Office of Civil Rights Begins HIPAA Phase 2 Audits

Tuesday, July 19, 2016

What covered entities and business associates can do to prepare for the next round of audits.

On July 11, the HIPAA Phase 2 audits commenced when 167 covered entities[1] received notice of a desk audit from the Department of Health and Human Services Office for Civil Rights (OCR), with responses due by July 22. Covered entities that have not received an audit notification letter can breathe a momentary sigh of relief, but they may still be selected for an onsite audit in early 2017.

HIPAA business associates can use lessons learned from the covered entity desk audits to prepare for the business associate desk audits set to begin this fall.

What Areas Are Being Audited?

OCR announced the launch of the Phase 2 audit program in March 2016 and released updated Phase 2 audit protocols in April 2016. Given the broad scope of the audit protocols, many expected the desk audits to cover a wide range of HIPAA standards. Instead, the Phase 2 desk audits focus on the following areas:

- Privacy Rule—Notice of privacy practices (content requirements, provision of notice, and electronic notice), and patient right of access to protected health information (PHI).
- Breach Notification Rule—Timeliness and content of breach notification.

A complete list of the Phase 2 audit questions is provided below. As expected, the desk audit process focuses primarily on the covered entity’s documentation of its compliance practices and provides little opportunity for explanation or narrative responses. Covered entities must upload the requested documentation to a newly developed OCR portal.

How Will the Audits Work?

The covered entities being audited received two emails from OCR—the first with the audit notification letter providing the audit questions, and the second requesting a list of each covered entity’s business associates. These lists of business associates will be used to select business associates for the second round of the Phase 2 audits scheduled for late September, which will target approximately 33 business associates—marking the first time that business associates have been audited.

The third round of the Phase 2 audits—set to commence in early 2017—will involve up to 50 more comprehensive onsite audits of both covered entities and business associates, bringing the total number of Phase 2 audits to between 200 and 250. Entities subject to desk audits will not be subject to follow-up onsite audits. The subjects of onsite audits will be selected through a random process.

Each entity being audited received either the desk audit questions relating to (i) the HIPAA Privacy and Breach Notification Rules, or (ii) the HIPAA Security Rule—but not both. Some desk audits were addressed to a covered entity’s legal entity, and others were addressed to multiple covered entity facilities affiliated with a covered entity, such as pharmacies in a pharmacy chain.
OCR’s Samuels: “Not a Gotcha Game”

On July 13, OCR conducted a webinar for the covered entities being audited to answer questions about the Phase 2 questionnaire and process. During the webinar, OCR Director Jocelyn Samuels emphasized that the Phase 2 audits are intended to permit OCR to gather information about the state of industry HIPAA compliance in order to develop new compliance tools and guidance documents. “We are not playing a ‘gotcha’ game,” said Samuels during the webinar, “this is not intended to be a punitive process.”

Samuels stated that if OCR sees reasonable, good faith efforts to comply with HIPAA, responses to the Phase 2 audits will not result in enforcement action. However, she added that if “significant threats” to the privacy and security of PHI are identified, OCR may initiate enforcement.

The covered entities being audited were selected by a random, computerized process designed to reflect an even geographic distribution from a list of more than 10,000 covered entities that completed “pre-audit questionnaires.” The covered entities being audited include hospitals, medical practices, elder care/skilled nursing facilities, health systems, and pharmacies.

OCR will review the desk audit documentation submitted by an audited entity and develop a report of draft findings for that entity. The covered entity will then have 10 business days to provide responses to the auditor’s findings. Those responses will be included in a final report, which will be provided to the audited entity. OCR will not post the final reports or a list of the audited entities, but the agency acknowledges that information may be discoverable pursuant to a Freedom of Information Act (FOIA) request. During the webinar, one participant asked if the security risk analyses submitted by audited entities would be subject to FOIA disclosure. OCR Deputy Director of Health Information Privacy Devin McGraw said that she doubted that the risk analyses would be discoverable under FOIA, but the agency would review that issue.

Takeaways for Covered Entities and Business Associates

What are the lessons to be learned for those entities that are not being audited in the first round of the Phase 2 audits? Covered entities should use the list of desk audit questions and the audit protocol as a guide to ensure that their HIPAA compliance efforts are aligned with current OCR areas of focus.

Even if a covered entity was not selected for a Phase 2 desk audit, it may still be subject to an onsite audit if it is in the audit pool that completed the pre-audit questionnaire. It is also important to remember that the Phase 2 audits are intended to be the beginning of a series of ongoing OCR audits utilizing the new portal. As such, even if a covered entity is not selected for audit, OCR may still investigate it as a result of a complaint or security breach, and the areas highlighted in the desk audit questionnaire have also been recurring themes in recent OCR enforcement actions.

HIPAA business associates should review the list of covered entity desk audit questions carefully because it is likely that the business associate desk audit questionnaire will be fairly similar. OCR representatives have previously stated that areas of emphasis for the business associate desk audits will include (i) security risk analysis, (ii) security risk management, and (iii) timely notification to covered entities of breaches. The questions relating to the notice of privacy practices and patient access rights are less applicable to business associates and are unlikely to be included in the business associate desk audit questionnaire. Business associates should consider conducting a mock desk audit to see if they are prepared to produce the documents that are likely to be requested in a Phase 2 desk audit within the required 10-business-day timeframe.

HIPAA Phase 2 Covered Entity Desk Audit Questions

1. Timeliness of Breach Notification. Using sampling methodologies, upload documentation of five breach incidents for the previous calendar year affecting fewer than 500 individuals, documenting the date the covered entity discovered the breach, and the reason, if any, for a delay in notification.

2. Content of Breach Notification.
   1. If the entity uses a standard template or form letter, upload the document.
   2. Using sampling methodologies, upload documentation of five breach incidents affecting 500 or more individuals for the previous calendar year.
   3. Upload a copy of a single written notice sent to affected individuals for each breach incident.

3. Content of Notice of Privacy Practices.
   1. Upload a copy of all notices posted on website and within the facility, as well as the notice
distributed to individuals, in place as of the end of the previous calendar year.

   1. Upload the URL for the entity web site and the URL for the posting of the entity notice, if any.
   2. If the entity provides electronic notice, upload policies and procedures regarding provision of the notice electronically.
   3. Upload documentation of an agreement with the individual to receive the notice via e-mail or other electronic form.

5. Right to Access PHI.
   1. Upload all documentation related to the first five access requests which were granted, and evidence of fulfillment, in the previous calendar year.
   2. Upload all documentation related to the last five access requests for which the entity extended the time for response to the request.
   3. Upload any standard template or form letter required by or used by the CE to document access requests.
   4. Upload the notice of privacy practices.
   5. Upload policies and procedures for individuals to request and obtain access to protected health information.

   1. Upload documentation of current risk analysis results.
   2. Consistent with 164.316(b)(2)(ii)-(iii) [relating to availability and updating of security policies and procedures], upload documentation from the previous calendar year demonstrating that documentation related to the implementation of this implementation specification is available to persons responsible for implementing this implementation specification and that such documentation is periodically reviewed and, if needed, updated.
   3. Consistent with 164.316(b)(2)(i) [relating to retention of security policies and procedures], upload documentation demonstrating that policies and procedures related to the implementation of this implementation specification were in place and in force six (6) years prior to the date of receipt of notification.
   4. Upload policies and procedures regarding the entity’s risk analysis process.
   5. Upload documentation of the current risk analysis and the most recently conducted prior risk analysis.

   1. Upload documentation demonstrating the security measures implemented to reduce risks as a result of the current risk analysis or risk assessment.
   2. Consistent with 164.316(b)(2)(i) [relating to retention of security policies and procedures], upload documentation demonstrating that policies and procedures related to the implementation of this implementation specification were in place and in force six (6) years prior to the date of receipt of notification.
   3. Upload documentation demonstrating the efforts used to manage risks from the previous calendar year.
   4. Upload policies and procedures related to the risk management process.
   5. Upload documentation demonstrating that current and ongoing risks are reviewed and updated.
   6. Consistent with 164.316(b)(2)(ii)-(iii) [relating to availability and updating of security policies and procedures], upload documentation from the previous calendar year demonstrating that documentation related to the implementation of this implementation specification is available to the
persons responsible for implementing this implementation specification and that such documentation is periodically reviewed and, if needed, updated.

[1] HIPAA covered entities include (i) a wide range of healthcare providers that engage in HIPAA standard electronic transactions, (ii) health plans (including HMOs, health insurers, and employer group health plans), and (iii) healthcare clearinghouses. See 45 C.F.R. § 160.103 (definition of “covered entity”).

Copyright © 2019 by Morgan, Lewis & Bockius LLP. All Rights Reserved.

Source URL: https://www.natlawreview.com/article/office-civil-rights-begins-hipaa-phase-2-audits