Codify
BY AAPC

Health Information Compliance Alert

Enforcement News: Beware: OCR's HIPAA Penalties Are Reaching New Heights

Plus: If the C-suite execs are ignoring HIPAA compliance, you're at risk for huge penalties.

If you ignore the HIPAA Security Rule, you're effectively painting a bullseye on your back and your organization's pockets will soon be millions of dollars lighter.

On Aug. 4, the **HHS Office for Civil Rights** (OCR) announced a staggering $5.55 million settlement with **Advocate Health Care Network** in Illinois for multiple potential HIPAA violations. This is the largest HIPAA penalty against a single entity to-date.

The settlement stemmed from an OCR investigation that began in 2013, when Advocate submitted three breach notification reports involving its subsidiary Advocate Medical Group. The breaches affected the electronic protected health information (ePHI) of a total of four million individuals.

The OCR's subsequent investigation also revealed that Advocate failed to:

- Conduct an accurate and thorough risk assessment;
- Implement policies and procedures, as well as facility access controls, to limit physical access to the electronic information systems housed within a large data support center;
- Execute written business associate agreements (BAAs) to ensure safeguarding of all ePHI in the BA's possession; and
- Reasonably safeguard an unencrypted laptop when left in an unlocked vehicle overnight.

OCR stated that the settlement was so large because of "the extent and duration of the alleged noncompliance (dating back to the inception of the Security Rule in some instances), the involvement of the State Attorney General in a corresponding investigation, and the large number of individuals whose information was affected by Advocate, one of the largest health systems in the country."

Warning: "We hope this settlement sends a strong message to covered entities that they must engage in a comprehensive risk analysis and risk management to ensure that individuals' ePHI is secure," said OCR Director **Jocelyn Samuels** in the Aug. 4 announcement. "This includes implementing physical, technical, and administrative security measures sufficient to reduce the risks to ePHI in all physical locations and on all portable devices to a reasonable and appropriate level."

In addition to the record-breaking penalty, OCR also devised a resolution agreement and corrective action plan for Advocate, which you can view at www.hhs.gov/sites/default/files/Advocate_racap.pdf.

Breach Lesson: Get Management's Attention On HIPAA Compliance

Are you performing regular risk analyses? If so, that's great! But if you're not following up on the vulnerabilities and risks that those analyses uncover, you're in deep trouble.

On July 18, OCR announced that **Oregon Health & Science University** (OHSU) in Portland has agreed to pay out $2.7

million and a three-year corrective action plan to settle potential HIPAA violations. The settlement follows an OCR investigation that found "widespread and diverse problems at OHSU."

OHSU had submitted three separate breach reports to OCR, two involving unencrypted laptops and one large breach involving a stolen unencrypted thumb drive. During an investigation that followed these breach reports, OCR found that OHSU had widespread vulnerabilities within its HIPAA compliance program.

Significantly, OHSU stored more than 3,000 individuals' electronic protected health information (ePHI) on a cloud-based server without a business associate agreement (BAA), OCR charged. And despite performing regular risk analyses, OHSU didn't cover all ePHI in its enterprise as the Security Rule requires. Further, OHSU failed to address identified vulnerabilities and risks to ePHI in a timely manner.

OHSU is a large public academic health center and research university. "I've always maintained that academic medical centers are the most difficult institutions for being into HIPAA compliance, and this is a perfect illustration," notes **Jim Sheldon-Dean**, founder and director of compliance services at **Lewis Creek Systems LLC**.

Takeaway: "From well-publicized large-scale breaches and findings in their own risk analyses, OHSU had every opportunity to address security management processes that were insufficient," OCR Director **Jocelyn Samuels** said in the announcement. "This settlement underscores the importance of leadership engagement and why it is so critical for the C-suite to take HIPAA compliance seriously."

Link: To read the resolution agreement and corrective action plan with OHSU, go to www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/OHSU/index.html.

Phase 2 HIPAA Audits Have Begun Check Your Spam Folder

On July 14, the **HHS Office for Civil Rights** (OCR) announced that Phase 2 of the HIPAA Audit program "has officially kicked into high gear." But did OCR's crucial emails end up in your spam folder?

OCR has selected 167 health plans, healthcare providers, and healthcare clearinghouses to participate in the covered entity (CE) portion of the desk audits. Emails went out to selected CEs on July 11. Although OCR sent these emails to the contact addresses verified during the pre-audit phase, they may have been incorrectly classified as spam in the recipient's email service, OCR warns.

Do this: OCR is urging CEs and BAs selected for the audits to monitor their spam filtering and junk mail folders for emails from OSOCRAudit@hhs.gov.

And on July 27, OCR released new guidance on the HIPAA desk audits. The desk audits will require selected entities to submit documentation of their compliance with requirements for the Notice of Privacy Practices (NPP), access, breach notification, risk analysis, and risk management standards.

OCR held a webinar on July 13 for CEs selected to participate in the desk audits. In the webinar, OCR staff walked through the processes those CEs can expect for the audit. (Desk audits of business associates (BAs) will begin this Fall.)

Following the webinar, OCR created three targeted guidance documents (go to www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html) in response to questions received. The guidance documents include a question and answer listing, a explanation of the specific audit document submission requests and associated audit protocol, and the slides used in the webinar.

These guidance documents are helpful not only for audited CEs, but also for CEs and BAs seeking assistance with improving their compliance with the HIPAA Rules, OCR says. Additionally, OCR outlined the following HIPAA requirements

that it has targeted for the desk audit review:

1. Privacy Rule

   a. NPP & Content Requirements [§164.520(a)(1) & (b)(1)]
   b. Provision of Notice Electronic Notice [§164.520(c)(3)]
   c. Right to Access [§164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)]

2. Breach Notification Rule

   a. Timeliness of Notification [§164.404(b)]
   b. Content of Notification [§164.404(c)(1)]

3. Security Rule

   a. Security Management Process Risk Analysis [§164.308(a)(1)(ii)(A)]
   b. Security Management Process Risk Management [§164.308(a)(1)(ii)(B)]