program if the expected outcomes were not attained.
- Implement the plans, evaluate the results, and revise the program if the expected outcomes were not attained.

RISK ANALYSIS

- Conduct risk analysis regularly in accordance with NIST guidelines.
- Conduct risk evaluations for systems that store electronic health information (ePHI).
- Assess the possibility and effect of potential ePHI issues, and create a risk management policy.
- Put in place adequate security measures for sensitive documents and hazards that have been identified.
- Establish security best practices and maintenance standards.
- Establish security best practices and maintenance standards.

PROCEDURES AND POLICIES

Ensure you're following the HIPAA Privacy Rule, HIPAA Security Rule, and HIPAA Breach Notification Rule in your policies and procedures. Documentation should be kept for annual evaluations. Make sure to design and implement the following:

- Data usage policies and processes, routine and non-routine disclosures, limiting requests for sensitive data, and similar concerns are covered by privacy policies and procedures.
- Business associates policies: Make sure to comply with HIPAA standards by amending existing contracts and agreements. Obtain appropriate contract assurances and document non-compliance sanctions.
- Procedures and deadlines for dealing with requests for access and complaints about privacy. Before using or disclosing PHI for treatment, payment, or healthcare operations, make sure you get written permission from patients.

DATA PROTECTION MEASURES AND SAFEGUARDS

Protect data integrity, availability, and confidentiality by using data safeguards.

Technical safeguards:

- I**ntegrity controls and auditing:** Use integrity controls to ensure that data is high quality and correct. Set up auditing mechanisms to track file access and alterations and alert you to any unusual activity.
- **Encryption:** Encrypt ePHI when sending it over the internet to comply with NIST cryptography requirements.
- **Controls over access, authorization, and authentication:** Make sure only the right people have access to sensitive electronic records. Passwords and key codes should be kept private.

Physical safeguards:

- **Document destruction:** Before destroying critical documents, shred them.
- **Workstation security:** Limit who has access to ePHI to specific workstations. Establish policies governing how and when these workstations can be used.
- **Mobile device and media control:** Establish procedures that regulate how to delete ePHI from a device if it is lost or stolen or if its owner quits the business if ePHI can be accessed via mobile devices.

Administrative safeguards:

- **Employee security awareness and training:** Employees should be taught on ePHI access governance and cybersecurity best practices, such as how to recognize and report malware.
- **Contingency plans:** Create a plan to keep vital business processes running in an emergency while also maintaining the integrity and security of ePHI.

EMPLOYEE COMMUNICATION AND TRAINING

- All staff should receive proper cybersecurity training, and team members should be educated on the necessity of HIPAA compliance:
- All HIPAA compliance training and staff attestation of HIPAA rules and procedures should be documented.
- In the event of a privacy infringement, develop consequences and disciplinary rules and procedures.

BUSINESS ASSOCIATES COMPLIANCE:

- Check that all business associates comply with HIPAA laws regularly.
- Identify all business associates with access to sensitive ePHI records which may receive, transmit, keep, process, or have access to them.
- Ascertain that each business associate has signed a Business Associate Agreement and reviewed BAAs and HIPAA compliance annually.
- Prepare written papers to prove and document your due diligence on your business partners.

CHECKLIST FOR THE BREACH NOTIFICATION PROCESS

- Establish security incident and breach response systems and procedures:
- Keep track of and coordinate investigations into any incidents that compromise PHI security.
- Create mitigating standards and guidelines, as well as disciplinary rules and processes in the event of a breach.
- Create a system for Establish security incident and breach response systems and procedures:
- Keep track of and coordinate investigations into any incidents that compromise PHI security.
- Create mitigating standards and guidelines, as well as disciplinary rules and processes in the event of a breach.

Compliance is a continuous process rather than a one-off occurrence. Monitor and secure your data with additional vigilance. Recognize the value of regular risk assessments, employee training, and good data governance in protecting your company and its clients.

With so many different regulations in place and new ones on the horizon, it can be difficult to stay on top of everything. Protected Harbor helps companies design, manage, and implement their privacy and compliance standards. Contact us today to learn how we can help you stay ahead of the curve in this ever-changing industry.