COSMOS
Navigate the Compliance Universe

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]

VA Reported Breach in 2015

While these alleged failings may have been straightforward, OCR's path to them—and to Peachstate—was anything but.

OCR provided the details in its settlement agreement, but first, an introduction to the firm.

"Peachstate Health Management, Inc. d/b/a AEON Clinical Laboratories (Peachstate), which is a covered entity, as defined at 45 C.F.R. § 160.103 , and therefore is required to comply with the HIPAA Rules," OCR said. Peachstate is certified under federal law (the Clinical Laboratory Improvement Amendments Act), and "provides, among other things, clinical and genetic testing services mainly through its publicly-traded parent company, AEON Global Health Corporation."

At the heart of the settlement, however, is yet another company—Authentidate Holding Corporation (AHC). This firm was a business associate (BA) to the U.S. Department of Veterans Affairs, which managed the VA Telehealth Services Program.

On Jan. 7, 2015, VA reported to OCR that an database of patients who had used telehealth services was posted online. At the time, news media reported that VA had "notified and offered credit protection to all 7,054 veterans in the database. VA says the type of security flaw was one that could have exposed veterans' data, including name, address, date of birth, phone number and VA patient identification number, via the Internet."[5]

Merger Changed OCR's Focus

Eighteen months later, OCR "initiated a compliance review of AHC to determine its compliance with the Privacy and Security Rules related to the breach," and learned that "AHC and Peachstate had earlier entered into a 'reverse merger' on January 27, 2016, whereby AHC acquired Peachstate."

OCR then turned its attention to Peachstate and "opened a compliance review into the clinical laboratories of Peachstate to assess the clinical laboratories' compliance with the Privacy and Security Rules."

As noted earlier, OCR found sweeping—but fairly common—noncompliance and negotiated a $25,000 settlement. While the number of patients potentially affected was relatively small, the size of the payment is also among the lowest OCR ever imposes and is somewhat surprising given the scope of the noncompliance.

As a corporate entity, Peachstate doesn't exist. Authentidate changed its name to Aeon Global Health Corp. in January 2018. Paul S. Suda, Aeon's general counsel, was to sign for the firm, according to the settlement agreement, which is dated April 28. Aeon and Suda did not respond to *RPP*'s requests for comment.

OCR refers to Aeon as Peachstate throughout the CAP, so *RPP* will as well.

Requirements in the CAP match the deficits the agency said it found in its compliance review, but go beyond those in mandating, as noted earlier, Peachstate hire an external monitor. The job of this individual is to "monitor and review Peachstate's compliance" with the CAP. The monitor needs to be hired within 60 days of the effective date of the CAP.

HHS Must Approve Monitor Selection

The monitor will need to "certify in writing that it has expertise in compliance with the HIPAA Security Rule and is able to perform the reviews described below in a professionally independent fashion taking into account any other business relationships or other engagements that may exist." Peachstate has to "submit the name and

qualifications of the designated individual or entity to HHS for HHS's approval."

The monitor will have some level of job security, as well—if Peachstate wants to fire the person, it must run that decision by HHS first. Additionally, HHS can conduct its own "validation review." If officials have reason to believe that "(a) the Monitor reviews or reports fail to conform to the requirements of this CAP; or (b) the Monitor report results are inaccurate, HHS may, at its sole discretion, conduct its own review to determine whether the Monitor reviews or reports complied with the requirements of the CAP and/or are inaccurate."

Specific duties of the monitor are to "assist in the collection of data to serve as evidence of the effectiveness of Peachstate's compliance program"; "further define and recommend the tools to assist Peachstate in protecting the PHI it creates, receives, maintains, and transmits"; and "recommend security measures to ensure the confidentiality, integrity, and availability of PHI received, created, maintained, and transmitted within Peachstate's enterprise-wide job related functions that involve exposure to PHI within its environment."

Additionally, the monitor must prepare quarterly reports that are submitted both to Peachstate and HHS. In turn, Peachstate management is required to respond to the reports and submit those responses to HHS. Under the CAP, more serious issues, however, can't wait to be transmitted via these reports.

"The Monitor shall immediately report any significant violations of the CAP to HHS and Peachstate, and Peachstate shall prepare a response, including a plan(s) of correction, and provide such response to HHS and the Monitor," the CAP states.

Detailed Risk Analysis Required

At the same time it is hiring and installing the monitor, Peachstate must also act quickly to complete a risk analysis.

CEs sometimes struggle with what constitutes, in OCR's eyes, an acceptable risk analysis. The settlement agreement can help inform that understanding, as it pointedly states that Peachstate "shall conduct a comprehensive, enterprise-wide risk analysis of the security threats and vulnerabilities of all electronic PHI created, received, maintained or transmitted by Peachstate, including all electronic media, workstations, and information systems owned, controlled or leased by Peachstate, which store or can access electronic PHI. As part of this process, Peachstate shall develop a complete inventory of all electronic equipment, data systems, and applications that contain or store ePHI which will then be incorporated in its risk analysis."

HHS will approve both the risk analysis and a corresponding risk management plan before Peachstate can implement the plan and make required changes in its policies and procedures—and these are also subject to review and revision by HHS.

The CAP contains other requirements common to previous settlements, including submission of training materials and evidence that training was conducted and completion of annual reports that review implementation and any potential HIPAA violations that have transpired.

1 HHS, "OCR Settles Nineteenth Investigation in HIPAA Right of Access Initiative," news release, June 2, 2021, https://bit.ly/3vVBBQ7.
2 HHS, "Clinical Laboratory Pays $25,000 to Settle Potential HIPAA Security Rule Violations," news release, May 25, 2021, https://bit.ly/3w8FAJf.
3 Jane Anderson, "Excellus Agrees to Pay $5.1M, Implement CAP To Settle OCR Investigation From 2015 Breach," *Report on Patient Privacy* 21, no. 2 (February 2021), https://bit.ly/3cgkDUH.
4 HHS, "Peachstate Resolution Agreement and Corrective Action Plan," resolution agreement, April 28, 2021,

https://bit.ly/3z9giN0.
5 Federal News Radio Custom Media, "Contractor security flaw puts data of 7,000 veterans at risk," December 24, 2014, https://bit.ly/3wYyDKt.