COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 19, Number 2. February 28, 2019 With Some Exceptions, OCR's 2018 Was More of the Same—Only Bigger

By Theresa Defino

Now that 2019 has arrived, HIPAA compliance eyes turn to the HHS Office for Civil Rights (OCR), awaiting word of this year's first settlement.

Although it's early, the year began the same way as in 2018, in that no settlements were issued in the month of January. In 2018, OCR settlements also skipped the months of April, May, July and August. But the agency packed a lot of enforcement wallop into the other seven months, with nine settlement agreements and one court-ordered action that in total brought the agency $21.335 million.

While this was not a record, it was close. In 2017, OCR collected $19.4 million from 10 organizations, a year after hitting its record of $24.5 million in 2016 (*RPP 1/18, p. 1*).

OCR officials always advise taking a close look at each enforcement action to understand where covered entities (CEs) and business associates (BAs) went wrong, and how they plan to fix those deficits—as directed by OCR. In most instances, settlements are accompanied by detailed, multiyear corrective action plans (CAP).

Targets Were Old Favorites

So here's one big red flag for compliance officials: All of the underlying incidents that gave rise to the settlements in 2018 were the result of errors by employees of the CE or BA. Even the so-called "sophisticated" cyberattack that led to the $16 million settlement with Anthem Inc.—OCR's largest ever—began with a successful phishing attempt that duped a worker into sharing access credentials.

Settlements last year again showed CEs' weakness in managing their BAs, but raise the question of why OCR has sanctioned so few BAs. This year saw only the second one in OCR's history, and in this case, OCR exacted a couple of ounces of flesh from a company that was already bankrupt and out of business. It also was connected to a CE it had previously sanctioned.

In 2018, OCR's actions also drew attention to one of its now-frequent targets—disclosures to the media—but for the first time, the central figure in one such settlement was a dog.

To Chris Apgar, a longtime HIPAA consultant and president of Apgar & Associates, 2018 settlements "were much the same as before" with the exception of the "size of the Anthem settlement."

Still, they bear review. The targets of OCR's settlements last year included several small organizations, reflecting what Apgar sees. Compliance by smaller CEs remains the one area that isn't experiencing a big enough improvement in compliance, says Apgar. These organizations are getting better, but "better is often not enough."

Issues continue to be "conducting risk analyses, monitoring audit logs, mock phishing and employee training and business continuity," among others, according to Apgar. Some of these problems plague large organizations. Another deficit: adoption of encryption.

“I just completed writing a risk analysis report for a large specialty practice,” says Apgar. “None of the practice’s laptops are encrypted.”

Without much OCR attention to BAs, they may get the impression they’re immune from enforcement, which puts CEs in the enforcer role. Increasing numbers of CEs have taken this on, says Apgar.

“From a BA perspective, I’m seeing more and more pressure being brought to bear by CEs to demonstrate robust security has been implemented,” he says. “Especially in health information technology, it seems BAs are looking at sound security as a market-driver and in some cases a differentiator—‘look what we have that our competitors don’t.’”

OCR should bring more cases against BAs, says Apgar. But he stresses that OCR’s focus should be narrow, looking at “more current potential violations.” He adds that other types of BAs—attorneys and consultants, for example—have not faced much “market pressure to implement sound security.”