HIPAA Associates

How to Prepare for Compliance

A HIPAA Compliance Checklist

Get the Help You Need

The Office of Civil Rights expects all organizations (covered entities and business associates) that manage protected health information to have a viable functioning compliance plan with policies and procedures in place. Are you prepared? Have you recently reviewed your plan? If you are unsure this is a good place to start.

Thank you for using our HIPAA Compliance Checklist. Preparing your organization for HIPAA compliance can be a very stressful and daunting process if you are not armed with all of the correct information. Our checklist will give you the important steps you need to complete this task. We have extensive experience with HIPAA programs and have assisted multiple organizations in developing plans geared for their own institutions.

Walk through the steps on the checklist provided to begin a successful implementation of this important task. If at any time you feel overwhelmed, we are available to assist you and your organization with your HIPAA compliance needs. Don't hesitate to contact us.

Mary & Al Lopez

WHERE TO FIND US

hipaa-associates.org

hipaasupport@hipaa-associates.org

linkedin.hipaa-associates

Legal

Table of *Contents*

Important Contacts

Office of Civil Rights

800.368.1019

ocrprivacy@hhs.gov

hhs.gov

HIPAA Associates

hipaasupport@hipaa-associates.org

HIPAA-associates.org

To Do List

Review the compliance checklist to draft or refresh your plan. This was written by the Office of Inspector General for billing compliance purposes; however, the principles are sound and apply to HIPAA compliance too. The words printed in red in the checklist below are additions to adapt the list for HIPAA.

HIPAA Compliance Checklist

1. Implementing written privacy and security policies, procedures and standards of conduct
2. Designating a privacy and security compliance officer, and if desired a HIPAA compliance committee
3. Conducting effective HIPAA privacy training and security awareness education
4. Developing effective lines of communication to privacy and security officer
5. Conducting internal monitoring and auditing periodically to assess program effectiveness
6. Enforcing standards of conduct through well-publicized disciplinary sanctions and guidelines
7. Responding promptly to complaints, investigations and detected offenses and undertaking efforts to mitigate damage to patient and implement corrective actions

Notes:

What is Important

The intention of HIPAA compliance is to effectively safeguard protected health information (PHI) and give patient's rights over their PHI. The seven elements of a compliance program is a good frame work for organizations to use to address HIPAA privacy rule requirements and security standards.

Seven Steps

1. Implementing written policies, procedures and standards of conduct

Policies and procedures help establish rules and processes that help workforce members carry out their roles in a manner to ensure compliance with privacy and security rules (HIPAA Rules). An organization must create the policies and procedures necessary to implement the requirements of the HIPAA Rules. In a well-crafted program it is necessary to create privacy policies covering patient rights, uses and disclosures of PHI, and to address administrative physical and technical safeguards for PHI. It is important that your HIPAA compliance team deal with all aspects of the plan. We are available to help craft these policies.

Key Points:

1. Privacy policies and procedures
2. Security policies and procedures

Notes:

2. Designating a compliance officer and security officer

The privacy officer is responsible for establishing and updating policies and procedures to protect all forms of PHI, whether electronic, paper or verbal. Additionally, the privacy officer will investigate and respond to complaints and the Office for Civil Rights (OCR) letters or investigations, manage breach responsibilities and oversee the day to day operation and monitoring of the program. The privacy officer may work with other key members of the organization such as compliance, legal, information technology, and human resources. Further, the privacy officer is responsible for the education and training of all workforce members on the HIPAA Privacy Rule and retaining documentation on HIPAA matters.

The security officer assures that safeguards are in place for the organization to protect the confidentiality, integrity and availability of electronic PHI (ePHI). In addition, the security officer will assist the organization in performance of a security risk analysis and update it on a regular basis.

Continued:

Besides those duties, the security officer will draft or oversee the creation of security policies and procedures to comply with security standards. Finally, the security officer is responsible for security awareness training and providing periodic security updates to the workforce.

Notes:

Key Points:

1. Designate privacy and security officer
2. Create a HIPAA compliance committee from key members of the entity

Notes:

Seven Steps

3. Conducting effective training and education

It is a requirement that all workforce members receive training on the privacy policies and procedures that affect their job duties and security awareness training. Workforce members are employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.

A good training program will cover all of the key features of HIPAA to ensure workforce members are comfortable working with PHI. The training will discuss the patient's rights under HIPAA and your organization's responsibilities, and the permissible uses and disclosures of PHI. We have trained thousands of employees, and using our

experience have created a practical on-line training program for teams and individuals who need HIPAA training.

Key Points:

1. Create or obtain HIPAA privacy and security training for your organization
2. Arrange for annual reviews of HIPAA and your plan

Notes:

.....

.....

.....

Contact us for your HIPAA Training

Link to Training

Seven Steps

4. Developing effective lines of communication

Workforce members must have avenues available to them for reporting concerns internally. An organization should have multiple ways to report such as the ability to send concerns or complaints to the privacy officer and also an anonymous method for complaints, such as a toll-free hotline. Organizations must take all reports seriously, conduct a thorough investigation, provide follow-up, and resolution for each report. This is a very important way to deal with concerns within the organization. We have seen multiple situations where there was not an effective internal reporting system in place and the lack of options led to complaint filing directly to the OCR. This creates a situation that may be preventable.

Key Points:

1. Assure the privacy officer is available to all employees for complaints
2. Establish a hotline or method for anonymous complaints.

5. Conducting internal monitoring and auditing

A well-functioning program will have an ongoing process in place to assess and detect areas of non-compliance. Additionally, the program should monitor privacy compliance to identify and correct potential privacy issues. An internal review or audit is an important part of monitoring a privacy compliance program.

Internal staff or an external contractor should conduct an audit of the compliance program on a regular basis. The findings should be made available to the privacy and security officers and others as determined by the organization.

The OCR has an audit program in place to audit activities of covered entities and business associates to support its other enforcement tools. It aims to proactively uncover risks and vulnerabilities to PHI and provide guidance to covered entities. It is recommended that your organization perform an internal audit and review

of your program to deal with any issues before you are faced with an OCR audit.

Key Points:

1. Perform a regular audit of your privacy program
2. Report all audit findings to privacy and security officers and senior management of your organization

Notes:

6. Enforcing standards of conduct through well-publicized disciplinary guidelines

It is important that an organization has privacy and security policies available to members of the workforce. These must outline an organization's responsibilities, policies, and procedures for protecting PHI.

A sanctions or disciplinary action policy should clearly state the implications and penalties of violating the HIPAA policies. In the event of an OCR investigation or to report a breach you will be asked by the OCR what disciplinary actions have been taken. The types of disciplinary actions might be reeducation, termination of the employee or fines based on the type of violation.

Key Points:

1. Establish standards early and make sure your employees are made aware

Seven Steps

7. Responding promptly to concerns, complaints, and breaches and undertaking corrective action

It is imperative for an organization to ensure timely and effective remedial action for offenses and mitigation for the party affected. Lack of a response may create additional exposure for the organization. In addition, every time there is a breach or an incident it is mandatory the privacy officer investigate, mitigate, offer a corrective plan and provide notice according to regulatory guidelines to prevent future issues.

Key Points:

1. Maintain a record of all disciplinary and mitigation action for offenses
2. Review disciplinary guidelines annually

What Is Your Next Step?

We are health professionals who understand HIPAA inside and out.

In today's health care climate, the occurrences of HIPAA violations appear to be on the rise. It is no longer a question of if, but when your organization will have a violation that results in significant penalties. We understand this can be a stressful occurrence in any organization.

Most important, an organization must follow all necessary steps to create a functioning HIPAA Compliance Plan.

HIPAA Associates

Why we can help you.

We have years of experience as privacy officers and with HIPAA issues.

We have assisted many organizations large and small with creation of their HIPAA Compliance Plans. We have the experience to know how best create your plan and assist in making sure it works to protect you in the future. We provide personal assistance to ensure your needs are met.

Mary is a former nurse and attorney. Al is a pulmonary critical care specialist, anesthesiologist, and medical coding specialist. They both have years of experience as HIPAA privacy and compliance officers, and with HIPAA + operational issues. They are certified in healthcare compliance and privacy.

We encourage you to contact us to assist with this important process. We can help your organization stay out of harm's way.

Contact Us Now

Helpful Contacts:

HIPAA Associates:

hipaasupport@hipaa-associates.org

Office of Inspector General:

https://oig.hhs.gov/compliance

Legal: