PRO BONO BRIEF™
NONPROFIT LEGAL NEWS
August 8, 2024

This article presents general guidelines for Ohio nonprofit organizations as of the date written and should not be construed as legal advice. Always consult an attorney to address your particular situation.

HIPPA and Nonprofits: Does Your Organization Need to Comply?

Chris Bennington, Esq., and Bailey Cremeans, J.D., *Epstein Becker & Green PC*

When a 501(c)(3) public charity has access to its clients' health information, a question often arises as to whether the organization must comply with the Health Insurance Portability Act of 1996 (HIPAA). In this article, we provide an overview of HIPAA, focusing on how it may apply to 501(c)(3) nonprofits and the implications for those that are subject to HIPAA.

What is HIPAA?

While HIPAA covers a variety of other subjects, the part relevant to this discussion protects individuals' private health information from being used and disclosed without their consent or knowledge. The U.S. Department of Health and Human Services (HHS) enforces HIPAA, and it has issued three key regulations that give individuals certain rights regarding their health information.

The first of these regulations is the HIPAA Privacy Rule, which protects patient privacy while permitting the flow of health information needed to facilitate quality healthcare. The Privacy Rule protects patients' individually identifiable health information, such as medical records. This information is referred to as "protected health information (PHI)." The Privacy Rule allows individuals the right to access and obtain their own PHI.

The Security Rule is the second regulation, and it protects PHI that is stored or transferred electronically. The Security Rule places safeguards on the disclosure and use of electronic PHI.

Finally, the Breach Notification Rule requires entities covered by HIPAA to notify affected patients, HHS, and in some cases, the media, when a "breach" of PHI occurs.

Who does HIPAA Apply to?

HIPAA applies to "covered entities" and "business associates." A **covered entity** is defined as a health plan, health care clearing house, or a health care provider that transmits health information in an electronic form. A health plan is an individual or group plan that provides or pays the cost of medical care. A health care clearing house is an entity that sends, receives, and processes health information – typically for billing purposes. HIPAA defines a health care provider as a provider of health services or any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

A **business associate** is a person or entity that arranges, creates, receives, maintains, or transmits PHI on behalf of a covered entity for the purpose of conducting an activity that is regulated by HIPAA. Examples of such activities include, but are not limited to, claims processing/administration, data analysis, utilization review, quality assurance, billing, patient safety activities, and benefit management. A person or entity that provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to a covered entity is also considered a business associate under HIPAA.

When Are 501(c)(3) Organizations Covered Entities?

Nonprofit organizations can be covered entities, but this depends on several factors. Often, nonprofits provide health care services, meaning they fall under HIPAA's definition of a health care provider. However, not all health care providers are considered covered entities under HIPAA. To be considered a covered entity, a health care provider must electronically transmit PHI for the purpose of specific transactions such as billing/claims for health care benefits, encounters, payments, eligibility requirements, referrals, or other financial transactions related to health care. Therefore, if a nonprofit transmits PHI electronically for payment, it will be considered a covered entity and will be subject to HIPAA.

For example, an organization that provides health care services using grant funds and does not bill the client's insurer for those services is not a covered entity under HIPAA. Additionally, if a nonprofit bills a client's insurer using only paper claims forms rather than electronic billing, it is not a covered entity. However, if a nonprofit receives grant funding but also bills insurers electronically for some health services, it is considered a covered entity and is bound by HIPAA. It is important to consider that, even when a nonprofit outsources its electronic billing to a third party, the organization will be a covered entity, and the third party will be a business associate, meaning that both parties are bound by HIPAA.

501(c)(3) public charities generally do not qualify as health plans, as they are not individual or group health plans that provide or pay the costs of medical care delivered to their clients. HIPAA does not apply to a 501(c)(3) public charity in its capacity as an employer, even though the organization often maintains medical information on file for its employees. However, if the organization offers a health plan to its employees, that health plan is subject to HIPAA. For fully-insured plans, the insurer will assume most of the HIPAA compliance obligations; for self-insured plans, the employer is responsible, though it may delegate much of the obligations to its third party administrator. However, a health plan with fewer than 50 participants that is administered by the sponsoring employer is excluded from the definition of "group health plan."

When Are 501(c)(3) Public Charities Business Associates?

Even if a nonprofit is not a covered entity, it may still be required to comply with many requirements of HIPAA if it serves as a "business associate" to one or more covered entities (or business associates of covered entities). In determining whether the organization is a business associate, it should first determine whether it provides services to or on behalf of any covered entities or business associates. If it does not, it is not a business associate. If it does, it should then determine whether it creates, receives, maintains, or transmits PHI

in the course of providing services to or on behalf of the covered entity or business associate. If it does not, it is not a business associate. If it does, it is likely a business associate. The nonprofit should confer with legal counsel for assistance in making this determination and, if the nonprofit is determined to be a business associate, assistance with establishing a HIPAA compliance program.

What must a 501(c)(3) Public Charity do to comply with HIPAA?

If an organization qualifies as a covered entity, it must comply with the HIPAA Privacy, Security Rules, and Breach Notification Rules. Nonprofits that are business associates must also comply with many of the requirements of the Privacy, Security, and Breach Notification Rules. The following is a brief overview of these requirements.

A. The Privacy Rule

Under the Privacy Rule, covered entities are required to provide individuals with access to their own PHI, such as medical records and billing records. The Rule allows individuals to inspect or obtain a copy of their PHI, or have it sent to a third party. Additionally, unless an exception applies, the Privacy Rule prohibits covered entities from disclosing an individual's PHI to third parties, unless all personal identifiers have been removed. The Privacy Rule establishes other individual rights, including the right to receive a notice of privacy practices, the right to request amendments to PHI, and the right to request restrictions on the use and disclosure of PHI.

B. The Security Rule

Under the Security Rule, covered entities must implement certain administrative, physical, and technical safeguards (and have written policies and procedures) to protect electronic PHI. These safeguards include the following:

Administrative Safeguards:

- Implement specific security measures to protect electronic PHI.
- Designate security personnel to uphold security measures.
- Limit the use and disclosure of electronic PHI to the minimum amount necessary.
- Provide proper training to employees regarding the handling of electronic PHI and all security measures that have been put in place.
- Perform periodic assessments of security measures.

Physical Safeguards:

- Limit physical access to facilities and devices, while ensuring that individuals who are authorized to access electronic PHI are able to do so without issue.

Technological Safeguards:

- Implement device security procedures to ensure electronic PHI is not readily accessible to those who are unauthorized to access it.
- Implement technical security measures to record and examine access to electronic PHI and ensure that PHI is not improperly altered or destroyed.

C. The Breach Notification Rule

Under the Breach Notification Rule, covered entities must provide certain notifications when a breach of unsecured PHI occurs. The Rule defines "breach" as an impermissible use or disclosure of PHI that compromises the privacy of the PHI. An impermissible use or disclosure is presumed to be a breach unless the covered entity can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment.

When the covered entity determines that a breach has occurred, it must notify each affected individual of the breach. It must also notify HHS, and if the breach impacted more than 500 individuals, it must notify local media as well. The Rule provides the required content and deadlines for these notifications.

The Bottom Line

Some 501(c)(3) public charities are HIPAA covered entities or business associates and are therefore bound by HIPAA's Privacy, Security, and Breach Notification Rules. Those organizations that do not qualify as HIPAA covered entities or business associates should still implement privacy and security safeguards to protect their clients' and employees' sensitive information. Additionally, it is important for nonprofits to consider applicable state laws when implementing privacy and security standards. Nonprofits that possess health information or other sensitive personally identifiable information should confer with legal counsel to determine which laws apply and how the organizations can achieve and maintain full compliance with those laws.

Need Legal Advice?

If you are a PBPO client and have questions regarding the content of this article or need legal assistance, please contact us at info@pbpohio.org or (513) 977-0304.

Not a Client? Apply to become a client by submitting a Request for Legal Assistance online, or contact us at info@pbpohio.org.

About the Authors:

Chris Bennington is a Member of the Firm of Epstein Becker and Green PC. He represents managed care organizations and hospitals, and is an expert in HIPAA, the FCA, and the Health Information Technology for Economic and Clinical Health Act.

Bailey Cremeans is a 2024 graduate of The Ohio State University Moritz College of Law. She was a summer associate at Epstein Becker and Green PC and will be joining the firm as an associate later in 2024.