Health Information Compliance Alert

Enforcement News: HIPAA Phase 2 Audits Underway -- BAs: You're Next

Plus: Lack of 'actual injury' saves insurer from class-action lawsuits.

Phase 2 of the **HHS Office for Civil Rights**' (OCR) HIPAA audits are in full swing, currently in the midst of the "desk audit" portion for covered entities (CEs). And if your organization is a business associate (BA), you could be next on OCR's hit list especially if you work with a CE that's undergoing a Phase 2 audit.

OCR recently held an informational webinar for organizations selected for the Phase 2 audits. The webinar came on the heels of OCR's notifications (on July 11) to the 167 CEs selected to participate in the HIPAA desk audits. OCR Director **Jocelyn Samuels, JD** and Division Deputy Director **Deven McGraw, JD, HIP** led the webinar presentation, joined by OCR staffers **Linda Sanches, MPH** and **Zinethia Clemmons, MBA, MHA, RHIA, PMP**.

The webinar largely covered the desk audit process, including what to expect, the HIPAA controls, the final report, and document request, receipt and response. The session opened with an overview of the Phase 2 audit program, the random selection process, and the differences between desk audits versus onsite audits.

For CEs, the desk audits are now underway and will be ongoing until the end of the year, while the onsite audits will begin in early 2017. If your organization is undergoing a desk audit now, OCR may select you for an onsite audit.

Pay attention: The business associate (BA) desk audits begin in September, and OCR will select the pool of auditees largely based on those BAs that the audited CEs identify in their document responses. Comprehensive onsite audits for BAs will also begin early next year.

For the desk audits, OCR is limiting the scope to a total of seven controls drawn from the HIPAA Security Rule, the Privacy Rule, and the Breach Notification Rule. Notably, OCR will audit entities on either Security Rule controls or Privacy Rule and Breach Notification rule compliance. The subsequent onsite audits, however, will evaluate auditees based on a comprehensive set of HIPAA compliance controls.

Hidden trap: If your organization has multiple locations or sub-entities under the same ownership, OCR might select two or more of your locations for separate desk audits. If this happens, don't be surprised if OCR selects one location for privacy and breach notification controls, and the other for security controls. Treating separate locations as separate CEs is intentional, according to OCR.

After reviewing submitted documentation during the desk audits, OCR will share its draft findings with you. Then, you can respond to those findings and OCR will include your written responses in the final audit report. The final audit report will also describe how OCR conducted the audit and present any findings.

OCR will announce onsite audits in late fall. OCR has noted that a CE's "lack of cooperation with the desk audit" would be the major factor that would lead to inclusion in the onsite audit pool.

Look out: After the onsite audit process, you might not be finished. OCR could then decide to open a separate compliance review if it found significant threats to PHI privacy and security during the audit. To access more information about the Phase 2 audits, go to www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html.

How To Win A Data Breach Class-Action Lawsuit

Patients collectively suing over a HIPAA breach is a healthcare organization's worst nightmare. But if you can prove no actual injury occurred, you have a good shot at walking away from the whole mess relatively unscathed.

That's what happened to health insurer **CareFirst, Inc.**, following a June 2014 data breach that sparked two class-action lawsuits. The breach compromised the names, birthdates, email addresses and subscriber identification numbers of approximately 1.1 million policyholders, according to an Aug. 17 analysis by Long Island, N.Y.-based associate attorney **Michal Ovadia** of **Nixon Peabody LLP**.

In Attias v. CareFirst, the plaintiffs argued "that they suffered harm in the form of an increased likelihood of identity theft and the costs plaintiffs purportedly incurred to mitigate that alleged increased likelihood," Ovadia noted. But the District of Columbia federal district court disagreed with the plaintiffs in its recent decision.

The court granted CareFirst's motion to dismiss the class action on the grounds that the plaintiffs failed to adequately prove "actual injury" due to the breach. Three months prior to this ruling, a Maryland federal district court dismissed the plaintiffs' claims in Chambliss v. CareFirst for the same reasons. Specifically, the court in Attias noted that merely having your personal data stolen in a breach isn't sufficient to establish standing to sue the entity from which the information was taken.

Trend: "Significantly, this decision will join the body of emerging case law that stands for the proposition that the occurrence of a data breach without more does not constitute a 'legally actionable injury' sufficient to withstand a motion to dismiss for lack of subject matter jurisdiction," Ovadia concluded.

Beware Of Hackers Wreaking Havoc With Network Servers

The month of August yielded a few mega-sized breaches, with healthcare providers and business associates (BAs) both feeling the pain of massive HIPAA incidents.

Of the 20 total breaches affecting 500 or more individuals that entities reported to OCR during the month of August, 17 were from healthcare providers, while two were from health plans and one was from a BA.

Nine reported incidents stemmed from unauthorized access/disclosures, eight were from hacking/IT incidents, two were from theft, and one was from loss. Most of the breaches in August involved network servers (nine), while the rest involved email (five), paper/films (two), "other portable electronic devices" (two), desktop computers (one), and simply "other" (one).

There were, however, several very large breaches reported to OCR in August. The largest breach report came from **Banner Health**, a healthcare provider in Arizona, which reported a breach that affected more than 3.6 million individuals' PHI. The breach stemmed from a hacking/IT incident involving a network server.

A BA in New York State, **Newkirk Products**, reported a breach affecting more than 3.4 million individuals, which also came from a hacking/IT incident involving a network server. Yet another breach with the same circumstances affected nearly 900,000 individuals' PHI, which Arizona healthcare provider **Valley Anesthesiology Consultants** reported to OCR on Aug. 12.

In fact, a total of seven large breaches involving hacking/IT incidents of network servers were reported to OCR in August. Entities reported five such breaches in July, eight in June, and seven in May. You can view the OCR's so-called "Wall of Shame," which displays all reported HIPAA breaches affecting 500 or more individuals, by visiting https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.