COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 24, Number 1. January 11, 2024 OCR Ends Year With Settlements That Tread Old Ground, Says New Rules Are Coming—Someday

By Theresa Defino

If the penultimate enforcement settlement of 2023 issued by the HHS Office for Civil Rights (OCR) sounds familiar, that's with good reason. And the last one of the year should ring some bells, too.

That's because OCR's two settlements announced in December for alleged HIPAA violations by an emergency medicine practice in Louisiana and a multispecialty group operating in parts of New Jersey and Connecticut demonstrate two common failings, both historic and more recent: lack of a security risk analysis and tardiness or nonresponsiveness to a patient's request to access medical records.

But while these settlements might not have been surprising, another HHS announcement was: according to the most recent update of federal rules under development, OCR is planning to revise the security rule as part of an agency-wide effort.[1] In addition, officials described a new cybersecurity strategy for the health care sector.[2]

Along with its regulatory actions, OCR pledged to continue pursuing enforcement when there are alleged HIPAA violations. In 2023, the agency issued a total of 13 settlements—bracketed on both ends by exactly the type of cases with which it concluded the year.[3]

Settlements Were Down, Recoveries Up

At the high end was a $1.3 million payment from L.A. Care following a small breach and a mis-mailing of some members' cards, but the lack of a security analysis was the primary basis for the high penalty. At the low end was a $15,000 payment in a case in which a psychiatrist did not give a father a copy of his minor children's records despite repeated requests.

In total, the 13 settlements last year brought OCR $3,982,500. In 2022, it took $2,172,640 from 22 regulated entities; 17 were right-of-access cases, compared to just four in 2023. Nary a dentist was among them: in 2022, eight dentists felt OCR's regulatory might.

Turning to the most recent settlement, records issues, as noted, involving Optum Medical Care of New Jersey, triggered a $160,000 settlement that includes a two-year corrective action plan (CAP), according to OCR's Dec. 15 announcement.[4] The practice was previously known as Riverside Medical Group and Riverside Pediatric Group. This marked OCR's 46th settlement of this type since the access initiative began in 2019 under then-OCR Director Roger Severino.

Optum officials did not respond to specific questions from *RPP* about the settlement or records access issues. "Optum has long supported patients' timely access to their health information. We have addressed the cause of this issue and are sorry for any inconvenience it may have caused," a spokesperson said in an email.

Spate of Complaints Got OCR's Attention

According to OCR, six Optum New Jersey patients complained to OCR from September to October 2021. "In

February 2022, OCR initiated investigations of these Right of Access complaints," the agency said. "The complaints disclosed that patients received their requested records between 84 and 231 days after their respective requests were submitted."

OCR noted that these "timeframes are well outside of the HIPAA Right of Access requirement that providers must give access to medical records requested no later than 30 calendar days from receiving the individual's request." However, OCR's statement is somewhat incorrect. Providers must respond to a request within 30 days, and the response may consist of a written statement that more time is needed, with an estimate of why and when the request is expected to be fulfilled.

The complaints were from adults requesting their own records or wanting their minor children's medical records. Requests were submitted to an email address and involved three of the group's practice sites, the settlement states.[5]

Most of the requirements under the CAP are fairly standard, but there are some additional ones. Under the CAP, Optum must "review, and to the extent necessary, revise the policies and procedures that apply to its workforce and relate to the right of access to protected health information (PHI) to be consistent with 45 C.F.R. § 164.524," and submit the revisions to OCR for approval within 30 days of the effective date of the settlement. The posted documents are dated Nov. 15.

Periodic Reports Due on Training, Requests

Appropriate employees must then be trained on the policies and procedures within 90 days. Further, every 90 days afterward during the CAP period, the practice "shall show evidence of the weekly New Hire Orientation Training and any other targeted trainings performed for [the practice] on the Privacy Rule requirements concerning an individual's right of access to PHI."

Another uncommon—but not unique among records settlements—requirement ensures that OCR has tight oversight over how access requests are handled.

Every 90 days, the practice must "submit to HHS a report which includes a monthly count of all requests for access to PHI received by [the practice] via all submission modalities except via its business associate, Ciox," the settlement states. The report must contain dates requests were received, when they were fulfilled, "the format requested, the format provided, the number of pages (if provided in paper format), fee charged (if any), excluding postage, and – if records were emailed to the requestor – whether [the practice] either (i) confirmed the requestor's receipt of the emailed records, or (ii) has no indication that its email(s) to the requestor were not received." The report also needs to include details of any requests for access that Optum denies.

The settlement makes no other mention of Ciox, and the Optum spokesperson did not address *RPP*'s question about Ciox's involvement in fulfilling requests.

First Settlement Due to Phishing?

In November, OCR said it reached its first settlement due to a ransomware attack, holding out a small medical billing company as an example of the dangers of this kind of breach. Yet, the CEO told *RPP* in an exclusive interview that no ransom was paid, no PHI was misused, and the organization was down for a day.[6] He only agreed to a $100,000 payment because OCR wouldn't negotiate further, and his insurance covered it. This situation is nothing like the recurrent, days-long sieges that cripple hospital systems across the country, seemingly daily or weekly.

OCR claimed a similar achievement in its Dec. 7 announcement of a $480,000 settlement with Lafourche Medical Group LLC, which the agency said was its first to impose sanctions stemming from a phishing-based attack.[7] Finalized in November, the penalty amount makes it the third priciest of 2023 but still a far cry from the millions OCR used to collect prior to its loss in court to MD Anderson Cancer Center, which had challenged a $4 million fine.

"Phishing is a type of cybersecurity attack used to trick individuals into disclosing sensitive information via electronic communication, such as email, by impersonating a trustworthy source," agency officials explained.

Breaches Commonly Involve Email

However, emails—either as a point of entry to steal credentials and/or install malware or as a source of unallowable disclosures—have figured prominently in OCR settlements for years. Moreover, many entries on OCR's breach reporting portal list email as the "location" of a breach—in fact, there are 177 such entries among cases that are still open and less than two years old, and 1,184 breaches involving email that are older than two years.

On May 28, 2021, HHS received a breach notification report indicating that two months earlier, the group "learned that an unauthorized individual obtained access to one of its owners' email accounts through a phishing attack," according to the settlement documents.[8]

The email account contained PHI, but the group was "unable to identify the specific patients affected," so it notified 34,862 individuals, or the whole patient base.

OCR notified Lafourche on Jan. 13, 2022, that it had begun its investigation. Interestingly, the settlement documents don't specify that the phishing resulted in an unallowable disclosure, something that usually is mentioned following this kind of attack.

And despite the novelty of phishing being involved, OCR ultimately concluded there were two common potential HIPAA violations. OCR alleged that Lafourche "never conducted a Security Rule risk analysis prior to the 2021 security See 45 C.F.R. § 164.308(a)(1)(ii)(A)" and "never implemented procedures to regularly review records of information system activity prior to the security See 45 C.F.R. § 164.308(a)(1)(ii)(D)."

RPP contacted the practice by phone seeking comment from Adam Arcement, M.D., described in the settlement documents as the owner of the medical group. He was unavailable for comment by phone and did not respond to repeated emails.

CAP Includes Ongoing Reporting to OCR

Arcement agreed to a two-year CAP in addition to making the nearly half-million-dollar payment. The requirements are standard in settlements of this type and do not obligate Arcement to hire an external monitor.

The CAP notes that the medical group completed a security risk assessment at the end of 2022 and requires it to develop a corresponding risk management plan. Specifically, it must "create, document and implement security measures sufficient to reduce risks and vulnerabilities to ePHI [electronic protected health information], identified in its December 2022 Security Risk Assessment, to a reasonable and appropriate level" within 60 days of the effective date of the CAP.

As is typical in these kinds of settlements, the group also must "annually conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of [its] ePHI…including any affiliates that are owned, controlled, or managed by [the group], and document the security

measures…implemented or is implementing to sufficiently reduce the identified risks and vulnerabilities to a reasonable and appropriate level."

Arcement also must develop or revise policies and procedures that address any of the threats and vulnerabilities uncovered during the initial risk assessment during the CAP period and submit them to OCR within 30 days of the agency's approval of the risk management plan. Such policies and procedures must also be reviewed and revised, if necessary, on an annual basis.

Revised policies are to be distributed to the workforce for training within 30 days of OCR approval and within 30 days to new hires. Before the training occurs, however, the medical group has to submit its materials —"including specific training related to the policies and procedures…as necessary and appropriate for workforce members to perform their job duties" to OCR for approval.

Lafourche must submit an implementation report to OCR within 120 days of the start of the CAP to provide attestations that it has met the initial requirements.

On a quarterly basis, Lafourche is required to notify OCR of any violations of its HIPAA-related policies and procedures and actions it took in response. At the end of each of the two years of the CAP, it must provide OCR with an annual report attesting that it is in compliance with the requirements.

1 Theresa Defino, "2024 Regulatory Outlook: OCR to Revise Security, Privacy Rules," *Report on Patient Privacy* 24, no. 1 (January 2024).
2 Jane Anderson, "HHS to Establish Cybersecurity Goals, Seeks Increased HIPAA Penalities" *Report on Patient Privacy* 24, no. 1 (January 2024).
3 Theresa Defino, "HHS Office for Civil Rights 2023 Enforcement Actions," *Report on Patient Privacy* 24, no. 1 (January 2024).
4 U.S. Department of Health and Human Services, "HHS' Office for Civil Rights Settles Multiple HIPAA Complaints With Optum Medical Care Over Patient Access to Records," news release, December 15, 2023, https://bit.ly/3vrIjSB.
5 U.S. Department of Health and Human Services, "Optum Care Resolution Agreement," content last reviewed December 13, 2023, https://bit.ly/4aO3Jcw.
6 Theresa Defino, "BA Depicted by OCR as Example of Ransomware Dangers Recovered Quickly, Didn't Expect Fine," *Report on Patient Privacy* 23, no. 11 (November 2023), https://bit.ly/41W7WqD.
7 U.S. Department of Health and Human Services, "HHS' Office for Civil Rights Settles First Ever Phishing Cyber-Attack Investigation," news release, December 7, 2023, https://bit.ly/4aKtIBH.
8 U.S. Department of Health and Human Services, "Lafourche Medical Group, LLC Resolution Agreement and Corrective Action Plan," content last reviewed December 7, 2023, https://bit.ly/3Rs3DP5.