Bloomberg BNA

Health IT Law & Industry Report™

VOL. 6, NO. 18 MAY 5, 2014

Future OCR Audits Have Little in Common With Previous Round—Here's How to Prepare

By Adam H. Greene and Rebecca L. Williams

Greene is a partner in the Washington office of Davis Wright Tremaine LLP. He counsels health care systems and technology companies on compliance with HIPAA privacy, security and breach notification requirements. Greene formerly worked for the Department of Health and Human Services Office for Civil Rights. He can be reached at adamgreene@dwt.com.

Williams is a partner in the Seattle office of Davis Wright Tremaine LLP. She is a registered nurse and chair of the firm's Health Information Technology/HIPAA Practice Group. She counsels clients on health care privacy and security. She can be reached at beckywilliams@dwt.com.

The Department of Health and Human Services Office for Civil Rights (OCR) recently presented information about the new look of its Phase 2 audit program (click here for slides from the Health Care Compliance Association's 2014 Compliance Institute). The new audits will look little like the old ones, with OCR conducting the audits itself and focusing on more high-risk areas, doing away with on-site visits (at least for the moment), and potentially integrating the audits into OCR's formal enforcement program.

To prepare for the next round of audits, which we describe below in more detail, we suggest that covered entities and business associates consider the following steps:

- Ensure that a current risk analysis is in place and that the risk analysis actually identifies and categorizes risks (e.g., low, medium, high) rather than merely documenting that controls are in place or documenting the gaps in compliance with the Security Rule (see OCR

Guidance on Risk Analysis and HHS' recently released Security Risk Assessment Tool (applicable to both covered entities and business associates)

- Verify that policies are up to date and dated, particularly pertaining to:
  - breach notification, risk analysis, and risk management (applicable to both covered entities and business associates)
  - notice of privacy practices and patient/enrollee access (only applicable to covered entities)
- Have supplemental documentation related to the above topics readily available and relatively self-explanatory (e.g., clearly labeled) such as:
  - breach investigations and risk assessments, risk analyses, and risk management plans (for both covered entities and business associates)
  - responses to patient requests (for covered entities)
- Know how to readily collect documentation of patient acknowledgments of receipt of the notice of privacy practices and, where there is no patient acknowledgment, documentation supporting the reason why an acknowledgement was not obtained (only applicable to covered entities)
- Maintain a current list of business associates with relevant contact information. An internal audit of accounts payable may help identify business associates and is a methodology that was used by OCR's contractors in phase 1 audits to identify business associates (only applicable to covered entities)

How Phase 2 Audits Will Be Different

While Phase 1 of OCR's audit program was conducted by contractors between 2011 and 2012, Phase 2 will be conducted primarily by OCR staff. This likely will require significant training of OCR staff, as auditing involves a somewhat different methodology than the investigations that OCR currently conducts.

OCR plans to audit 350 covered entities (including 100 health care providers, 45 health plans, and five health care clearinghouses) and 50 business associates (including 35 IT-related business associates and 15 non-IT related business associates).

In spring 2014, OCR will confirm email addresses for a pool of covered entities, with future contact coming through the confirmed email addresses. OCR learned in Phase 1 that without sufficient address confirmation, a hard copy audit notification could languish for weeks.

In summer 2014, OCR will collect relevant information from 550 to 800 covered entities to obtain information necessary for selecting an appropriate sample. OCR will follow up in fall 2014 with notifications and data requests to 350 covered entities.

Phase 2 audits will be more narrowly focused than the comprehensive audits in Phase 1. Phase 2 topics are based on deficiencies identified in Phase 1. OCR will audit 100 covered entities on the Privacy Rule, focusing on compliance with requirements related to the notice of privacy practices and patient access to protected health information.

While additional details are not available at this time, data requests could include:

- a policy on provision of the notice of privacy practices;
- documentation of individuals' acknowledgment of receipt of the notice or of the covered entity's effort to obtain the acknowledgment;
- a copy of the notice;
- a policy on providing individuals with access to protected health information and addressing any denials of access (including appeal rights); and
- documentation of responses to individuals' requests for access.

OCR will audit 100 covered entities on breach notification, including content and timeliness of notifications. Additional details are not available at this time; however, data requests could include:

- a policy on breach notification;
- a copy of recent breach notifications;
- a copy of any breach risk assessments where notifications were not made;
- documentation of the timelines from the discovery of a breach until the notifications of the breach were made; and
- documentation of investigations relating to breaches.

OCR will audit 150 covered entities on security. This will focus on risk analysis and a

For the first time, business associates also will be included in OCR audits. OCR will request a list of business associates from covered entities.

It appears that OCR will request a list of business associates from the 350 covered entities that are selected for audit, but it remains possible that OCR will request the information from the larger pool of covered entities that are initially surveyed (e.g., perhaps the 550 to 800 covered entities to be contacted during the summer).

OCR then will audit 50 business associates in 2015. The business associate audits will focus on breach notification to covered entities and risk analysis and risk management. Although we do not have additional details, data requests to business associates could include:

- a policy on breach notification;
- a copy of recent breach notifications to covered entities;
- a copy of any breach risk assessments where full breach notifications were not made;
- documentation of investigations and timing related to breach notification;
- a copy of a current risk analysis; and
- a corresponding risk management plan.

Projected ''round 2'' of Phase 2 audits and those conducted in 2016 and beyond may move to device and media controls, transmission security (e.g., encryption of transmitted PHI), Privacy Rule safeguards (e.g., governing hard copy and verbal information), encryption and decryption, physical facility access controls, breach reports (e.g., to OCR), and complaint processes.

Covered entities and business associates will have two weeks to respond to initial data requests, which will be narrower than those of Phase 1. OCR has indicated that auditors will not seek clarification or additional data and only data submitted on time will be considered. OCR discourages submitting extraneous information. OCR will not consider documentation dated after the audit request. OCR will provide a draft report to audited entities and provide an opportunity for comment prior to a final report.

Unlike Phase 1, OCR does not intend for Phase 2 audits to include on-site visits. OCR may return to on-site audits in the future if additional funds become available.

While OCR's messaging surrounding Phase 1 audits was that they would not be used as a vehicle for formal enforcement, OCR has indicated that Phase 2 and future audits may be more closely tied to enforcement, where adverse findings could lead to civil monetary penalties or a resolution agreement. However OCR leadership is likely to change soon, which may significantly impact how the audit program ties to enforcement.

This describes OCR's most recent information on its audit program. The information, especially dates, is subject to significant change as OCR rolls out Phase 2.