Health Information Compliance Alert

Enforcement News: Look Out: OCR Now Has 'Something To Prove'

Plus: Mobile health developers are getting a HIPAA education.

As if you didn't have enough to worry about regarding the **HHS Office for Civil Rights**' (OCR) increasingly punishing HIPAA enforcement actions now, a new government watchdog report says that OCR isn't doing enough to crack down on HIPAA violations.

On Sept. 28, the **HHS Office of Inspector General** (OIG) released a report that examines whether OCR is providing sufficient oversight responsibilities. And the report is critical of the OCR's HIPAA enforcement performance, "effectively giving OCR 'something to prove,'" according to an Oct. 1 analysis by attorneys **Dianne Bourque** and **Jordan Cohen** for the law firm **Mintz Levin P.C.**

The OIG studied statistical samples of privacy cases that OCR investigated, as well as surveys of OCR staff and interviews with OCR officials, Bourque and Cohen said. And after examining this data, the OIG decided that OCR's oversight is lacking in several areas, finding that:

- OCR's oversight is primarily reactive, with investigations of possible noncompliance largely in response to complaints;
- OCR has not fully implemented the required audit program to proactively assess possible noncompliance among covered entities (CEs);
- OCR subsequently failed to obtain complete documentation of corrective actions that CEs had taken in 24 percent of cases where OCR requested corrective action;
- Some OCR staff rarely or never checked to determine whether the OCR or another enforcement entity had investigated a CE, and the staff's failure in this task may be due to the limited functionality of the OCR's case tracking system; and
- More than one-quarter of Medicare Part B providers did not address all of the applicable HIPAA Privacy Rule standards and may therefore be failing to adequately safeguard protected health information (PHI).

The OIG recommended that the OCR should fully implement a permanent audit program, maintain complete documentation of corrective actions, and continue to expand outreach and education efforts to CEs, according to Bourque and Cohen. The OIG also recommended that the OCR develop an efficient method in its case-tracking system to search for and track CEs, as well as develop a policy requiring OCR staff to check for previous investigations of CEs.

Significance: "The OIG's report comes amidst the impending start of OCR's Phase II audit program," Bourque and Cohen wrote. "Whether the OIG's report will impact how OCR conducts its Phase II audits, if at all, remains to be seen. However, it is not inconceivable that OCR could feel pressured to more aggressively investigate potential Privacy Rule noncompliance, and [CEs] would be well-served to ensure that they are ready to respond to such audits."

The OCR agreed with all of the OIG's recommendations and is planning specific activities to address them. To read the OIG's report, go to http://oig.hhs.gov/oei/reports/oei-09-10-00510.pdf.

Check Out A New Platform For Mobile Health & HIPAA Privacy Protection

If you're like many healthcare entities, you've probably experienced working with a software or mobile health developer who is less than knowledgeable about HIPAA regulations. The good news is that the **HHS Office for Civil Rights** (OCR) is launching a new campaign to better educate these developers.

OCR recently launched a new platform at http://hipaaqsportal.hhs.gov/, which is specifically tailored for mobile health developers and others interested in how health information technology (HIT) and HIPAA privacy intersect. On Oct. 5, OCR

released a bulletin inviting developers to ask questions about HIPAA Privacy and Security.

"We are experiencing an explosion of technology using data about the health of individuals in innovative ways to improve health outcomes," OCR says. "Building privacy and security protections into technology products enhances their value by providing some assurance to users that the information is safe and secure and will be used and disclosed only as approved or expected."

Problem: OCR points out that many mHealth developers are not familiar with the HIPAA Privacy and Security Rules, not how the Rules apply to their products. OCR wants stakeholders to browse the site, which is on the Ideascale cloud-based idea management platform, and then submit questions or offer comments.

Specifically, OCR wants stakeholders to provide input on the following:

- What topics should OCR address in guidance?
- What current provisions confuse you?
- How should this guidance look to make it more understandable and accessible?
- Submit questions about HIPAA or present a use case.

How You Could Face (Successful) Negligence Claims For A Data Breach

The increasing number of unsuccessful HIPAA breach-related lawsuit may make you feel safe, but they shouldn't. Negligence claims could prove lethal, especially if your organization has written policies that reference your duty regarding data privacy laws.

Background: In July 2013, **Advocate Health and Hospital Corporation** experienced a data breach when thieves stole four unencrypted laptops from one of its administrative offices. Affected patients filed a series of class-action lawsuits following the breach.

In one lawsuit, Tierney v. Advocate Health and Hospitals Corporation, the **Seventh Circuit Court of Appeals** affirmed a lower court's ruling that Advocate was not a "consumer reporting agency" under the federal Fair Credit Reporting Act (FCRA) and therefore dismissed the plaintiffs' FCRA claims in August 2015.

But despite dismissing five of six claims in a consolidated class-action lawsuit against Advocate, an Illinois circuit court judge allowed a negligence claim to remain standing, based on the healthcare provider's duty to reasonably safeguard information. This claim is now still pending against Advocate, according to a Sept. 24 analysis by attorneys **Carolyn Metnick** and **Jason Betke** for the law firm **Akerman LLP**.

The complaint in the Illinois class-action alleges that Advocate's written policies, which referenced compliance with data privacy laws, formed part of its promise to the plaintiffs, Metnick and Belke explained. Advocate's failure to follow its own policies and procedures, as well as to adequately protect patient information, was a "breach of contract."

Advocate also faced two other state court cases that involve negligence claims and violations of state data breach laws, but the courts dismissed those cases earlier this year for lack of standing. On an unsuccessful appeal, the appellate court consolidated the cases and held that the plaintiffs' allegations of injury based on only an increased risk of identity theft were "speculative and conclusory," Metnick and Betke said.

Bottom line: "As the Advocate cases demonstrate, data breaches will continue to generate claims under both federal and state laws," Metnick and Betke warned. "While HIPAA litigation is alive and well, a developing caveat is that state laws through data breach and negligence claims are becoming litigation pressure points for healthcare providers."

"Additionally, the enactment of new and amended state laws aimed at further protecting the consumer and medical information may provide fertile grounds for data breach claims under state law," Metnick and Betke added.

'Encryption' Is The Hottest Buzzword At NIST/OCR HIPAA Security Conference

Want to know what people at the **U.S. Department of Health and Human Services** (HHS) think is the most important

precaution you can take to avoid a HIPAA breach? If so, you're in luck.

The sessions from the annual HIPAA Security Conference presented by the **HHS Office for Civil Rights** (OCR) and the **National Institute of Standards and Technology** (NIST) will be available to the public at www.nist.gov/itl/csd/safeguarding-health-information-building-assurance-through-hipaa-security-2015.cfm. The speakers are top officials at HHS who deal specifically with HIPAA and related issues.

"The word encryption was emphasized by many of the speakers at the annual official NIST/OCR HIPAA Security Conference," says **Jim Sheldon-Dean** , founder and director of compliance services for **Lewis Creek Systems LLC**, who attended the conference. "The sessions are definitely worth watching. You will learn a lot," he enthuses.

Also, "an OCR official stated at the conference that the risk analysis is the cornerstone of HIPAA security compliance," according to attorneys **Anna Watterson** and **Sean Baird** of **Davis Wright Tremaine LLP**.

NIST and OCR held the conference on Sept. 2 and Sept. 3 in Washington, D.C. The conference explored the current health information technology security landscape and the HIPAA Security Rule.