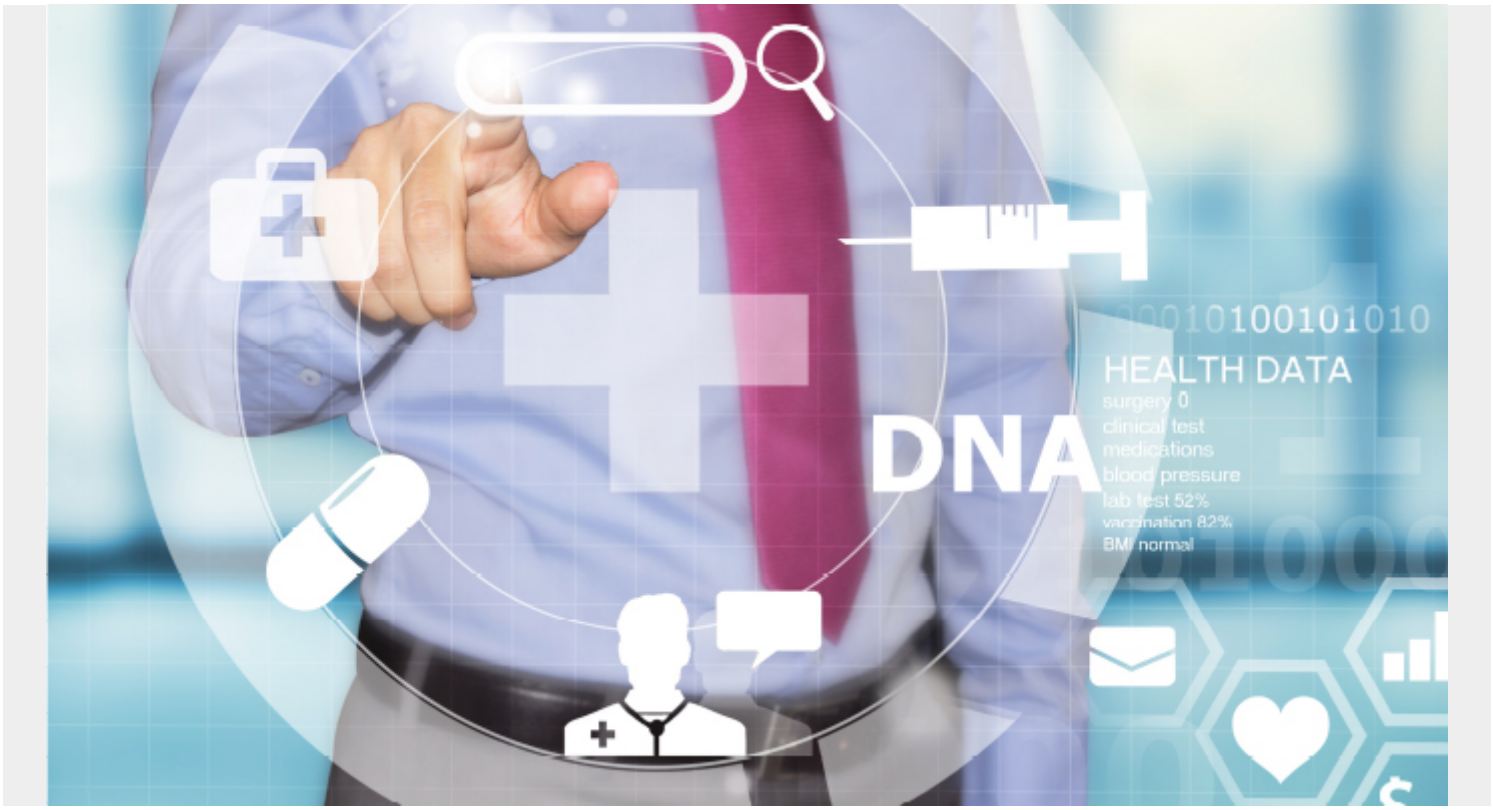
HIPAA INTRODUCTION AND COMPLIANCE CHECKLIST



In a world where healthcare records are increasingly found electronically and on the cloud, protecting this sensitive and confidential information has never been more vital. If you work in healthcare, you

know how often you find yourself with access to sensitive personal information, all of which needs to be properly stored, transmitted, and protected. Patients rely on healthcare organizations to keep their private information private, and to guarantee it never falls into the wrong hands. The federal government also recognizes the importance of protecting this information, which is why they passed the Health Insurance Portability and Accountability Act, also known as HIPAA.

HIPAA establishes the standard for covering the security and privacy of any sensitive or confidential patient data. If your organization deals with protected health information in any form, then you must follow all rules and regulations as outlined by HIPAA. By becoming familiar with these guidelines, you will understand what your company needs to do in order to become compliant.

If you have begun the process of achieving HIPAA compliance, however, you have probably already found yourself overwhelmed with the amount of information it covers, not to mention the sheer volume of content it contains. Luckily, we have done the research for you and put together a HIPAA compliance checklist to assist your business in meeting and exceeding these federal regulations.

What is HIPAA?

HIPAA is a federal legislation in the United States that provides provisions for how to protect the privacy and security of confidential medical information. Originally enacted in 1996 by the U.S. Department of Health and Human Services (HHS), HIPAA was later expanded when the omnibus rule was put into place in 2013. The omnibus rule increased penalties for HIPAA compliance violations to a maximum of $1.5 million per incident, and incorporated the modifications that were set in 2009 by the Health Information Technology for Economic and Clinical Health (HITECH) Act. HIPAA is enforced by the HHS Office for Civil Rights (OCR).

What information does HIPAA protect?

In short, HIPAA protects what is referred to as Protected Health Information (PHI). This information includes anything that relates to:

- The patient's past, present, or future physical condition or mental health condition
- The provision of healthcare to the patient
- The past, present, or future payment for the provision of healthcare to the patient
- Any information, including demographics, that identifies the patient or for which there is a reasonable basis to believe it could identify the patient. Some common personal identifiers include name, address, birthdate, and Social Security Number.

All of this PHI is protected under HIPAA regardless of whether it is stored or transmitted on paper, orally, or electronically.

What is HIPAA Compliance?

If you are a covered entity (health plans, health care clearinghouses, health care providers); provide treatment, payment, or operations in healthcare; have access to patient information; provide support in treatment or payment; are a business associate; or a subcontractor, then you must be in compliance of HIPAA at all times.

Failure to comply with HIPAA regulations can result in criminal charges or hefty fines, regardless of

whether the violation resulted from willful neglect or intention. Even inadvertent violations are not considered justifiable by the Office for Civil Rights of the Department of Health and Human Services, so it is vital that you understand the rules outlined in HIPAA, as well as how your company can comply with them.

Essentially, HIPAA Compliance means that your company follows all of the guidelines and regulations that HIPAA outlines. The largest regulations are often referred to as "rules", and can be summarized into distinct categories:

- Privacy Rule
- Security Rule
- Enforcement Rule
- Breach Notification Rule

It is important to note that while we have provided overviews of each rule, as well as HIPAA compliance checklists, these summaries are extremely brief compared to the actual HIPAA paperwork. Make sure you review all of the rules in detail in order to achieve compliance.

HIPAA Privacy Rule

The HIPAA Privacy Rule sets national standards that protect personal health information and medical records. The rule establishes that specific safeguards must be put in place to protect this privacy, and also sets certain conditions regarding the use of PHI without patient authorization. It explicitly states that patients have the right to access their health records at anytime, and may add corrections when necessary.

How to comply with the Privacy Rule

- Select a privacy official that will be responsible for developing and implementing all privacy policies
- Understand the definition of PHI as well as what is covered under it
- Understand the guidelines for the proper and improper uses and disclosures of PHI
- Keep a record of all uses and disclosures of PHI in your organization
- Identify all of your business associates, as defined by HIPAA
- Establish ongoing employee training of all privacy policies and procedures

HIPAA Security Rule

The HIPAA Security Rule outlines the specifications for the appropriate Technical, Physical, and Administrative Safeguards. Each of these parts add up to ensure the confidentiality and security of patient PHI that is received, maintained, or transmitted in electronic form. Along with the Privacy Rule, the Security Rule is one of the most crucial regulations of HIPAA.

Technical Safeguards

The Technical Safeguards focus on the technology that protects PHI and controls access to it. The type of technology your organization uses to do this is not specified, as long as it addresses the proper standards. The four standards under the Technical Safeguards section include:

- Access Control
- Audit Controls
- Integrity
- Authentication
- Transmission Security

Physical Safeguards

Physical Safeguards are a set of rules and guidelines that focus on the physical access to PHI. Physical access can extend beyond the walls of the office, such as to employees' personal computers and homes, as it includes any place where PHI may be looked at. The four standards under Physical Safeguards include:

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls

Administrative Safeguards

The Administrative Safeguards are a collection of policies and procedures that govern the conduct of the workforce, and the security measures put in place to protect ePHI. There are 9 standards under the Administrative Safeguards section:

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts and Other Arrangements

How to comply with the Security Rule

- Perform a risk analysis for electronic PHI in your organization
- Implement safeguards to address security gaps identified by the risk analysis:
    - Technical
    - Physical
    - Administrative
- Make sure everything is documented appropriately

HIPAA Enforcement Rule

The HIPAA Enforcement Rule outlines the procedures that would happen if your organization would be investigated for possible HIPAA violations. These violations can carry jail time as well as heavy fines up to $50,000 per violation per day.

How to comply with the Enforcement Rule

- This rule is only relevant to you should your company be investigated for any reason

HIPAA Breach Notification Rule

The HIPAA Breach Notification Rule establishes that all healthcare organizations must provide immediate notification of a PHI breach occurs. This notification may include to the affected individuals, the media, or the HHS Secretary, depending on the type of breach. Failure to report a breach will result in major federal fines.

How to comply with the Breach Notification Rule

Again, this rule is only relevant should your organization experience a breach of PHI. For more information on the guidelines of this rule, or for the definition of a breach, see here.

Conclusion

While HIPAA compliance is an extremely important and necessary process, it should not end up being a traumatic experience for your organization. Overall, HIPAA compliance is about adopting good processes within your organization, and ensuring you are protecting confidential and sensitive information. By becoming familiar with the guidelines, and utilizing our checklist, you are one step closer to achieving complete HIPAA compliance.

Resources from BMC

For more information about achieving HIPAA compliance, check out BMC's guide an Introduction to HIPAA Compliance: Everything you need to know about HIPAA Compliance.