THOMAS D. BIXBY
LAW OFFICE LLC
LEGAL ADVICE FOR HEALTH PLANS

PRIVACY LAW ALERT
March 22, 2016

OCR Announces Phase 2 HIPAA Audits

Every Covered Entity and Business Associate is Eligible for an Audit

The Office for Civil Rights (OCR) announced yesterday that it has begun to collect information on covered entities and business associates that will be subject to audit in Phase 2 of its HIPAA Audit Program. OCR, which is the agency tasked by the Department of Health and Human Services to enforce the HIPAA Privacy, Security, and Breach Notification Rules, will "obtain and verify contact information to identify covered entities and business associates of various types [to] determine which are appropriate to be included in potential auditee pools." But, the agency stresses that "[e]very covered entity and business associate is eligible for an audit."[1] Even an "entity that does not respond to OCR [e-mails] may . . . be selected for an audit or subject to a compliance review," because the agency "will use publically available information about the entity to create its audit pool" when necessary.

OCR Expectation: Junk Mail Checking. The OCR is in the process of sending e-mails to covered entities and business associates requesting contact information for purposes of creating audit pools. The agency warns covered entities and business associates to be aware that its e-mails could be classified as spam and that the agency "expect[s] you to check your junk or spam email folder for emails from OCR: OSOCRAudit@hhs.gov."

Pre-Audit Screening Questionnaire—List of Business Associates. According to the OCR announcement (available here), after the agency collects contact information from entities, it will send "pre-audit screening questionnaires" "designed to gather data about the size, types, and operations of potential auditees." Questionnaires for covered entities will request a list of business associates and OCR "encourage[s] covered entities to prepare a list of each business associate with contact information so that [the covered entities] are able to respond to this request."

[1] In phase 1 of the HIPAA Audit Program, "OCR audited as wide a range of types and sizes of covered entities as possible; covered individual and organizational providers of health services, health plans of all sizes and functions, and health care clearinghouses could all be considered for an audit." Similarly, in Phase 2, OCR intends to look at "a broad spectrum of audit candidates" based on sampling criteria such as size, type, and present enforcement activity. The sampling criteria are designed to ensure that "OCR can better assess HIPAA compliance across the industry," rather than to focus on (for example) only large covered entities or business associates.

Nature of Audits. Initially, OCR will conduct desk audits only of covered entities. Later it will conduct desk audits of business associates. The desk "audits will examine compliance with specific requirements of the Privacy, Security, or Breach Notification Rules and auditees will be notified of the subject(s) of their audit in a document request letter." Thus, it appears as though—in at least some cases—desk audits will cover targeted HIPAA requirements, rather than all HIPAA requirements.

Once the desk audits are completed—which should be by the end of 2016—the agency will begin a series of onsite audits to "examine a broader scope of requirements from the HIPAA Rules than desk audits." Although entities subject to desk audits may also be subject to the more-intensive on-site audits, "OCR will not audit entities with an open complaint investigation or that are currently undergoing a compliance review."

The OCR explains that the "audits present an opportunity to examine mechanisms for compliance, identify best practices, discover risks and vulnerabilities that may not have come to light through OCR's ongoing complaint investigations and compliance reviews, and enable us to get out in front of problems before they result in breaches. OCR will broadly identify best practices gleaned through the audit process and will provide guidance targeted to identified compliance challenges."

Although OCR does not plan to post a list of audited entities or identifiable findings of the audits, it emphasizes that the audits may be subject to the Freedom of Information Act and could therefore become available to the public.

* * * * * * * * * *

For more information, please contact Tom Bixby at (608) 661-4310 or
TBixby@tbixbylaw.com