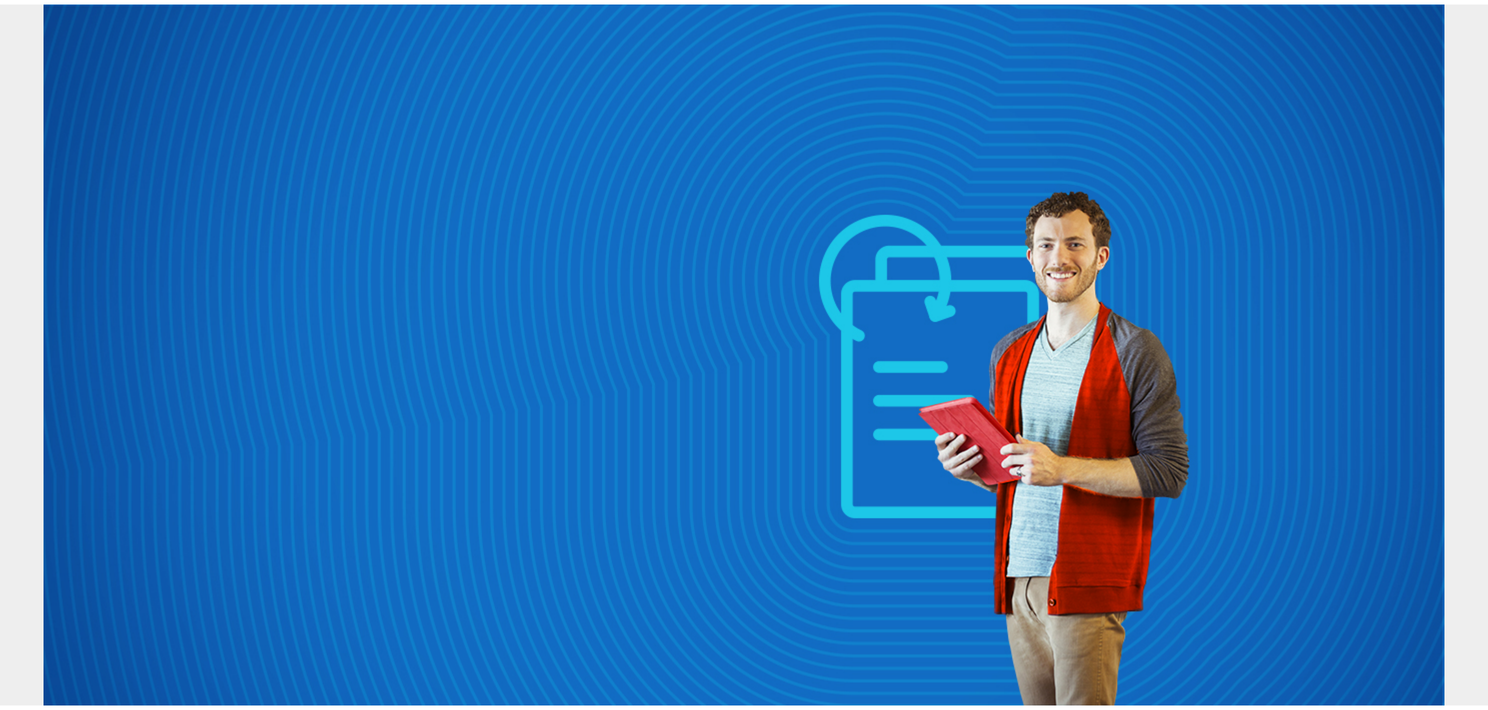
INTRODUCTION TO HIPAA COMPLIANCE



What is HIPAA Compliance?

The American Health Insurance Portability and Accountability Act of 1996, or HIPAA, is a group of regulations that medical providers must follow to ensure that all patients' charts, accounts and records are handled properly. While HIPAA applies to all patient information whether it is stored on paper or transmitted verbally, some of the rules are specific to electronic medical transactions only. Most medical establishments either store, process or transmit medical information electronically, so these facilities must ensure that they are HIPAA compliant.

To comply with HIPAA, medical providers must allow patients to access their medical records and enable them to correct erroneous information. Patients must also be notified of privacy procedures and the way their personal information will be utilized. HIPAA requirements have brought about widespread changes in the way many companies that deal with patient information manage their recording and billing systems.

(This article is part of our Security & Compliance Guide. Use the right-hand menu to navigate.)

What information does HIPAA protect?

HIPAA protects patient information that can be individually identified, whether it is stored or transmitted on paper, orally or electronically. Any information that includes data relating to a patient's health history or current conditions, payment for medical treatment, history of treatment or plans for future treatment along with patient identifiers is protected under HIPAA. Patient identifiers include the patient's name, address or social security number. If health information is not paired with patient identifiers, it may be shared or disclosed at will.

HIPAA’s five rules

The Privacy Rule

HIPPA’s Privacy Rule specifies the people that can access PHI. This rule covers any type of sharing of information, including verbal, written or electronic disclosures. In most cases, the patient must sign a waiver that allows the organization to release health data to certain parties. Without written permission, covered entities cannot share identifiable patient information with anyone not listed under HIPAA’s permitted uses and disclosures section.

Covered entities may disclose PHI to the individual whose information is being shared. Covered entities are also allowed to use and disclose patient information as necessary to maintain its operations, including treatment and payment procedures.

In some circumstances, the covered entity may request informal permission from patients to use and disclose their information. Some healthcare providers maintain patient directories so that visitors who ask for the patient by name may be told where in the facility the patient is located and the status of his or her condition. Medical providers can also use a patient’s informal permission to disclose information to those involved in paying for services or making arrangements in the case of the patient’s death.

The Privacy Rule also allows medical establishments to release information to public health authorities that are legally approved to obtain the data in order to prevent or control illness, injury or incapacity. Public health officials may require the investigation of personal health data when dealing with disease outbreaks, terrorism preparation and program monitoring.

The Security Rule

This rule outlines guidelines, specifications and processes for safeguarding electronic PHI. It designates how PHI must be transmitted and does not apply to verbal sharing of information. The Security Rule involves specifications for administrative, physical and technical safeguards. Covered entities should appoint a specific person or team to implement and monitor compliance within an organization. When it comes to maintaining compliance with HIPAA, covered entities should utilize firewalls, encryption and up-to-date software and operating systems.

The Transactions Rule

Transactions are electronic transfers that involve sending information between two entities for a particular reason. Doctors’ offices transmit claims to health plans via healthcare clearinghouses to request payment for the medical services that they provide. HIPAA implemented a list of accepted transactions and guidelines for the transmission of PHI. If one of these transactions is performed electronically by a covered entity, the HIPAA guidelines must be followed. In addition, HIPAA has designated code sets to be used for electronically transmitting information about diagnoses and procedures.

The Unique Identifiers Rule

To simplify the administration of HIPAA, three identifiers are used to represent covered entities in all transactions. This helps standardize the process, minimizing errors and increasing efficiency. The standard unique employer identifier is the organization’s EIN number. The national provider identifier is a 10-digit number assigned to all healthcare providers. The national health plan identifier represents health plans and financiers.

The Enforcement Rule

The Health Information Technology for Economic and Clinical Health, or HITECH (sometimes called HIPAA-HITECH) Act was passed along with the American Recovery and Reinvestment Act of 2016. The HITECH Act encourages healthcare facilities to implement electronic health records, or EHRs. Monetary incentives and grants are offered through the HITECH Act so that healthcare providers can improve the efficiency of their services. The act is allowing physicians to claim up to $44,000 from Medicare to help them implement EHRs that will help them run their organizations more effectively and make it easier for them to remain HIPAA compliant.

The American Recovery and Reinvestment Act also states ways in which HIPAA will be improved. This act has made enforcement more rigorous. Penalties for failure to comply with HIPAA standards have been increased, and the standards themselves have become more rigorous. The HITECH Act has extended many HIPAA regulations to business associates of covered entities. Many of the enforcement procedures that stem from this act will not be in place until after February of 2016. Penalties for violations can include fines of up to $250,000 or imprisonment.

Managing HIPAA

Although every covered entity must comply with HIPAA, the procedures are relatively flexible. Some providers are small and consist of only one physician in one office. Other covered entities are health plans that have offices across the nation. When implementing HIPAA compliance, covered entities are responsible for examining their specific needs and executing solutions that work for them.

Privacy

Covered entities are required to establish written privacy policies and procedures that are in accordance with HIPAA's Privacy Rule. An administrator must be designated to manage these policies and procedures. All employees working under the covered entity must be trained in privacy policies and procedures.

Complaints

The covered entity must establish a contact person or team to handle complaints and provide information about the entity's policies and procedures. If any use or disclosure of PHI violates the policies and procedures and causes a harmful effect, the organization is responsible for mitigating the damage.

Documentation

Everything must be documented for six years from the last effective date, including privacy policies and procedures, complaints and actions designated by the Privacy Rule. Organizations that employ comprehensive, simple and effective software for maintaining patient data should have more efficient recording procedures.

Covered Entities

HIPAA's rules apply to health plans, healthcare providers and healthcare clearinghouses that convey protected health information, or PHI, electronically in association with specified HIPAA transactions.

Health Plans

Health plans refer to group or individual organizations that pay for medical care, including health, vision and dental insurance providers. If a company establishes and manages a group health plan for fewer than 50 employees, it is not a covered entity. Community health centers are also exempt from

HIPAA requirements.

Healthcare Providers
Healthcare providers are covered by HIPAA whether they are large or small practices. Even if a healthcare provider uses a third party to transmit information associated with a HIPAA transaction, that provider is still responsible for complying with the rules. The third party is considered a business associate and must also comply with HIPAA regulations. Healthcare providers include hospitals, dentists, chiropractors or any practitioner that provides medical attention in exchange for payment.

Healthcare Clearinghouses
Healthcare clearinghouses typically process information for health plans and healthcare providers. They act as intermediaries between practitioners and insurance companies, verifying information on insurance claims and formatting the information so that it can be processed by the insurance company.

A HIPAA compliance checklist

If you believe your organization must comply with the HIPAA regulations, the checklist below can help you develop an implementation plan.

Get a General Idea
The HIPAA rules are so specific and detailed that it is easy to get overwhelmed. Instead of worrying about each specific protection measure, make sure that you understand the basics. Before going any further, ensure that your organization is a covered entity. If it is not, you have to make sure you comply with the regulations. If your organization is a covered entity, you must understand HIPAA's general rules and how they apply to you as well as to your business associates.

Set Up a Team
HIPAA requires organizations to appoint a security officer to be in charge of managing compliance. Because HIPAA's administration safeguards require organizations to document everything, a team should be created to handle compliance issues. Members of this team must have excellent organizational skills. Thorough documentation of all compliance activities and complaints is a HIPAA requirement. Your organization must stay current on HIPAA rules as they are altered and updated. Attempting to do this without a designated team is inefficient and time consuming. Failing to comprehensively adopt HIPAA rules can lead to errors and violations.

Start with the Basics
Any organization dealing with electronic records should implement fundamental security measures. These include installing a firewall and protection against viruses and malware. This software should be updated regularly as well. All staff members working with the electronic system should be trained on these security measures. They should not be allowed to write down passwords or keep them near the computers. In addition, passwords should be exceptionally strong and changed regularly.

Because many individuals in your organization may be working on mobile devices and using removable media, all data should be encrypted. HIPAA does require encryption of individually identifiable PHI when it is transmitted over a public network. However, encryption is not required for private network connections.

Basic security measures should be enforced for the destruction of records. Paper records must be shredded with HIPAA-compliant, high-security equipment. HIPAA also addresses the way in which hard drives and other electronic storage devices must be destroyed when taken out of use.

Map It Out
In order to effectively comply with HIPAA regulations, you must have a good idea of where data flows within the organization. Record all aspects of data movement. Document where it is stored and how it travels through your facility. Make sure that you know who has access to it along the way. This becomes even more complex when you work with business associates who also have access to your data. They need to be HIPAA compliant as well. Mapping out the stream of information will help you develop physical and technical safeguards and get a sense of vulnerable areas.

Required vs. Addressable
Some implementation stipulations are required and must be applied by all covered entities. Others are addressable, which means that the covered entity must evaluate whether the specification is reasonable and appropriate for its facility. This involves analyzing possible threats and determining whether the safeguard will actually protect the PHI in that case.

This makes the HIPAA regulations more flexible. Every addressable specification does not have to be implemented if it doesn't fit the scope of the organization's EHRs. Of course, this requires documentation. If an organization chooses not to implement an addressable specification, the reason must be documented.

Systematically Address Risk
If you're not implementing every rule, make sure that you have an organized procedure for assessing the risk and documenting your decision. For every addressable specification, forecast and describe every potential risk. Go over the security precautions you have in place to mitigate that risk. Decide which threats are more dangerous for your organization and prioritize them by level of risk. Address each specification based on your list of prioritized threats. Most organizations successfully auditing their own HIPAA compliance use automation and management tools like TrueSight Automation for Servers, TrueSight Vulnerability Management for Third-Party Applications, Discovery and CMDB (Configuration Management Database). By starting with basic audits, out of the box HIPAA Compliance Content, and re-using Automation infrastructure, you can get rolling quickly.

Get Help
It may not be feasible for every organization to devote a team to HIPAA compliance. An expert can help you implement the right systems and make sure you're on the right track. Setting up the appropriate technology correctly from the beginning can save you headaches in the future. Implementing HIPAA-ready software can ease the stress of becoming HIPAA compliant. In addition, working with someone who is familiar with HIPAA regulations can ensure that you don't let anything fall through the cracks. BMC provides expert consulting services with ready-made packages, highly-skilled in Transformation, Architecture, experienced and well-versed in implementing Regulatory Compliance.