AbsoluteOps

BRINGING YOU

EASY, AFFORDABLE, AND SECURE CLOUD FOR YOUR BUSINESS

Contact Absolute Ops and we can help you achieve your business and compliance goals!

- Do you need help understanding your compliance responsibilities?
- Have you been given a security questionnaire and need to show compliance?
- Ready to start preparing for HIPAA in your business or product?

hipaa@absoluteops.com 910-500-7335 absoluteops.com/hipaa

The Health Insurance Portability and Accountability Act (HIPAA) is legislation standardizing best practices for maintaining the security and privacy of healthcare data It is a critical safeguard for healthcare organizations and businesses that work with healthcare information. Compliance with HIPAA can feel like quite a daunting task. If you work with healthcare information or have been tasked with becoming HIPAA compliant, the HIPAA compliance checklist below will clearly articulate the high-level steps needed.

HIPAA protects the confidentiality, integrity and availability of patient data or Protected Health Information (PHI). It mandates covered entities and business associates put the correct PHI safeguards in place. There are three main rules:

The Privacy Rule

The Security Rule

The Breach Rule

Below is an overview of the mandatory considerations you need to implement within your policies and procedures to ensure your company is HIPAA compliant.

THE PRIVACY RULE

1. Notice of Privacy Practices

You must share with patients how you will use and disclose their PHI. Along with organizational practices you have in place to protect their PHI.

2. Business Associate Agreement (BAA)

There must be a contract or a written arrangement between covered entities and their business associates (e.g. a vendor). It must clearly specify each entities' responsibilities when it comes to handling and protecting PHI.

3. Minimum Necessary

The use and disclosure of PHI is limited to when it is necessary. For example, a healthcare employee should not view PHI/PII just because they have access. They should only access/transmit the minimum necessary PHI when it is required to perform certain job functions.

4. Authorization

You must get patient authorization to use or disclosure PHI beyond what's permitted by the HIPAA Privacy Rule. There are instances where this is not required.

For example, if your company is collecting PHI to provide treatment and you have already provided the patient notice of privacy practice you don't need authorization in this specific case. However, if you want to use a patient's PHI for research purposes you must obtain authorization.

5. Individual Rights

Under the privacy rule, here are some examples of the individual rights patients have:

- Right of Notice
- Right of Access
- Request of Accounting of Disclosures
- Right of Amend
- Right to Request Restrictions
- Other rights include alternate communications, special requests and the right to file complaints.

6. Release of Information

Your company must confirm the identity of the person requesting PHI before releasing it to ensure they have the proper authorization. An example of this is a release authorization form that a doctor's office requires a patient to complete.

7. Documentation

HIPAA requires covered entities to keep all PHI documentation, including amendments or requests, for at least six years.

THE SECURITY RULE

The HIPAA security rule focuses on security measures for electronic PHI and it requires covered entities to protect electronic PHI using the appropriate technical safeguards. These safeguards work to protect the confidentiality, integrity, and security of electronic PHI.

There are three critical elements of the security safeguards that HIPAA requires.

You'll see more on how to implement some of these safeguards in the HIPAA compliance checklist in the following section.

ADMINISTRATIVE

Polices and procedures, risk analysis, employee training, contingency planning, BAA's and other agreements.

PHYSICAL

Facility access controls, computer use and security, media controls

TECHNICAL

access and authentication, logging and monitoring, data encryption, backups, and data integrity.

SOC 2 and ISO 27001 have roughly a 50% overlap with HIPAA so if you're already compliant with one of these frameworks you are partially compliant with HIPAA.

There are various technical controls that your company will need to have in place to demonstrate compliance against the Security rule. AbsoluteOps can guide you through the planning, design, implementation and support of solutions to enable secure file transfer, encrypted email, muti-factor authentication, endpoint security and data integrity and other software packages to mitigate risk and ensure your data remains secure.

THE DATA BREACH NOTIFICATION RULE

This HIPAA regulation states that covered entities must notify the Secretary of Breaches of Unsecured Protected Health Information within the U.S. Department of Health and Human Services (HHS) if a data breach or security breach of PHI occurs. Covered entities must further notify individuals impacted by the breach within 60 days.

This rule also requires business associates to notify HIPAA-covered entities they are in business with if a data breach of PHI occurs within their organization.

Not reporting a data breach or not following any other HIPAA requirement can result in some heavy fines which can be up to $50,000 per incident.

HIPAA COMPLIANCE AUDIT CHECKLIST

The Office for Civil Rights (OCR) performs HIPAA audits and you can be audited by the OCR including random audits due to a complaint or a data breach.

The checklist below provides an overview of some of the key items the OCR will be checking if you have to go through a HIPAA audit:

1. Documentation

Are your companies' HIPAA policies and procedures documented, up-to-date and effective? Have staff members signed a document to show they acknowledge each HIPAA policy and procedure?

2. Risk Analysis

Have you completed a company-wide risk analysis? Risk assessments are extremely important for passing any InfoSec audit.

3. Training

Have all staff members undergone annual HIPAA training? Could staff members show an auditor they understand HIPAA's privacy and security rules?

4. Ongoing Monitoring

Do you have an ongoing program to monitor risk management and to detect HIPAA violations? This could include internal audits or assessments to ensure all your HIPAA controls and safeguards are working as intended.

5. Business Associates

Have you identified your business associates/vendors and implemented a BAA (Business Associate Agreement)? BAA's must undergo review at least annually and you must document proof of the review.

6. Response Team

Is someone managing your security and privacy compliance? Do you have a dedicated team member assigned to overseeing your HIPAA program and ensuring you maintain continuous compliance?