Report on Patient Privacy Volume 21, Number 1. January 07, 2021

# Belated OCR Audits Shine New Light on Old Issues, Including Security Failures

By Theresa Defino

It’s been almost 10 years since the compliance community was abuzz with word that the HHS Office for Civil Rights (OCR) was embarking on a program to audit covered entities (CEs) for compliance. Many were anxious about the possibility of enforcement action against those who ran afoul of HIPAA rules governing privacy, security and breach notification. Audits were required by Congress under the 2009 HITECH Act.

After completing a pilot of 115 on-site audits in 2012-2013, OCR ultimately used contractors to conduct desk audits—largely reviews of policies and procedures—for 166 CEs and 41 business associates (BAs); these took place from 2016 to 2017.[1]

What those audits revealed remained unknown until the middle of last month, when OCR finally released the results of the program—perhaps of limited use because they are now so dated.[2]

In other respects, though, the areas of noncompliance the auditors found,[3] such as the failure to conduct a security risk analysis and corresponding risk management plan, are the same ones that the health care community has struggled with since the security rule went into effect in 2005.

In its Dec. 17 announcement of the audit findings, OCR did not address why it took so long to release the results. *RPP* did not receive a response from OCR about the timing of the findings or possible next steps for the audit program.

Of the 165 CEs audited, 90% (150) were providers. Of these, 55% (83) were practitioners, 18% (27) were pharmacies, 17% (25) were hospitals, 3% (5) were health systems, 2% (3) were skilled nursing facilities, 1% (2) were elder care facilities, and 3% (5) were classified as “other.”