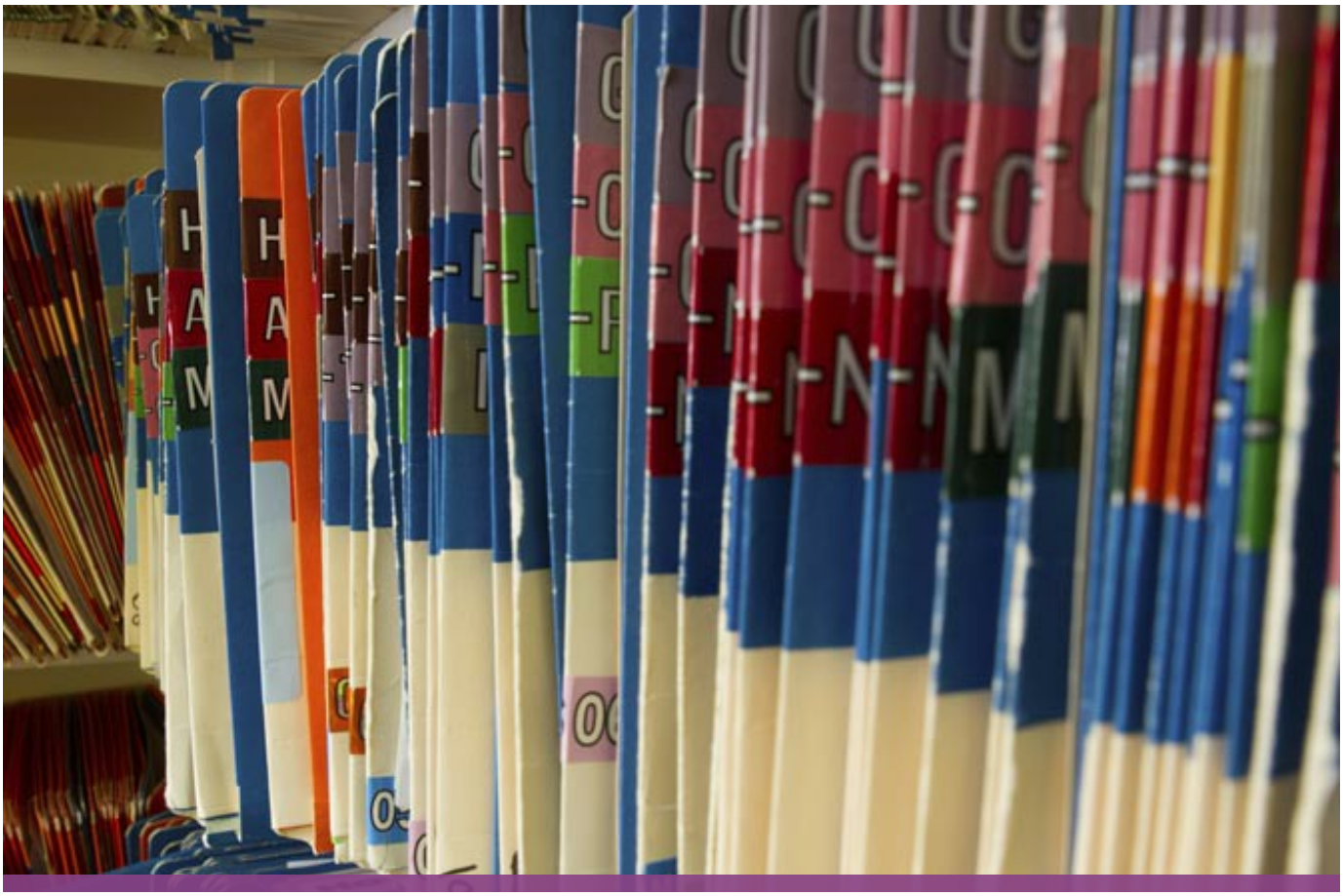
Phase 2 HIPAA audits are coming



Emily A. Johnson, James J. Giszczak, Rick L. Hindmand, Dominic A. Paluzzi | Monday, March 28, 2016

The Department of Health and Human Services (HHS) recently announced that the Office for Civil Rights (OCR) started Phase 2 of its audits of covered entities and business associates. This initiative is part of OCR's efforts to assess compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security and Breach Notification Rules. OCR uses the data it obtains during the audit process to examine compliance mechanisms, determine best practices, and discover program risks and vulnerabilities. Phase 1 took place in 2011 and 2012, during which OCR assessed the systems used by 115 covered entities to maintain compliance with HIPAA requirements.

Phase 2

Unlike Phase 1, in Phase 2 the audits will not be limited to covered entities, so business associates can find themselves subject to an audit. OCR is in the process of identifying covered entities and business associates to include in its audit pools, and requests for information are being sent to verify contact information in preparation for sending audit selection letters.

Phase 2 will consist of three rounds of desk and on-site audits. The first round of audits will be desk audits of covered entities, the second round will be desk audits of business associates, and the third round of audits will be on-site audits that focus on a broader scope of HIPAA requirements than the desk audits. Selection for the first or second round of desk audits does not preclude selection for the onsite audits conducted during the third round, so some entities may be subject to both desk and on-site audits.

Audit selection

Any covered entity or business associate can be audited, regardless of size or type of provider. Recent enforcement activities have shown that OCR is actively investigating smaller providers and is no longer focusing its efforts on large covered entities such as hospitals or health systems. Audit selection criteria includes the size of the entity, type of entity, affiliation with other healthcare organizations, whether the entity is public or private, and geographic factors. The only entities that are exempt from an audit are those entities with an open complaint investigation or ones that are currently the subject of a compliance review.

OCR will notify (via email) covered entities and business associates that are selected for an audit. It is expected that covered entities and business associates regularly monitor their email and spam folders so that communications from OCR are not missed. If an entity does not respond to a request for information from OCR, it can still be subject to an audit, or even worse, a compliance review.

Upon notification that it has been selected for a desk audit, a covered entity or business associate has 10 business days to submit the initial documentation requested by OCR via OCR's secure online portal. Once OCR receives the documents, the assigned auditor will review the information and send the audited entity its draft

findings. Upon receipt of the draft audit findings, the entity is given 10 business days to review and provide a written response to the auditor's comments. The auditor will then prepare a final audit report within 30 business days of a written response from the entity, and the audited entity will be provided with a copy of such report.

Covered entities and business associates will be notified of their selection for an on-site audit in the same manner as selection for a desk audit – via email. Prior to coming onsite, the auditors will schedule an entrance call to discuss the audit process and expectations. The onsite audit will take place over three to five days, depending on the complexity of the entity. All other elements of an on-site audit remain the same as desk audits, including the timeframe for submitting initial document requests, the timeframe for responding to an auditor's draft findings, and the timeframe that the auditor has to complete its final audit report.

The time to prepare is NOW

It is imperative that covered entities and business associates evaluate their compliance with HIPAA requirements now. Do not wait until you are selected for an audit. Unless currently subject to an investigation or a compliance review, no covered entity or business associate is exempt from audit selection. Although the goal of the audit program is to identify best practices, if serious compliance issues are found OCR can initiate a compliance review to further investigate. Covered entities and business associates should conduct a thorough review of their HIPAA policies and procedures, confirm that those policies and procedures have actually been implemented, and assess their effectiveness. Keep in mind that the requested documents will need to be submitted electronically within 10 business days, and so should be available in electronic form if feasible. See our previous alert on preparing for HIPAA audits for additional action steps.

Although OCR audits are limited to federal HIPAA requirements, many states have their own requirements for protecting health and medical information as well as other categories of personally identifiable information. In the event of a data privacy incident or breach, covered entities and business associates must also comply a multitude of state law requirements. For this reason, it is critical that entities review applicable state privacy laws and ensure that their HIPAA compliance programs comply with all applicable health privacy laws, including state and federal.

Even if not selected for an audit, ensuring that your organization has a working and trusted HIPAA compliance program will benefit your organization and reduce the likelihood of investigations, complaints, security incidents, and significant time and money spent responding to such issues.

For more information, please contact one of the attorneys listed below.

Emily A. Johnson

James J. Giszczak

Rick L. Hindmand

Dominic A. Paluzzi