HIPAA Compliance IT Checklist

Healthcare professionals and businesses are susceptible to violating the Health Insurance Portability and Accountability Act (HIPAA). Violations most often occur due to security failures and compliance oversights. Unfortunately, when it comes to protected health information and the compliance measures designed to protect it—claiming ignorance has not been a successful approach to dodging penalties and fines.

Often, the same technologies that make sharing and bridging personal health information easier can become HIPAA security and compliance threats when they are not effectively implemented and maintained. Healthcare providers may also fall out of HIPAA compliance by not regulating the use of technology and maintaining best practices in their business. You should ask yourself two things— Is your business technology HIPAA compliant and what are you doing to maintain compliance?

911 IT

Terms

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is the federal law that required the creation of standards to protect personal health information from being shared or disclosed without the individual's consent or knowledge.

PHI and ePHI

Protected health information (PHI) includes any personal information such as diagnoses, treatment information, medical test results, and prescription information. Not your business? Keep reading! National identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact are also PHI. ePHI is simply any PHI stored electronically.

The Security Rule

The Security Rule establishes standards for protecting personal health information that is transferred in electronic form. It protects information privacy while allowing a business to adopt technologies to improve the quality and efficiency of PHI record keeping. The Security Rule is also designed to be flexible and scalable so your business can implement policies, procedures, and technologies that are appropriate for your size and organizational structure.

HIPAA History

So what existed before HIPAA? It’s hard to believe, but prior to HIPAA, no standards or general requirements for protecting health information existed. All the while, new technologies were evolving, and the health care industry and all businesses began to move away from paper processes and rely on the use of electronic information systems to pay claims, answer eligibility questions, store and provide health information and conduct a host of other administrative and clinically based functions.

HIPAA Security Checklist

Basics

- Ensure the confidentiality, integrity, and availability of all e-PHI created, received, maintained, or transmitted
- Identify and protect against threats to the security or integrity of the information
- Consider technical, hardware, and software infrastructure
- Consider the likelihood and the possible impact of risks

Risk Analysis

- Evaluate the likelihood and impact of potential risks to e-PHI
- Implement appropriate security measures to address the risks identified in the risk
- Document security measures
- Maintain continuous security protections
- Risk analysis should be an ongoing process, in which a covered entity regularly reviews its records to track access to e-PHI and detect security incidents

Administrative Safeguards

- Identify and analyze potential risks to e-PHI, and implement security measures that reduce risks and vulnerabilities
- Designate a security official who is responsible for developing and implementing its security policies and procedures.
- Evaluate Information Access Management
- Train all workforce members regarding security policies and procedures
- Perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule

Physical Safeguards

- Limit physical access to its facilities while ensuring that authorized access is allowed
- Implement policies and procedures to specify proper use of and access to workstations and electronic media.
- Establish policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of electronically protected health information

Technical Safeguards

- Implement technical policies and procedures that allow only authorized persons to access electronically protected health information.
- Implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.
- Implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.
- Implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.

Resources

HIPAA for Professionals

Health Human Services HIPAA Home Page

Summary of the HIPAA Security Rule