HIPAA | GENERAL CHECKLIST ✓

There's a lot to tackle when it comes to maintaining HIPAA Compliance. Complete this quick cheat sheet as a starting point to see where your practice needs to improve when it comes to HIPAA training, risk assessments, and more.

HIPAA Security Rule

Physical Safeguard Requirements

- □ Clear and specific procedures for physical access to prevent theft of ePHI from servers or devices
- □ Protection for workstations that may access ePHI (i.e., workstations are not available in areas where patients may see ePHI on monitors, etc.)
- □ Policies for mobile device access to ePHI
- □ Asset log of all hardware devices that house or transmit ePHI (whether in the past or currently)

Administrative Safeguard Requirements

- □ Conduct a yearly risk assessment
- □ Conduct and document regular, ongoing HIPAA training for all employees
- □ Have a designated HIPAA Compliance Officer to implement and enforce risk management policies
- □ Create policies for maintaining the integrity of ePHI within the organization
- □ Get Business Associate Agreements completed with all qualifying business vendors
- □ Restrict access for all ePHI that is not absolutely necessary, and when accessed limit ePHI to only the minimum necessary information
- □ Have a policy in place to report all potential security incidents as required to the HIPAA Compliance Officer

Technical Safeguard Requirements

- □ Control access to ePHI with unique usernames or codes for each user
- □ Establish specific procedures around the release or disclosure of ePHI to patients, business associates, and during an emergency
- □ Provide data quality measures to track changes or alterations to ePHI
- □ Encrypt all data, especially when sent outside the practice, and decrypt received data
- □ Log all access to ePHI in an access log
- □ Document proper login and log out procedures for staff to safeguard ePHI

HIPAA Privacy Rule Requirements

- □ Provide appropriate internal training to employees regarding what information can and cannot be shared
- □ Ensure written patient consent is received before their health information is used for marketing, fundraising or research purposes.
- □ Have procedures in place to comply with patient right of access to ePHI, provided within 30 days unless required sooner by local state laws
- □ Issue Notices of Privacy Practices (NPPs) to advise patients when their data will be used or shared

HIPAA Breach Notification Requirements

- □ Have policies in place to submit breach notifications promptly to OCR or HHS as required, as well as to send a press release if the breach affects more than 500 individuals
- □ Have policies in place to submit breach notifications for less than 500 individuals to the OCR website

Becoming HIPAA Compliant

Trying to maintain HIPAA compliance on your own, typically requiring **more than 80+ hours a year,** can be daunting. Using a software solution that automates your HIPAA program or a consultant can help provide an accurate and thorough review of your practice's needs - without the stress of trying to create and manage a HIPAA program internally. Whatever your path, make sure you adhere to **all the requirements of each part of the HIPAA rules** and regulations to make sure your organization is ready to pass a HIPAA audit.

Abyde

abyde.com
800.594.0883
info@abyde.com

PROUD PARTNER
NMA
Nebraska Medical Association