Codify
BY AAPC

Health Information Compliance Alert

Case Study: Don't Do Business Without a BAA - It's Just That Simple

Manage risks, or fines will ensue, OCR case suggests.

If you're weighing the costs of a risk analysis in 2019, you may want to follow through and fork over the cash for a comprehensive assessment. One organization dropped the ball on its risks - and is now paying the price.

Background: Last month, the HHS Office for Civil Rights (OCR) reached a $500,000 settlement with **Advanced Care Hospitalists PL (ACH),** a Florida-based organization that supplies contracted internists to hospitals and nursing homes, for major HIPAA violations. From November 2011 to June 2012, the physicians' group conducted business with a nefarious individual, claiming to work for Doctor's First Choice Billings, Inc. (First Choice) without the billing company's knowledge, an OCR release said.

However, according to the OCR, it gets worse. In February of 2014, a local hospital advised ACH that its patients' personal information (names, birthdays, and social security numbers) were available for public display on the First Choice website. Originally, the physicians' group thought only 400 individuals were impacted, but on further review, it was discovered that an additional 8,855 patients were also exposed, noted the OCR.

Here's the Rub

After the agency was notified and the feds began their investigation of the breach, details started to emerge about ACH's risk analysis shortcomings and its lack of a business associate agreement (BAA) with First Choice, the OCR release indicated. "ACH, as required by HIPAA... failed to adopt any policy requiring business associate agreements until April 2014," the OCR said. In addition, "although ACH had been in operation since 2005, it had not conducted a risk analysis or implemented security measures or any other written HIPAA policies or procedures before 2014."

"While this settlement is a particularly egregious example of an unvetted vendor gone rogue, it highlights the importance of covered entities carefully examining their vendors who may have access to PHI, implementing policies and procedures requiring BAAs for such vendors, and keeping track of their BAAs through a database or other method," writes attorney **Sarah Beth S. Kuyers** with national law firm **Mintz, Levin, Cohn, Ferris, Glovsky, and Popeo, PC** in legal analysis.

Resolution: According to the resolution agreement (RA), ACH must reform its ways with a "robust" corrective action plan (CAP) in addition to the large financial settlement. The compliance requirements under the CAP include:

- Write new OCR-approved policies and procedures.
- Perform an "enterprise-wide" risk analysis, manage the detailed risks, and implement new protocols with approval at each stage from HHS.
- Address certain aspects of the HIPAA Privacy, Security, and Breach Notification Rules in the compliance planning.
- Account for business associates and engage in BAAs with all partners and vendors.
- Provide annual compliance reports to HHS.
- Train all staff using HHS-endorsed educational materials.

Timeline: ACH must submit "all documents and records relating to compliance with this CAP for six (6) years from the effective date" to the OCR "for inspection and copying," and whenever requested, according to the RA.

Read the ACH's agreement at www.hhs.gov/sites/default/files/ach-signed-ra-cap.pdf.

"The ACH settlement and RA highlight that the financial and intrinsic costs associated with a breach of patient

information are much higher than the initial time and costs for a physician practice to implement a privacy and security program," cautions Cincinnati-based attorney **Paulette Thomas** with national law firm **Baker Hostetler** in its Health Law Update blog.

Federal warning: "This case is especially troubling because the practice allowed the names and social security numbers of thousands of its patients to be exposed on the Internet after it failed to follow basic security requirements under HIPAA," stressed OCR Director **Roger Severino** in a release.

Review the OCR release at www.hhs.gov/about/news/2018/12/04/florida-contractor-physicians-group-shares-protected-health-information-unknown-vendor-without.html.