ClearDATA
SECURE · HEALTHCARE · CLOUD

HIPAA Compliance Beyond IT Security

HIPAA Guide

What is HIPAA Compliance?

HIPAA is a federal law that protects the privacy and security of health data. It is enforced by the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS).

HIPAA was passed in 1996 with the sole purpose of improving the efficiency and effectiveness of healthcare systems by standardizing the electronic exchange of administrative and financial data. In 2009, the act was updated to include a law called the HITECH Act, which expanded the responsibilities of organizations that provide certain services to healthcare provider's actions (Business Associates) under the Privacy and Security Rules, and also added weight to enforcement.

The HIPAA Rules are quite complicated, with hundreds of key activities subject to audit. A comprehensive HIPAA compliance program should allow you to quickly and effectively prove to an auditor or investigator that you have monitored, and both reactively and proactively mitigated risks.

Who is impacted by HIPAA requirements?

HIPAA applies to individuals or entities who create, process, store or transmit any personally identifiable health information in connection with certain transactions. Typically, these entities fall into one of two categories:

- **Covered Entities** - HIPAA defines health plans, healthcare clearinghouses and healthcare providers that electronically transmit any applicable health information as Covered Entities. These organizations have the responsibility to keep patient information confidential and available to appropriate individuals.
- **Business Associates** - HIPAA regulations extend beyond covered entities to cover business transacted via business associates. A business associate is defined as a person or entity who performs a function or activity on behalf of, or provides services to, a Covered Entity that involves Personally Identifiable Health Information, or Protected Health Information (PHI). HIPAA requires that business associate relationships be formalized in a contract or agreement, commonly called a "Business Associate Agreement" or BAA. These agreements are designed to support patient rights by outlining the responsibilities of the parties to protect PHI, among other duties.

If you or your organization fall into one of these categories, HIPAA requires that you:

- Maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting PHI
- Ensure the confidentiality, integrity, and availability of all PHI (create, receive, maintain or transmit)
- Identify and protect against reasonably anticipated threats to the security or integrity of the information
- Protect against reasonably anticipated impermissible uses or disclosures
- Ensure compliance by your workforce
- Have procedures in place for patients to access or amend their information, as well as to request and receive an accounting of disclosures of their data

How do you become HIPAA compliant?

The simple answer is just "follow the HIPAA rules." If you comply with the rules, then you are "HIPAA compliant." There are several challenges with the simple answer:

1 **Complexity** - Take a careful look at a sample audit protocol; even if you understand the applicable rules and satisfy them all at a single point in time, maintaining compliance over time is difficult and expensive, especially in terms of your team's time.

2 **Ambiguity** - In order to maintain HIPAA compliance, you are responsible for implementing what HIPAA calls "reasonable and appropriate safeguards" for PHI, but it's not always clear which rules apply to you, and how. For example, encryption in transit is an "addressable" implementation specification under the Security Rule. Is it reasonable and appropriate not to encrypt traffic between an app and a database inside a virtual private cloud?

What if the database protocol doesn't support encryption? Should you use a different database? There is little official guidance for engineers and developers today, although HHS has announced plans to publish more details in the future. The point is that what may be reasonable to some, may not be reasonable to others.

3 **Uncertainty** - There is no official certification for HIPAA. Ultimately only the OCR can decide whether you have been compliant or not, following an investigation or enforcement action. Obviously you would like to avoid those. Hopefully the upcoming HITECH audit program results will clarify how HHS interprets some of its own rules.

A better answer to "How do you become HIPAA compliant?" might be:

- Decide which HIPAA rules apply to you. For example under the Privacy Rule, posting a Notice of Patient Privacy on a website may not make sense.
- Determine how your policies, procedures, training programs, technology and physical safeguards map to the rules.
- Decide on a repeatable, scalable strategy for tracking compliance events. The low end might be a spreadsheet, the high end might be a GRC ("governance, risk management, and compliance") system.

Examples of things you might want to track include:

- Checklists for regular organizational and application security reviews
- Audit logs for app and backend access permission establishment, modification, and termination
- Audit logs for app and backend access events
- Product security documentation
- Internal control documentation (i.e., "policies and procedures")
- Internal and external security assessment results
- BAAs and other critical legal contracts
- Incident response tickets and reports
- Your own vendor security assessments
- Decide on a risk management framework (e.g., NIST SP 800-37 Rev 1) and begin with a preliminary risk assessment
- Decide on internal administrative controls (aka "policies and procedures")
- Design, conduct, and audit training for your workforce

Repeat all of the above on a regular basis. "No less than annually and as needed based on operational events" is a good starting point.