TIC International Corporation
Benefit Administrators and Consultants

2016-39

July 22, 2016

CLIENT BULLETIN

Phase Two HIPAA Privacy Audits Have Begun

The Office of Civil Rights (OCR) is the *HIPAA Privacy and Security Rule* enforcement arm of the Department of Health and Human Services. In prior newsletters we discussed OCR's Phase One *HIPAA* Audits (pilot program). OCR has recently announced that Phase Two of its *HIPAA* audit program is currently underway. According to OCR, 167 selected covered entities received an audit notification letter on Monday, July 11, 2016. Desk audits of business associates begin in the Fall of 2016.

The OCR compliance and enforcement webpage states that the "desk" audits (versus "onsite" audits) will be used to examine the selected entities' compliance with certain requirements of the *Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security, and Breach Notification Rules ("HIPAA Rules").* All desk audits in Phase Two will be completed by the end of December 2016.

Phase Two Overview

Communications from OCR concerning the Phase Two *HIPAA* Rule audits are sent via email. OCR has warned that such emails may be incorrectly classified as spam and **covered entities and business associates should check their junk or spam email** folder for emails from OCR at OSOCRAudit@hhs.gov, or enable the receipt of such emails. A sample email audit notification letter is available by "*clicking here.*"

The first e-mail from OCR includes a notification letter providing instructions for responding to the desk audit document request, the timeline for response, and a unique link for each organization to submit documents via OCR's secure online portal.

A second email from OCR contains an additional request to provide a listing of the entity's business associates and also provides information about an upcoming webinar, where OCR will explain the desk audit process for auditees and take their questions. Entities have 10 business days, until July 22, 2016, to respond to the document requests.

Prepared for TIC by Mike Ewing, J.D.
Director of Research
United Actuarial Services, Inc.
(317) 580-8659 • Fax (317) 580-8651
email: mewing@unitedactuarial.com

OCR has selected compliance with certain provisions of the *HIPAA Rules* to examine as these provisions were found during the OCR pilot audits and enforcement activities to be frequent areas of noncompliance. These areas are listed below:

Requirements Selected for Desk Audit Review	
Privacy Rule	Notice of Privacy Practices & Content Requirements [§164.520(a)(1) & (b)(1)]
	Provision of Notice – Electronic Notice [§164.520(c)(3)]
	Right to Access [§164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)]
Breach Notification Rule	Timeliness of Notification [§164.404(b)]
	Content of Notification [§164.404(c)(1)]
Security Rule	Security Management Process -- Risk Analysis [§164.308(a)(1)(ii)(A)]
	Security Management Process -- Risk Management [§164.308(a)(1)(ii)(B)]

OCR indicated that a third set of audits will be onsite and will examine a broader scope of requirements from the *HIPAA Rules* than desk audits. Some entities selected for desk audits may be subject to a subsequent onsite audit.

Audit Timeline

OCR explained that the audit process will ask for various documents and other data in response to a document request letter. Audited entities will submit documents on-line via a new secure audit portal on OCR's website. OCR expects covered entities that are the subject of an audit to submit requested information via OCR's secure portal within 10 business days of the date on the information request.

OCR stated that there will be fewer in person visits during these Phase Two audits than in Phase One, but that *OCR may request an onsite visit if a visit is deemed appropriate*. As part of the process, the OCR auditors will review the documentation and share its draft findings with the covered entity being audited. The party being audited will have the opportunity to respond to these draft findings and their written responses will be included in the final audit report.

After these documents are received by OCR, the auditor will review the information submitted and provide the auditee with draft findings. Auditees will have 10 business days to review and return written comments, if any, to the auditor. The auditor will complete a final audit report for each entity within 30 business days after the auditee's response. OCR will share a copy of the final report with the audited entity.

Phase Two Onsite Audits

If an entity is selected for an onsite audit during the Phase Two audit process, it will be notified by email of its selection. The auditors will schedule an entrance conference and provide more information about the onsite audit process and expectations for the audit. Each onsite audit will be conducted over three to five days onsite, depending on the size of the entity. Onsite audits will be more comprehensive than desk audits and cover a wider range of requirements from the *HIPAA Rules*. Like the desk audit, entities will have 10 business days to review the draft findings and provide written comments to the auditor. The auditor will complete a final audit report for each entity within 30 business days after the auditee's response. OCR will share a copy of the final report with the audited entity.

After the Audit

According to OCR, audits are primarily a *compliance improvement* activity. OCR will review and analyze information from the final reports and will use the audit reports to determine what types of technical assistance should be developed and what types of corrective action would be most helpful. OCR will then develop tools and guidance to assist the industry in compliance self-evaluation and in preventing breaches.

However, if an audit report indicates a serious compliance issue, OCR may initiate a compliance review to further investigate. OCR will not post a listing of audited entities or the findings of an individual audit which clearly identifies the audited entity.

Resources

OCR has released an updated *HIPAA Rule* audit protocol to help covered entities engage in self-compliance efforts at *http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html.*

Links to a host of helpful aids can also be found at: *http://www.hhs.gov/hipaa/for-professionals.*

* * *