OCR Releases Report of Second Phase HIPAA Audit Findings

Issue Date: March 17, 2021

Introduction

Late last year, the Office for Civil Rights (OCR) released its findings from the series of HIPAA privacy and security audits it conducted of approximately 200 covered entities and business associates in 2016 and 2017. OCR is the division of the Department of Health and Human Services (HHS) responsible for overseeing and enforcing compliance with HIPAA's requirements. The purpose of the report is to describe OCR's findings and recommend assistance for covered entities and business associates in areas where deficiencies were common.

Background

In 2009, the Health Information for Clinical and Economic Health Act (HITECH) was passed as part of the American Reinvestment and Recovery Act (ARRA). HITECH made a number of substantive changes to HIPAA's privacy and security requirements and introduced detailed new breach reporting requirements. As part of this legislative overhaul, OCR was put in charge of HIPAA compliance and oversight and was tasked with conducting a series of compliance audits of covered entities and business associates. It undertook its first phase of audits in 2012. This series of audits consisted mainly of onsite audits for a small number of covered entities. In 2016/2017, OCR broadened its pool of subjects to include business associates and focused mainly on desk audits using a comprehensive audit protocol to assess compliance with various requirements.

Findings

The 2016/2017 audits focused on key provisions within the following areas: 1) notice of privacy practices (NPP); 2) breach handling; 3) individual access to protected health information (PHI) requests; and 4) security risk management efforts.

In general, OCR found that entities complied with some key requirements (i.e., providing a Notice of Privacy Practices and making timely breach notifications), but observed prevalent non-compliance in more complex areas, including in the content of the NPP and breach notifications; responding to individual rights requests; and conducting the required HIPAA security risk analysis and implementing a corresponding risk management program. Below is a more detailed discussion of the areas reviewed and of OCR's findings and recommendations for enhanced compliance.

<u>Notice of Privacy Practices (NPP)</u>

Requirement: Health plans and providers must develop and distribute an NPP that provides a plain language explanation of individuals' rights with respect to their PHI and the privacy practices of the health plan or provider providing the NPP.

Audit Findings: Generally, OCR found that, although covered entities and business associates provided a Notice of Privacy Practices (NPP), the notice was missing certain required elements. For example, many notices failed to provide sufficient information concerning the entity's uses and disclosures of PHI, including examples of how an individual's PHI might be used or disclosed. NPPs also often failed to include a sufficient description of an individual's rights with respect to their own PHI (e.g., right to access PHI, right to amend PHI, etc.) and information about how these rights can be exercised. OCR encourages covered entities and business associates to review the model notices available on OCR's website to ensure that all required elements are included in their NPP.

Electronic Provision of NPP

Requirement: If a covered entity maintains a website that provides information about the entity's customer service or benefits, then it must prominently post its NPP and make it available electronically through that website.

Audit Findings: Covered Entities that failed to meet this standard generally did so because they failed to prominently post the NPP – e.g., they posted it on a page other than, and/or not directly accessible from, the homepage. Examples of non-prominent posting included:

- Maintaining two links with the same title (e.g. "Privacy Policy") on the homepage that connect to two different privacy guidelines, one of which was the NPP.
- Posting NPPs that appear to be provided on behalf of different covered entities.
- Having non-functional links to the NPP that resulted in an error message.

Covered Entities with webpages about their health plan benefits/customer service should review the site to ensure that the NPP is prominently posted and identifiable and that any links are correct/functioning.

Individual Access to PHI

Requirement: Covered entities must provide individuals who request it access to their PHI that the covered entity maintains in a "designated record set." Access may include inspecting or obtaining a copy of records. Individuals may also direct a covered entity to transmit electronic PHI maintained in an electronic health record to a third party.

Audit Findings: Almost all covered entities audited failed to fully comply with the individual right of access requirement. Specifically, covered entities:

- Failed to document such requests, sometimes mistakenly believing they had not received a request;
- Failed to abide by the 30-day response time frame required by the privacy rules (sometimes incorrectly believing they had 60 days);
- Failed to develop or implement internal policies and procedures for receiving and accurately responding to access requests;
- Implemented incorrect policies for access requests (e.g., requiring a signed Authorization form before releasing an individual's records to them);
- Incorrectly denied certain access requests;
- Limited the formats in which an individual could request that their records be provided (e.g., to fax or email); and/or
- Failed to provide a clear, reasonable cost-based fee for provision of records.

OCR recommends that covered entities review available resources, such as OCR's audit protocol, to review the requirements and ensure that they have a compliant process in place.

Breach Notification Response Time Frame

Requirement: HIPAA requires covered entities and business associates to provide certain notifications when there has been a breach (i.e., an acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule that compromises the security or privacy of the PHI) of unsecured PHI. Specifically, entities must provide notification to affected individuals (within 60 days), HHS, and in some cases, the media. Business Associates must provide notification to the covered entity if the business associate experiences a breach.

Audit Findings: The majority of audited covered entities issued notices to individuals within the regulatory time frame. Entities should review breach notification requirements and ensure that they have policies and procedures in place to make timely notifications.

Content of Breach Notification

Requirement: Breach notifications to individuals must be written in plain language and include certain required elements, such as a description of the breach (including the date of the breach and date of discovery, if known); a description of the types of information involved in the breach; the steps an individual should take to protect themselves against potential harm; a brief description of what the covered entity is doing to investigate the breach and mitigate the harm/prevent further breaches; and contact information.

Audit Findings: Most breach notification letters were missing required information. Examples of deficiencies included:

- A lack of a description of the type of PHI involved in the breach;
- Failure to outline the steps the individuals should take to protect themselves;
- Failure to include a meaningful explanation of the covered entity's investigation and mitigation activities; and
- Incorrect contact information.

Many entities also failed to keep adequate documentation of notification letters sent.

Covered entities must ensure that all staff are properly trained on requirements that notification letters contain all the provisions outlined in the regulation and that they establish procedures to properly document and keep affected individuals informed.

Notification of Breach by Business Associate to Covered Entity

Requirement: The Breach Notification Rule requires that business associates notify covered entities within the time frame set forth in the business associate agreement, but in no case more than 60 days after the breach is discovered. Whenever possible, notifications must identify each individual affected and include any other available information required for notification to individuals. Although a covered entity ultimately maintains the obligation to notify, it may delegate such responsibility to a business associate.

Audit Findings: Generally, business associates failed to include required information in their notifications, which impeded the covered entity's ability to meet their own notification obligations. Information most often missing included identifies of individuals, a description of information involved in the breach, and information about steps the individual should take to protect themselves from potential harm. In some cases, business associates failed to keep records indicating that they had made notifications within the required time frames.

HIPAA Security Risk Analysis

*Requirement***:** Covered entities and business associates must conduct security risk analyses to assess the potential risks to, and vulnerabilities of, the confidentiality, integrity, and availability of ePHI held by the entity.

Audit Findings: Many covered entities and business associates are failing to adequately safeguard their ePHI and to conduct thorough risk analyses. Entities generally failed to:

- Identify and assess risks to their ePHI;
- Identify threats and vulnerabilities, consider potential likelihoods and impacts, and rate the total risk to ePHI; and

- Review and periodically update the risk analysis in response to changes in the environment/systems/operations.

Entities often assumed that purchasing a security product was sufficient to reduce risks to an acceptable level without also conducting the required security risk analysis. OCR emphases that entities must understand and comply with the risk analysis requirement to appropriately safeguard ePHI, and points to many available online tools to assist entities with this effort (including OCR's own risk analysis tool).

HIPAA Security Risk Management

Requirement: Entities must implement security measures sufficient to reduce risks and vulnerabilities identified in the risk analysis to a reasonable and appropriate level.

Audit Findings: Because many entities failed to conduct adequate security risk analyses, they were similarly unable to implement meaningful risk management programs. However, some entities did conduct security risk analyses and then failed to take any further action to address identified risks/vulnerabilities. In some cases, entities provided risk analyses that were conducted to comply with other security standards and did not sufficiently account for ePHI. And some entities had completed adequate risk analyses at one point, but failed to update them/continue to account for risks over time.

Conclusion

The report does not yield any major surprises to anyone who has paid attention to the types of settlements that have been reached over the past few years, but it is helpful to see OCR's findings disseminated and explained for purposes of understanding what issues OCR is paying attention to and considers important from a compliance perspective. Covered entities and business associates should take this opportunity to review the audit protocol OCR used to identify the areas of focus, and should review existing policies and procedures to ensure that they adequately address the requirements of the privacy, security, and breach notification rules.

OCR 2016-2017 HIPAA Audits Industry Report: https://www.hhs.gov/sites/default/files/hipaa-audits-industry-report.pdf

OCR Comprehensive Audit Protocol: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html