Implementing an Effective HIPAA Compliance Plan

Written By: Emily Tait, M.A.
May 2018

Background

Established in 1996, the Health Insurance Portability and Accountability Act (HIPAA) set forth requirements for the U.S. Department of Health and Human Services (HHS) to develop regulations that protect and secure health information. HIPAA was broken up into two rules, the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) and the Security Standards for the Protection of Electronic Protected Health Information (Security Rule). Together, these rules define specific standards when it comes to how organizations should handle protected health information (PHI), thus protecting patients’ health records and personal information. HIPAA also protects the organizations that deal with PHI because it requires necessary safeguards that help prevent potential breaches of PHI or other vulnerabilities that could put the organization, its workforce, and its patients at risk.

Why a HIPAA Compliance Plan is Important

In order for organizations to guarantee that they are fulfilling all rules and regulations laid out in the HIPAA Privacy and Security Rules, they must have a HIPAA compliance plan in place. HIPAA compliance plans are important for many reasons, but the most important reason is that they ensure all medical records and information considered PHI are secure and efficiently protected from possible breaches. Organizations should include guidelines for physical, technical, and administrative safeguards in their compliance plan to protect the confidentiality, integrity, and availability of PHI and e-PHI. HIPAA compliance plans also hold providers and other workforce members accountable for protecting PHI, and explain the consequences of a PHI breach or violation of the policies in the plan. If a breach or violation of patient information does ever happen, HIPAA compliance plans help mitigate and manage the breach. They also reduce potential risks and vulnerabilities in the future, and can save the organization money by appropriately informing the organization on and enacting necessary safeguards.

Additionally, having a compliance plan assures patients that their PHI is secure. As a result, they may be more likely to disclose important details about their condition or situation, possibly leading to more accurate diagnoses and improved provider-patient relations. HIPAA compliance plans also ensure that all workforce members, employees, physicians, and volunteers are properly trained on how to handle PHI. Guaranteeing that patients’ information is safe, protected, and in dependable hands builds patients’ trust with the organization and bolsters the organization’s reputation in their community.
Top Practices and Policies to Include in HIPAA Compliance Plans

While HIPAA compliance plans vary in every organization depending on the type and size of facility, development level of their compliance program, etc., there are some standard HIPAA practices and policies that are important to implement in any organization that must comply with HIPAA.

HIPAA Compliance Practices and Policies

General

- Implement policies and procedures to ensure compliance with and enforcement of PHI security, use, and disclosure with third parties
- Implement appropriate administrative, technical, and physical safeguards to protect the privacy of PHI
- Perform ongoing monitoring, assessment, and revision, as necessary, or business processes and operations to ensure continued compliance and enforcement of HIPAA standards and in response to any environmental, operational, workforce, technical, or legal changes
- Implement a training plan that informs all workforce members of all policies and procedures that apply to them in their individual roles and train all workforce members regarding HIPAA policies and procedures and PHI use/disclosure upon employment and annually thereafter

Privacy and Security Officials

- Appoint Privacy and Security Officials to oversee HIPAA Programs
- Privacy and Security Officers should address all HIPAA hotline calls in an appropriate and timely manner
- Privacy and Security Officers must track all privacy and security complaints, document all investigative steps taken, and include a case file with all materials
- Privacy and Security Officers will not retaliate against workforce members for reporting a PHI breach or filing a complaint with the Department of Health and Human Services Office for Civil Rights (OCR)

Documentation

- Maintain policies and procedures in written form, including formalized HIPAA Privacy and Security Official position descriptions
- Enter into a written agreement with each organization or vendor that transmits or receives PHI to or from the organization and requires regular access to PHI, and ensure appropriate safeguards are in place for PHI and e-PHI
- Retain written (paper or electronic) record of actions, activities, or assessments required to be documented by HIPAA regulations (including but not limited to committee minutes, executive memorandums, quality improvement evaluations, and/or corrective action plans) for six years from the date it was created and make this documentation available to all workforce members responsible for implementing policies and procedures
- Document and process any complaints of alleged HIPAA violations, mitigate any damages, and investigate and address any violations
• Inform patients of the organization’s HIPAA policies and procedures, and their rights and responsibilities, and receive written acknowledgement that they read and understood all information

Policy Violations/PHI Breaches

• Provide a hotline that is available 24 hours a day, 365 days a year as a way for workforce members to anonymously report complaints concerning violations of policies or procedures and regarding the use and disclosure of PHI
• Workforce members should report any actual or potential violations of laws, regulations, policies, procedures, code of ethics, or business standards to the Privacy and Security Officials
• Workforce members who knowingly falsely accuse another of a breach of HIPAA rules and policy will be subject to appropriate disciplinary action
• Mitigate the effects of inappropriate use or disclosure of PHI that violates HIPAA policies and procedures
• Apply appropriate sanctions against workforce members who fail to comply with HIPAA regulations
• Fully investigate violations of HIPAA policies and procedures and/or breaches of PHI prior to disclosing them to OCR for additional investigation

Steps to Implement a HIPAA Compliance Plan

Given the recommended policies and procedures, organizations should create an effective HIPAA compliance plan that ensures all safeguards are in place and the organization is ready to appropriately handle and protect all PHI. The steps to do this successfully include:

1. Choose a Privacy Officer who will be responsible for overseeing the development, implementation, maintenance of, and adherence to privacy policies and procedures regarding the safe use and handling of PHI and a Security Officer who will be in charge of the ongoing management of information security policies, procedures, and technical systems.
2. Conduct a risk assessment and implement a security management process
   a. Review and document workplace operations for potential risks/vulnerabilities
   b. Check all computers, mobile devices, paper records and storage of records, and additional security measures to ensure that all PHI is being stored, used, and distributed appropriately and securely
   c. Conduct risk assessments after any breach or theft of PHI and after any major change in hardware or software
3. Develop and implement policies and procedures
   a. Utilize policies and procedures to manage and mitigate HIPAA risks
   b. Clearly document all policies and procedures and make them accessible to workforce members
   c. Review and update policies and procedures regularly
4. Train workforce members on HIPAA regulations and the organization’s policies and compliance plan
   a. Communicate HIPAA regulations with patients
5. Monitor, audit, and update facility security measures on an ongoing basis

In Review

Effective HIPAA compliance plans help keep organizations on track when it comes to protecting PHI. Not only do they provide necessary security requirements for PHI, HIPAA compliance plans also implement safeguards that can prevent PHI breaches and other violations of HIPAA policies and procedures that could potentially put the organization, and its patients, at risk. By applying recommended practices, organizations can guarantee a HIPAA compliance plan that patients can trust and that successfully abides by federal and state privacy and security requirements.

About the Author: Emily Tait is the Marketing and Proposal Manager at Compliance Resource Center. She has a master’s degree in professional writing from Carnegie Mellon University and has been part of the Compliance Resource Center team since April 2017.

About Compliance Resource Center: Compliance Resource Center has been leading the compliance industry since 2010 with our complete suite of solutions that are geared towards improving Compliance Program operations. Our solutions ensure that organizations regularly meet federal and state laws and supply the necessary resources to sustain long-term compliance.