OCR Launches Phase 2 HIPAA Audits

On July 11, 2016, the U.S. Department of Health and Human Services ("HHS") Office for Civil Rights ("OCR") notified 167 covered entities of their selection for Phase 2 desk audits. The audits will examine compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy, Security, and Breach Notification Rules. Under the Health Information Technology for Economic and Clinical Health Act ("HITECH"), HHS is required to conduct periodic audits of covered entities and business associates for compliance with these rules. According to OCR, these audits present an opportunity for it to review mechanisms for compliance, identify best practices for protecting health information, and better target the technical assistance it provides. For industry, the audits reflect continuing focus by the government on testing organizations' HIPAA compliance.

These are not the first large-scale HIPAA audits conducted by OCR. In 2011, OCR conducted an Audit Pilot Phase. That was followed in 2012 by Phase 1 audits. The Phase 2 audits are, however, the first wave following OCR's issuance of the 2013 Final Rule. This Alert describes the audit process, the audit scope, and what the audits mean for the industry—including those who have been selected, and those who have not.

The Audit Process

The first round of Phase 2 desk audits includes only covered entities (health plans, health care providers, and health care clearinghouses), not business associates. The audits began with pre-audit letters that OCR sent to a larger group of covered entities in May 2016. The letters were followed by a pre-audit questionnaire, which recipients had 30 days to complete. Entities that failed to respond remain subject to audits. OCR will rely on publicly available information—which, of course, may be incomplete, exposing a non-responding entity to risk of false conclusions—if it cannot obtain information from the entity directly.

Through the pre-audit questionnaire, OCR gathered data about the type, size, and operations of each entity. OCR used that information to create a pool for selecting the 2016 audit subjects. After excluding entities with an open OCR investigation or undergoing a compliance review, OCR chose audit subjects through random sampling. On July 11, 2016, by e-mail, OCR notified entities of their selection, and provided instructions for their responses. OCR followed this with a second e-mail requesting a list of each entity's business associates.

In the fall, OCR will begin the second round of Phase 2 audits, focusing on business associates. This round also will be conducted as desk audits, and is expected to be completed by the end of the year.

The third round of audits will involve more comprehensive on-site reviews. OCR will notify selected entities of their selection by e-mail. Those audits will begin with entrance conferences to discuss the on-site audit process and expectations. Each on-site audit is expected to last between three and five days.

Audit Scope

In the desk audits, OCR will examine each entity's documentation to support HIPAA compliance. OCR will focus on areas it has indicated present frequent or significant noncompliance. Those include:[1]

- Privacy Rule
  1. Notice of Privacy Practices and Content Requirements (§ 164.520(a)(1), (b)(1))

[1] The full audit protocol, which contains criteria used by the OCR auditors, is available here.

2. Provision of Notice – Electronic Notice (§ 164.520(c)(3))

3. Right to Access (§ 164.524(a)(1), (b)(1-2), (c)(2-4), (d)(1, 3))

- Security Rule
  1. Security Management Process – Risk Analysis (§ 164.308(a)(1)(ii)(A))

  2. Security Management Process – Risk Management (§ 164.308(a)(1)(ii)(B))

- Breach Notification Rule
  1. Timeliness of Notification (§ 164.404(b))

  2. Content of Notification (§ 164.404(c)(1))

OCR has not identified the focal areas for the business associate desk audits. For business associates, the Privacy Rule regulations described above obviously would be less relevant. However, the Security Rule standards, including the Security Management Process, may remain within scope.

Although the main purpose of the OCR Audit Program is assessment, not enforcement, OCR may initiate a separate compliance review for further investigation if an audit reveals serious compliance issues or lack of cooperation. Such an investigation may be significantly broader than the desk audit.

What the Audits Mean for Industry

Phase 2 audits have obvious significance for covered entities that already have been selected, as well as for business associates selected in the months ahead. They also provide lessons for the industry as whole. Five take-away points follow.

1) Review your current HIPAA risk analysis processes.

Phase 2 audits are expected to look at risk analyses, reflecting OCR's view of their importance. A risk analysis should involve an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of protected health information ("PHI"). No single optimal plan guarantees compliance—risk analysis processes should account for the unique needs of individual organizations. However, all risk analyses should involve elements such as data collection, identification and documentation of potential vulnerabilities, and determination of the likelihood and impact of threat occurrence.

2) Review your policies and procedures to ensure compliance with the Breach Notification Rule.

Phase 2 audits also are expected to look at compliance with the Breach Notification Rule. Covered entities should ensure that the unsecured PHI in their possession is adequately safeguarded, and notify the appropriate parties if a breach is discovered. A breach occurs when PHI is used, acquired, accessed, or disclosed in an impermissible manner that compromises the security or privacy of the PHI. In the event of a breach of unsecured PHI, covered entities and their business associates should have policies in place to notify the affected individuals and HHS. If the breach affects more than 500 residents of a state, the covered entity also must notify the media. Of course, business associates who discover a breach must notify the covered entity and comply with any additional notification and other contractual obligations it may have to the covered entity.

3) Account for your business associates and review your contracts.

As part of the Phase 2 audits, OCR required covered entities to submit detailed information regarding their business associates. A business associate generally is a person or entity that performs certain functions or activities involving the use or disclosure of PHI, on behalf of or in service to a covered entity. Covered entities should ensure that their business associate agreements comply with HIPAA requirements to adequately protect PHI.

4) Ensure that your entity has appropriate security safeguards in place.

The HIPAA Privacy and Security Rules require covered entities to have administrative, physical, and technical safeguards in place to protect PHI. *Administrative* safeguards include policies and procedures to manage security measures and the conduct of the entity's workforce. *Physical* safeguards are the physical measures put in place to safeguard PHI, such as controlled access to the facility in which health information is stored and policies that specify proper use of workstations. *Technical* safeguards are measures addressing the use of technology to protect and control access to PHI, such as encrypting data or assigning a unique user identifier to track specific users' activity when logged on to an information system.

Security safeguards should be dynamic and adapt to changes in the organization and its technologies. Each entity has unique factors that should inform the development of appropriate security safeguards. Some factors to consider are the size, complexity, and capabilities of the entity, the entity's technical infrastructure, the costs of security measures, and the probability of potential risks to PHI.

5) Business associates should look for and respond to OCR requests.

Now that OCR has sent the first round of notices to covered entities for Phase 2 audits, we suggest that business associates look for an e-mail from OCR requesting contact information. The e-mail will be sent from OSOCRAudit@hhs.gov and look similar to this sample letter found on the OCR website.

Important Points for Audited Organizations

Some important points for organizations that are or become the subject of an OCR Phase 2 audit are below.

- Monitor receipt of OCR correspondence.
    - Ensure the correspondence is legitimate.
    - Review e-mail "junk mail" folders, as e-mails from the OCR (*i.e.*, OSOCRAudit@hhs.gov) may be incorrectly classified as spam.
- Answer each OCR audit inquiry, including the pre-audit questionnaire, in a concise and direct manner.
- Ensure responses are timely and submissions are in the required format.
    - Complete and submit the pre-audit questionnaire within 30 days.
    - Submit the required audit information within 10 business days.
    - Submit documents in digital form to the OCR address or portal.
- Consider the applicability of the Freedom of Information Act ("FOIA"), as OCR may be required to release audit information to the public upon request.
- Review and provide comments, as applicable, to OCR's draft findings.
    - Audit subjects will have 10 business days to respond to draft findings. Written responses will be included in the final audit report.
    - As such, ensure your organization returns any comments or qualifications to the auditor in writing, keeping a copy for your records.

- Continue to take improvement actions.
    - Although an audit report may indicate a serious compliance issue, and OCR may initiate a compliance review to investigate further, OCR gives significant consideration to corrective action steps.
- Ensure future compliance with the areas and issues identified in the Phase 2 audit.
    - Because the areas and issues identified in an audit are important to OCR, OCR is likely to scrutinize these areas and issues in connection with any future breach report or complaint.

***

For more information, please contact any member of Ropes & Gray's health care practice or visit the Ropes & Gray HIPAA Audits Resource Center, an online HIPAA audit information source offering in-depth resources to help organizations with all aspects of HIPAA audits.