Report on Patient Privacy Volume 21, Number 6. June 10, 2021
New Settlement Shows a Return To Enforcement, Security Basics

By Theresa Defino

Remember a time *before* the HHS Office for Civil Rights (OCR) decided to make patients' access to medical records a priority?

With its 19th settlement under its belt just last month, those who may be caught up in OCR's medical records focus could be forgiven: the agency has settled with a record number of covered entities (CEs) for a single issue.

In 2018, then OCR Director Roger Severino launched the agency's Right of Access Initiative, with a steady drumbeat of settlements to follow. Six of this year's eight settlements are part of that effort—and on June 2, OCR announced yet another agreement with a CE over this issue, for $5,000 with an endocrinology practice in West Virginia.[1]

But there also was a nonaccess settlement in May for $25,000 with Peachstate Health Management LLC,[2] and it differs from the first 2021 OCR security rule agreement in more than just financial terms.

The year started off with a whopper of a settlement—New York-based Excellus Health Plan Inc. agreed to pay $5.1 million and implement a two-year corrective action plan (CAP) related to the discovery in 2015 of a hacking in 2013 that exposed the protected health information (PHI) of 9.3 million individuals.[3]

Announced May 25, Peachstate's settlement, unlike many OCR agreements, calls for the firm to hire an external monitor to ensure its compliance with a three-year CAP, a year longer than the term the agency has imposed in the majority of cases in the recent past.

OCR Documented Failures

According to the settlement, Peachstate:

- "Failed to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI held by Peachstate," as required under 45 C.F.R. § 164.308(a)(1)(ii)(A));
- "Failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level identified in its risk analysis or assessment," as required under 45 C.F.R. § 164.308(a)(1)(ii)(B)).
- "Failed to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI," as required under 45 C.F.R. § 164.312(b)).
- "Failed to maintain policies and procedures to comply with Subpart C in written (which may be electronic) form and to maintain written (which may be electronic) record of any action, activity, or asssessment (sic) required by Subpart C or these policies and procedures," as required under 45 C.F.R. § 164.316(b)).[4]