

## **HOW DOES HIPAA APPLY TO EMPLOYERS?**

by

Julie R. Shank  
Partner, Bowles Rice LLP

### **Overview**

Many employers wonder if they need to comply with HIPAA. Of course, there is never an easy answer, and a fact intensive analysis should be performed to determine if HIPAA applies. This article is intended to discuss the common situations in which HIPAA applies to employers.

### **General Principals of HIPAA**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was adopted by Congress in 1996. HIPAA's purpose is “to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.” HIPAA, Pub.L. No. 104–191, 110 Stat.1936l; *U.S. v. Jones*, 471 F.3d 478 (3d Cir.2006). The statute authorizes the Secretary of Health and Human Services to “adopt standards” that will “enable health information to be exchanged electronically, ... consistent with the goals of improving the operation of the health care system and reducing administrative costs,” and that will “ensure the integrity and confidentiality of [individuals' health] information [and protect against] ... unauthorized uses or disclosures of the information.” 42 U.S.C. § § 1320d–2.

HIPAA's Privacy Rule sets forth that "protected health information" may not be disclosed except as provided by HIPAA. To determine if HIPAA applies to a given situation, two questions must be asked. First, is the disclosing person or entity a "covered entity?" Second, is the information sought "protected health information?"

Under the Privacy Rule, if the information is not created or received by a health care provider, health plan, or health care clearinghouse, it is not protected. "Covered entity means: (1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter." 45 C.F.R. § 160.103. A "health care provider" is "a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business." 45 C.F.R. § 160.103. The key to qualifying as a "health care provider" under HIPAA is engaging in health care transactions.

The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number). The Privacy Rule calls this information "protected health information" (PHI). Protected health information means individually identifiable health information:

- (1) Except as provided in paragraph (2) of this definition, that is:
  - (i) Transmitted by electronic media;

- (ii) Maintained in electronic media; or
  - (iii) Transmitted or maintained in any other form or medium.
- (2) Protected health information excludes individually identifiable health information:
- (i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
  - (ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);
  - (iii) In employment records held by a covered entity in its role as employer; and
  - (iv) Regarding a person who has been deceased for more than 50 years.

45 CFR § 160.103. Individually identifiable health information is defined as:

...information that is a subset of health information, including demographic information collected from an individual, and:

- (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
  - (2) Relates to the past, present, or future physical or mental health or 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; and
- (i) That identifies the individual; or
  - (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

*Id.*

### **How does HIPAA apply to employers?**

The good news is that unless an employer clearly operates as a health plan, health care clearinghouse, or health care provider, it is likely not required to comply with the stringent requirements of HIPAA. As stated above, employment records are not PHI as defined by HIPAA. So, simply offering a group health plan through a health insurance policy does not

make the employer a “covered entity.” Whether or not an employer is subject to HIPAA largely depends on whether the employer and insurer share PHI for plan administration purposes. *See* 45 CFR 164.504(f). It should also be noted that an employer does not violate HIPAA by asking an employee for a doctor’s note if it needs the information for sick leave, workers’ compensation, wellness programs, or health insurance.

However, if an employer sponsors one or more self-insured group health plans, such as group health, dental, vision, pharmacy benefits, long-term care, health care reimbursement flexible spending accounts, or employee assistance programs.<sup>1</sup> In this situation, the employer is acting as the covered entity and must comply with HIPAA regulatory requirements, including workforce training, physical, technical, and administrative safeguards for PHI, notifying plan participants when a breach occurs, designating Privacy and Security Officer, and restricting access to PHI.

Additionally, if an employer is a “business associate” to a covered entity, then it will need to comply with HIPAA. A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. 45 CFR 160.103. Common examples of employer-business associates relationships with covered entities include accounting firms, third-party administrators, and consultants.

---

<sup>1</sup> Health plans with less than 50 eligible participants that are self-insured and administered in house by an employer are exempt from compliance. *See* 45 CFR § 160.103.

### **What about workers compensation information?**

An employer disclosing health information for workers compensation purposes does not subject it to HIPAA, except to the extent that it is otherwise considered a covered entity. 45 CFR § 164.512(l), *[u]ses and disclosures for which an authorization or opportunity to agree or object is not required*, states that “[a] covered entity may disclose protected health information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.” So, an employer needs to look to state law to determine the extent of health information that is required to be disclosed. In West Virginia, transmitting an employee’s record of injury to the workers compensation board office without an authorization from the employee will not violate HIPAA.

### **Do employers need to consider other laws?**

Even though HIPAA may not apply in every situation, employers need to consider the restrictions of other laws in handling employee health information. For example, state privacy laws, the Family and Medical Leave Act (FMLA), the Americans with Disabilities Act (ADA), and the Genetic Information Nondiscrimination Act (GINA) contain restrictions on how employee health information is handled.

### **Conclusion**

HIPAA can be intimidating. However, it is narrowly drawn and does not apply to employment records. While there are several situations which invoke HIPAA, employers largely are not subject to full HIPAA compliance.