BDO USA

ARTICLE

June 20, 2024

BY:

Sophie Luu
Senior Manager, Privacy and Data Protection

Spencer Togia
Senior Associate, Privacy and Data Protection

U.S. Federal Privacy Landscape for Nonprofit Organizations: HIPAA

Introduction

The U.S. federal privacy landscape for nonprofit organizations (NPOs) consists of sectoral laws and regulations that apply to specific public and private uses of personal data. One of the federal bills that was signed into law in 1996 is the Health Insurance Portability and Accountability Act (HIPAA). This federal law required the creation of national standards that address the use and disclosure of

protected health information (PHI). The U.S. Department of Health and Human Services (HHS) implemented the Standards for Privacy of Individually Identifiable Health Information (Privacy Rule) that may impact NPOs.

HIPAA Privacy Rule

The privacy rule provides the most definitive privacy rights to individuals as it relates to their PHI. NPOs that process PHI must be aware of their obligations under the HIPAA privacy rule. PHI must be individually identifiable, which means that the information identifies the individual or there is a reasonable basis to believe that it can be used to identify the individual. Under HIPAA, qualifying NPOs have a series of obligations to inform, protect and otherwise use PHI only for limited purposes. NPOs that function as health plans, healthcare clearinghouses, or a healthcare provider who transmit health information electronically in connection with certain transactions would be considered “covered entities” and must adhere to these obligations. Business associates, or a person or organization that performs certain functions or activities on behalf of a covered entity, are also subject to the privacy and protection requirements of PHI under contractual requirements. NPOs should evaluate their organization against these definitions to determine their specific obligations.

The focus of this article is on covered entity obligations, which include the annual completion of five audits that assess the NPOs’ adherence to the privacy and security standards established by HIPAA. Obligations also consist of any remediation plans associated with the results of those audits. Remediation can include the development of policies and procedures that specifically support an NPO’s overall privacy and security program. In particular, the areas of employee training and awareness as well as incident response should be prioritized to develop a culture of compliance and preparedness.

Obligations also include a series of individual rights that organizations are required to provide. Individuals are afforded the following rights:

- **Notice of Privacy Practices:** Covered entities are to provide a notice to individuals that includes, among other things, the way PHI may be used or disclosed as well as a point of contact for any privacy complaints.
- **Access to PHI:** Individuals have the right to review and obtain a copy of their PHI retained

by a covered entity. While exceptions do exist to prevent harm to the individual, this right must be afforded without undue delay.

- **Disclosure of Accounting:** Individuals have the right to know of any disclosures of their PHI by a covered entity or their business associates.
- **Amendment:** Individuals have the right to request changes to their PHI when that information is inaccurate or incomplete. The covered entity can deny the request based on the details of the request but must provide a written denial notification to the individual explaining the denial.
- **Restriction:** Individuals have the right to request that a covered entity restrict the use or disclosure of their PHI for treatment, payment or notification of family.
- **Confidential Communications:** Individuals may request an alternative means or location for receiving communications of PHI. Reasonable accommodations must be met if the individual disclosed that the current disclosure method could endanger the individual.

Privacy Rule Enforcement

HHS' Office for Civil Rights (OCR) is responsible for enforcing the HIPAA privacy and security rules. The OCR enforcement process consists of complaint investigations, compliance reviews, and education and outreach.

OCR reviews all complaints that it receives and may take action only when the following conditions are met:

- The alleged action occurred in the past six years.
- The complaint is filed against an entity required to comply with the HIPAA rules.
- The complaint alleges activity that, if proven true, would violate the HIPAA rules.
- The complaint must be filed within 180 days of when the person submitting the complaint knew or should have known about the alleged violation.

When OCR investigates complaints, it will traditionally close the case under one of the following

categories:

- **Resolved after intake and review (no investigation):** OCR determined a lack of jurisdiction, or the case does not warrant investigation for reasons such as the alleged organization not qualifying as a covered entity or business associate, or the behavior implicated is not covered under the HIPAA rules.
- **Technical Assistance (no investigation):** OCR provides technical assistance to the organization through early intervention.
- **No Violation (investigated):** Following an investigation, OCR does not find any violations of the HIPAA rules.
- **Corrective Action (investigated):** OCR investigates and either provides technical assistance or requires the organization to make changes regarding privacy and security policies, procedures, training or safeguards as they relate to the HIPAA privacy and security rules.
- **Other:** OCR does not continue with an investigation if (a) the case is referred to the Department of Justice, (b) the case involved a natural disaster, (c) it was managed by state authorities, or (d) the organization has taken steps to comply with the rules and OCR determines resources are better deployed elsewhere.

The Federal Trade Commission (FTC) can also be involved in the enforcement of the privacy rule for NPOs that process health information if they are misleading individuals as to the use of that information. Misleading individuals also means that the processing of health data cannot cause more harm than good. This is under the FTC Act's obligations for organizations that collect, use or share health information that are not required to comply with HIPAA.

Conclusion

NPOs should be aware of their current and potential HIPAA obligations. Under HIPAA, NPOs are considered covered entities if they function as health plans, healthcare clearinghouses or a healthcare provider who transmits health information electronically in connection with certain transactions. NPOs, who perform certain function or activities on behalf of a covered entity, are also subject to the privacy and protection requirements of PHI under contractual requirements.

Understanding the current HIPAA obligations can provide NPOs the knowledge necessary to plan and prepare for HIPAA compliance. Partnering with BDO to assess gaps, generate a HIPAA program maturity roadmap and implement the necessary changes, can sustainably benefit both the short- and long-term goals of the organization.

Have Questions? Contact Us