What is HIPAA?

HIPAA, the Health Insurance Portability and Accountability Act, was designed to provide privacy standards and security requirements for Protected Health Information, or PHI. The Act governs the way health care providers and benefit plans collect, maintain, use, and disclose PHI. In addition, the regulations include standards that are intended to protect health information from unauthorized uses and disclosures.

What is HITECH?

The Health Information Technology for Economic and Clinical Health Act, or the HITECH Act, was passed in 2009 with the goal of encouraging the use of electronic health records and health information technology. It also expanded the scope of regulations that apply directly to Business Associates, like law firms. The Act added new penalties for non-compliance with HIPAA regulations and added the requirement that periodic audits be conducted.

What is the Omnibus Rule?

Effective in March of 2013, the Omnibus Rule clarified security and privacy expectations of Business Associates, or BAs, which includes law firms. The Rule focuses on audits, enforcement, and procedures for breach notification. Finalized in September 2013, the government began enforcing the Rule’s steep penalties for violators and the specific requirements for reporting breaches of protected information.

# HIPAA-related Terms to Know

| **Term** | **Definition** |
| --- | --- |
| **BA** Business Associate | A person or an organization doing business with or performing services on behalf of a health care Covered Entity, such as a hospital or health insurer. BAs are subject to HIPAA guidelines with regard to how they handle Protected Health Information (PHI), and are subject to penalties for disclosure of that information. Because of their work, law firms are classified as Business Associates. |
| **BAA** Business Associate Agreement | An agreement between a Covered Entity and a Business Associate, or between two Business Associates. The agreement stipulates that the Business Associate will comply with the appropriate guidelines and regulations related to handling, using, and securing PHI. Business Associate Agreements typically include requirements for reporting a breach or the disclosure of protected information. |
| **CE** Covered Entity | An organization or corporation that directly handles Personal Health Information (PHI). Common examples include hospitals, doctors’ offices, health insurance providers, and assisted living facilities. Under HIPAA and HITECH, Covered Entities are required to comply with specific guidelines for collecting, maintaining, and securing PHI. |
| **PHI** Protected Health Information | Individually identifiable information relating to the past, present, or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. |
| **ePHI** electronic Protected Health Information | Protected Health Information that is transmitted or maintained electronically. |

*(Continued)*

# Confidential Vs. Protected Information

**Confidential information** is a broad term applied to information with some level of sensitivity for which unauthorized access to or disclosure could result in an adverse effect but not necessarily legal consequences. **Protected information** is highly sensitive information that is protected by law or regulation. It requires the highest level of access control and security protection while in storage or in transit, and there are regulatory consequences associated with failing to secure it appropriately.

How HIPAA Affects Law Firms

Law firms can be affected by HIPAA because they may fall under the Act’s definition of a Covered Entity (CE) if they handle their health care plan funding in a particular way. However, more common is for a law firm to be classified as a Business Associate (BA) as a result of doing work for a Covered Entity, such as a hospital. Three key components of HIPAA relevant to firms:

Privacy Rule

This Rule addresses who may access PHI and states that the amount of PHI provided should be the minimum necessary to achieve the intended purpose. The Rule also explains that appropriate and reasonable should be taken to ensure the security of PHI.

Security Rule

The Security Rule specifies requirements for handling ePHI in the areas of Administrative Safeguards, Technical Safeguards, and Physical Safeguards. Administrative Safeguards might include implementing security measures to reduce risk, managing firm employees’ access to ePHI, and providing training on relevant security policies and procedures. Technical Safeguards can include hardware, software, and/or procedural mechanisms implemented to control access, to audit, and to ensure data integrity. Physical Safeguards include facility access and workstation and device security.

Breach Notification Rule

The Breach Notification Rule defines what constitutes a breach and establishes the requirements for reporting one. A breach is defined by the US Department of Health and Human Services as the "acquisition, access, use, or disclosure" of PHI in violation of the Privacy Rule that "compromises the security or privacy" of the PHI.

Best Practices for HIPAA Compliance

* **Know Where PHI is Stored**: Familiarize yourself with what constitutes PHI and the types of work at the firm that might involve PHI.
* **Understand PHI Procedures**: Learn firm procedures for handling, storing, and securing PHI and know the Business Associate Agreement requirements for the work you participate in. Make it a point to understand how protected information is managed at the firm.
* **Know the Protocol for Reporting Breaches**: Follow the firm procedures for reporting the incident and raise any concerns regarding a possible breach or any PHI-related issues.