Report on Patient Privacy Volume 19, Number 1. January 31, 2019 With a Focus on BAs, OCR Releases Two New Settlements, Closes Out 2018 With $21 Million

By Theresa Defino

A tiny public medical center in Colorado and a group of hospitalists in Florida were the final organizations in 2018 to face HIPAA enforcement actions by the HHS Office for Civil Rights (OCR). While the amounts paid were wildly divergent—the physicians paid OCR five times what the hospital did—the settlements shared much in common. Central to both settlements was the lack of a business associate agreement (BAA).

The settlements also fit OCR's mold for the year of noteworthy and unusual cases. The pair of settlements brought OCR's total enforcement actions for the year to 10 and a near-historic high of $21.335 million. The 2018 total is $2 million shy of the record set in 2016 (*RPP 12/16, p. 1*).

In 2018, OCR collected the largest payment in its history—$16 million from Anthem Inc. for a 2015 cyberattack that affected records for 78.8 million individuals (*RPP 11/18, p. 1*). During the year, OCR also returned to other favorite themes in its settlements, including dinging organizations for inappropriate disclosures of protected health information held on mobile devices and sharing PHI with the media (*RPP 12/18, p. 1*).

The larger settlement of the two released in December involved a billing company and an apparent rogue worker that resulted in the PHI of 9,200 patients being posted online.

Advanced Care Hospitalists (ACH) PL of Lakeland, Florida, paid OCR $500,000 and agreed to a two-year corrective action plan (CAP) for failing to have a BAA with the billing service.

But perhaps more noteworthy is OCR's statement that ACH "failed to implement any" policies and procedures to comply with the privacy, security and breach notification rules until the spring of 2014, even though the physician group had been operational since 2005. ACH provides internal medicine physicians under contract to hospitals and nursing homes.

The privacy rule went into effect in 2003, the security rule two years later. The breach notification requirements have been in place since 2009. It has been a while since OCR has deemed an organization completely noncompliant. ACH did not admit to wrongdoing as part of the settlement.

According to OCR, from November 2011 through June 2012, ACH used the services of an individual who "represented himself to be a representative" of a billing firm called Doctor's First Choice Billings Inc. OCR doesn't specify what services the billing individual provided.