

# HIPAA for Labor and Employment Attorneys: What you Need to Know

---

Written By **J. Michael Fields** (jmf@wardandsmith.com)

February 11, 2022



**In their law practices, attorneys can regularly handle sensitive patient information that's protected under the Health Insurance Portability and Accountability Act (HIPAA). Lawyers have a duty and responsibility to safeguard such information or face severe penalties for**

**noncompliance.**

This article summarizes a webinar we hosted for the Law Firm Alliance's Employment Community. It lays out some HIPAA basics that are helpful for employment attorneys to understand, starting with three aspects associated with HIPAA.

## **What is HIPAA?**

- Privacy Rule - attempts to protect the privacy of patients by restricting the allowable uses and disclosures of protected health information (PHI):
  - Stipulates when, with whom, and under what circumstances PHI may be shared
  - Gives patients the right to obtain and examine their health records
  - Gives patients the right to direct covered entities' disclosures to third parties
  - Gives patients the right to request corrections to health records
- Security Rule - attempts to ensure that PHI a covered entity creates, receives, maintains, or transmits electronically is appropriately secured
- Breach Notification Rule - requires notification of a breach of PHI

The HIPAA Privacy Rule does not apply to everyone, and it does not apply to everything. Instead, the HIPAA Privacy Rule applies to covered entities and business associates. Within that context, the HIPAA Privacy Rule generally only applies to PHI.

## **Who Must Comply with HIPAA Regulations?**

For HIPAA, a covered entity may include:

1. Health Care Providers

2. Health Care Clearinghouses
3. Health Plans

Regardless of size, every health care provider that electronically transmits PHI in connection with certain types of transactions is a covered entity. Benefit eligibility inquiries and referral authorization requests are covered transactions; the Department of Health and Human Services (HHS) has established standards for other transactions.

The privacy rule applies to a health care provider, whether it electronically transmits these transactions directly or uses a third party to do so on its behalf. The definition of a health care provider covers nearly all providers of services, whether public or private hospitals, sole proprietors, or group practices.

Health care clearinghouses are more complicated and less common. A health care clearinghouse is any entity that processes information on behalf of another entity, such as a health care billing service.

According to HIPAA, a health plan is defined as an individual or group plan that provides or pays for the cost of medical care. The term includes the following:

- Group Health Plans
- Dental Insurer
- Vision Insurer
- Prescription Drug Insurer
- Health Maintenance Organizations
- Medicare and Medicaid

There are two alternatives for eligibility to be a group health plan under HIPAA. The plan has to have 50 or more participants, or there must be a third-party administrator. If a plan has less than 50 participants and is self-administered, it is not a group health plan under HIPAA.

Under HIPAA, several plans, policies, and programs are not covered by the definition of a group health plan. A few of these exceptions include:

- Accidental Death Policies
- Dismemberment Policies
- Disability Income Insurance
- Liability Insurance
- Worker's Compensation Insurance
- Coverage for On-Site Medical Clinics

The other category covered by HIPAA is a business associate, defined as a person or entity that performs certain functions or activities on behalf of a covered entity. Business associates are covered under the HIPAA Privacy Rule if the functions or activities involve the use or disclosure of PHI.

A few examples of functions or activities that could result in a particular person or entity being termed a business associate include claims processing or administration, data analysis, utilization, review, quality assurance, billing, benefit management, and practice management. Other services that might be implicated include legal actuarial accounting, consulting, management, and financial and intellectual property.

The HHS website has frequently asked questions and day-to-day examples of what may constitute a business associate. A law firm that provides legal services to a health plan or a health care provider involving access to PHI would be a business associate; an independent medical transcriptionist that provides transcription

services to a health care provider would also qualify.

A janitorial service that maintains a health care provider's office and has the potential to inadvertently or incidentally come into contact with PHI would not be a business associate, however. This is due to the fact the janitorial service is not tasked with receiving or transmitting PHI.

### **What Does HIPAA Protect?**

PHI refers to individually identifiable health information held or transmitted by a covered entity or business associate in any form of media, whether electronic, paper, or oral. As the name implies, individually identifiable health information is defined as demographic data associated with an individual that could identify that individual.

This could be an address, birthday, or social security number, basically anything for which there is a reasonable basis to believe the individual's identity could be determined. The HIPAA Privacy Rule excludes two items from the definition of PHI:

- Employment Records - pertains to records with PHI a covered entity maintains in its capacity as an employer, as opposed to its capacity as a covered entity
- Education Records - subject to the Family Educational Rights and Privacy Act

Generally, the use or disclosure of PHI is only permitted if a patient specifically authorizes it in writing or if it is required or permitted elsewhere in the HIPAA Privacy Rule. HIPAA requires that a covered entity disclose PHI in only two situations:

1. When requested by the individual or the individual's personal representative
2. When requested by HHS as part of a compliance investigation, review, or enforcement action

The use and disclosure of PHI are permitted, but not required if it is for the purpose of treatment of a patient. For example, consulting with a specialist to discuss a patient's care is a treatment disclosure that does not require the patient's authorization.

Uses and disclosures associated with obtaining payment for health care services do not require patient authorization. If a provider hired a law firm or collection agency to assist with collecting an unpaid bill, patient authorization to disclose PHI would not be required. However, a business associate agreement would be required.

Uses and disclosures associated with health care operations also do not require patient authorization. An example could arise in merger and acquisition discussions between two health care providers, where the buyer entity asks to review certain books and records of the selling entity.

### **Key Takeaways for Attorneys**

One thing attorneys should know is that generally, employers do not meet the definition of a covered entity under HIPAA. The HIPAA Privacy Rule would apply if an employer obtains health information on behalf of the employer-sponsored group health plan. Conversely, the rule would not apply if PHI is being collected as:

- An aspect of the ordinary course of employment
- A means of tracking employee vaccination status

An exception pertains to on-site medical clinics. With regard to on-site clinics, the employer is exempt from direct compliance; however, the actual providers/clinicians at that on-site clinic may be covered entities and

thus may very well be bound by the HIPAA Privacy Rule.

However, HIPAA Privacy Rule typically does not apply to some attorneys that constantly receive subpoenas for employment records. Even if there is PHI in the file, HIPAA does not apply and does not prohibit you and/or your client from disclosing that information.

Many attorneys that do not deal with HIPAA frequently will have employees sign a PHI disclosure authorization when it isn't necessary. There is nothing wrong with that, and it improves the chances of getting the requested information.

But at what point does an attorney become a business associate? A good practice is to have a new covered entity client sign a business associate agreement when it signs the engagement agreement. This is due to the fact that situations can quickly change, and HHS can sometimes fine business associates for not having an agreement in place when one was required. To ensure certain items do not bind the firm in the business associate agreement, it's best to include a provision stating the agreement only applies if and to the extent that HIPAA applies.

I often recommend that attorneys visit the HHS website as it includes HIPAA guidance, frequently asked questions, and a sample business associate agreement to help ensure compliance.

--

© 2022 Ward and Smith, P.A. For further information regarding the issues described above, please contact J. Michael Fields.

*This article is not intended to give, and should not be relied upon for, legal advice in any particular circumstance or fact situation. No action should be taken in reliance upon the information contained in this article without obtaining the advice of an attorney.*

*We are your established legal network with offices in Asheville, Greenville, New Bern, Raleigh, and Wilmington, NC.*