SATINSKY CONSULTING

FALL 2016 NEWSLETTER

Earlier this year, the HHS Office for Civil Rights (OCR) announced Phase 2 of its HIPAA Audit Program. On July 11, 2016, OCR notified 167 health plans, healthcare providers, and healthcare care clearinghouses of their selection for a desk audit. This newsletter tells you what you need to know about the HIPAA enforcement efforts, audit program objectives, selection, how the program works, timelines, and post-audit activities.

Margie Satinsky

HIPAA AUDITS IN 2016 – WHAT YOU NEED TO KNOW

Overview of HIPAA Enforcement Efforts

Since the passage of the HIPAA legislation in 1996 and the subsequent enactment of the Privacy and Security Rules in the early 2000s, OCR has had in place a process by which complaints could be submitted and, if appropriate, investigated. The HITECH Act of 2009 created the concept of Breach Notification, laying out the definition of a breach as well as requirements for reporting on the occurrence.

Both the complaint and breach notification processes begin with parties outside the enforcing agency. The audit program starts with OCR, allowing the agency to assess the controls and processes that covered entities and business associates have put in place.

In 2011 and 2012, OCR implemented Phase 1 of the Privacy, Security, and Breach Notification Audit Program. This first phase was a pilot, and it focused on 115 covered entities selected at random. OCR's goal was not only to look for problems with compliance, but also to identify best practices that might be shared with others. Most of the audit work was done onsite.

Phase 2 of the OCR HIPAA Audit Program began in 2016 and is currently underway. All covered entities and business associates are eligible for an audit. Nobody is under the radar screen, and the audit will impact individual and organizational providers of health services, health plans of all sizes and functions, healthcare clearinghouses, and business associates of these entities.

Selection of Candidates for Audit

OCR is looking across the entire spectrum of covered entities and business associates. Criteria for selection will include size of the entity, affiliation with other healthcare organizations, type of entity and relationship to individuals, public/private status, geography, and present enforcement activity with OCR. Entities that are currently involved in

complaint investigation or that are currently undergoing a compliance review will not be selected. If a covered entity selected for an audit is part of a larger organization, the audit will focus on just the covered entity itself.

How the Audit Program Works

Identity Verification – OCR is well aware of organizational complexities. Prior to selecting an entity for an audit, it will go through an extensive process of identifying and verifying covered entity and business associate point people, addresses, and contact information. This important first step should ensure that communication regarding audits reaches the right person in the right place.

Obligation to Respond – If an entity fails to respond to OCR's requests for information, including address verification, OCR will use publically available information about the entity to create the audit pool. Failure to respond to a request for information does not guarantee non-selection for an audit.

A Multi-Audit Process – OCR will conduct both desk audits that require submission of specific HIPAA-related material and onsite audits. Entities that are selected for a desk audit may be subject to a later onsite audit. There will be three sets of audits. Sets one and two, desk audits of covered entities and business associates, respectively, will be completed by December 31, 2016. Both will examine compliance with specific requirements of the Privacy, Security, or Breach Notification Rules. Entities that are audited will receive notice of the subject(s) of the audit in a document request letter. The third and last set of audits will be onsite and more extensive than the first two sets. The focus will be on a broader scope of requirements than the desk audits.

OCR will use a standard audit process. Entities selected for an audit will receive an email notification of their selection and a request to provide documents and other data that responds to the requirements of a document request letter. Submission will be online via a new secure audit portal on the OCR Website. Once OCR receives and reviews the documentation, it will share draft findings with the entity audited. Written responses to the OCR draft will be included in the final audit report.

Timelines

With respect to the desk audits of covered entities and business associates, OCR will send an email notification of selection for a desk audit. The letter will introduce the audit team, explain the process, discuss OCR expectations, and request documentation. Recipients will have 10 business days to submit information electronically through the OCR secure portal.

Following receipt of the draft findings, entities that have been audited will have 10 business days to review the material and return written comments, if any. The auditor will then have 30 business days to submit a final report for the entity.

With respect to onsite audits, entities will receive an email notification of selection. The auditors will schedule an entrance conference and provide more information about the process and expectations. Onsite audits will take three to five days, depending on the size of the entity. As with the desk audits, entities will have 10 business days

SATINSKY CONSULTING

to review the draft findings and provide written comments. The auditor will have 30 business days to prepare the final report.

After the Audit

The purpose of the audit program is to facilitate compliance improvement activity. OCR plans to review information from the final reports and aggregate the findings in order to better understand compliance with particular aspects of the HIPAA Rules. The results will guide OCR in determining what types of technical support and corrective action would be most helpful.

If the audit report indicates a serious compliance issue, OCR may initiate a compliance review and investigate further. OCR does not plan to post a listing of audited entities or findings of an individual audit that clearly identify the entity that has been audited. However, the Freedom of Information Act (FOIA) allows the public to request audit notification letters and other information about the audits upon request.

What's Next for Your Organization?

We've said it before and we'll say it again. Nobody is under the radar screen with respect to HIPAA Audits. The best way to prepare for the possibility of an audit is to become and remain HIPAA compliant. For additional information, please contact Margie Satinsky, MBA, President, Satinsky Consulting, LLC at **Margie@satinskyconsulting.com** or **919.383.5998**. We've helped more than 100 organizations become HIPAA compliant. We'd be happy to help you too!

- **If you haven't formalized your HIPAA compliance program**, we provide customized Privacy and Security Rule Manuals tailored to your specific needs. Both contain assessment tools that help you determine your current situation and identify next steps. The package includes staff training.
- **If you are a current client** for whom we have already prepared the Privacy and Security Manuals, completed assessments, and conducted staff training, we can update the material and re-train your staff.
- **If we did not participate in the development of your HIPAA program**, we can review current materials, make suggestions for change, and retrain your staff.

Satinsky Consulting, LLC
201 Cedar Ridge Way
Durham, NC 27705-1981
919.383.5998
Fax 919.309.0109
www.satinskyconsulting.com