COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 18, Number 11. November 30, 2018 OCR Exacts Its Pound of Flesh From Anthem With $16 Million Settlement, Corrective Actions

By HCCA Staff

Nearly two months to the day after a judge signed off on a record-breaking $115 million class action lawsuit triggered by Anthem Inc.'s massive breach, the HHS Office for Civil Rights (OCR) announced a historic $16 million settlement against the Indiana-based health plan for the same incident.

In addressing the size of the settlement, OCR Director Roger Severino says that the "largest health data breach in U.S. history fully merits the largest HIPAA settlement in history." But OCR provided no specific information regarding how it arrived at the $16 million figure. Anthem also would not address this issue.

For its part, Anthem seemed glad to put the matter behind it—especially given OCR's action marks Anthem's third set of formal consequences stemming from the 2014 phishing attack in which hackers laid in wait for almost a year before siphoning the protected health information (PHI) from an estimated 78.8 million individuals, presumably Anthem's entire book of business (*RPP 3/15, p. 1*).

With less than 60 days to go in 2018 and $20.6 million already in the bank, the settlement inches OCR closer to its 2016 record of collecting $23.5 million from errant HIPAA covered entities (CEs) and business associates (BA). (For a look at annual amounts, see table, p. 7.) The settlement is OCR's sixth of the year, although three were part of a mega-settlement related to the filming of a Boston television series (*RPP 10/18, p. 1*).

Anthem Alleged to Suffer Multitude of Problems

The 2014 Anthem Inc. hack, according to the individuals who sued following the breach affecting 79 million individuals, was a crime of opportunity that resulted because the health plan "failed to implement basic policies and procedures that could have prevented the attack," in the words of current and former Anthem members. A class action suit against Anthem was recently settled for $115 million (*RPP 9/18, p. 1*). In addition, the HHS Office for Civil Rights collected $16 million from Anthem for the same breach (see story, p. 1).

The suit alleged Anthem also "needlessly maintain[ed] information regarding former customers (as far back to 2004) on their databases and servers."

Filed in 2017, a 291-page amended complaint, representing plaintiffs from suits around the country, alleged a list of "failures" in basic HIPAA-related practices. Although some of the list was redacted, much is not.

Generally, the suit derides Anthem for failing to "implement basic technology monitoring systems that would have detected the cyber attackers' activities, such as monitoring data usage on the system, monitoring data extraction, or performance monitoring." Of interest to compliance officers, the list also includes that Anthem "lacked reasonable encryption policies."

An Anthem official, according to the suit, "publicly admitted that a large portion of the Anthem database was not encrypted. Instead, Anthem and Anthem affiliates only used encryption when data was being moved around within their information environment and for such things as mobile phones and laptops."