Report on Patient Privacy Volume 20, Number 10. October 08, 2020 Settlement Involves 'Dark Overlord' Hack, Tip by Breach-Tracking Journalist

By Theresa Defino

September was quite the month for enforcement actions by the HHS Office for Civil Rights (OCR). The agency announced eight settlements totaling more than $10 million. Five of these were released in a batch to show that OCR means business when it comes to covered entities and business associates failing to provide patients access to their records or those of their loved ones.[1]

Two of the five were multimillion-dollar settlements—Premera BlueCross paid $6.85 million and Community Health Systems Inc. paid $2.3 million (see story, p. 1).[2] The third, announced Sept. 21, was with Athens Orthopedic Clinic, which agreed to pay $1.5 million and implement a two-year corrective action plan (CAP).[3]

Even though it was the lesser of the three cases in terms of payment, the circumstances surrounding the Athens settlement are worthy of examining for a variety of reasons, not the least of which is that it's not every day the words "The Dark Overlord" appear in an OCR settlement. Additionally, the settlement can be viewed within the context of comments provided to *RPP* by both OCR Director Roger Severino and by Dissent, a pseudonymous journalist whom OCR credits in the settlement agreement for tipping off Athens that there was a breach. Athens officials and an attorney who signed the settlement agreement did not respond to *RPP*'s requests for comment.

As OCR described it, on June 26, 2016, Dissent, who blogs at the website www.databreaches.net, alerted the practice that patient records that likely belonged to it were online for sale.[4] Two days later, the hacking group The Dark Overlord emailed the practice and "demanded money in return for a complete copy of the database it stole without sale or further disclosure." Alarmingly, access was determined to have begun on June 14 and continued for another month, until July 26, according to OCR. Access had been obtained through a "vendor's credentials," OCR said, and had continued despite the fact that Athens had "terminated the compromised credentials on June 27."

The breach affected 208,557 individuals. "Due to the breadth of system applications affected, a variety of protected health information (PHI) was exposed including patient demographic information (name, date of birth, social security number, etc.), clinical information (reason for visit, 'social history,' medications, test results, medical procedures, etc.), and financial/billing information (health insurance information, payment history)," OCR said.

Agency officials review an entity's overall HIPAA compliance when they begin an investigation and do not focus solely on the event that triggered their inquiry. In this instance, OCR alleged Athens violated seven requirements, and it provided various time frames for when these occurred. The list includes the typical failing of not conducting a risk assessment, but also encompasses a lot more related to basic compliance and privacy policies and procedures.

Indicative of 'Low-Hanging Fruit'

As such, the case stands out as an example for OCR. In response to a question from *RPP* about whether hacks are

preventable, Severino said "low-hanging fruit" has been the target of OCR's enforcement efforts.

"We're focusing on entities, which, for example, are informed by the FBI that they may have been subject to a hack and don't do anything to fix it. There are many cases where entities aren't doing the basics, [which start] with a risk assessment," Severino said. He added that "not everybody falls victim to a hack. There are things you can do to prevent [them]."

RPP noted that the three cases with settlements stemmed from incidents that were several years old and asked Severino whether the agency was currently seeing an increase in cases. Severino said he could "not comment on any existing investigations." He pointed out that OCR officials "have not seen the trend of hacking diminish over the last five years."

According to data OCR shared with *RPP*, 62% of breaches affecting 500 or more individuals reported from January to the end of August of this year stemmed from a hacking or information technology incident. Although not a precise comparison because 2020 data are included, the percentage from this category from 2009 also through the end of August was 33%, OCR data show.

OCR: Policies, Procedures Missing

OCR said Athens failed to:

- Prevent unauthorized access to the individuals' PHI that was breached by The Dark Overlord.
- Maintain copies of its HIPAA policies and procedures. Compliance did not begin until August 2016.
- "Implement sufficient hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use" electronic PHI (ePHI) with noncompliance spanning from Sept. 30, 2015, to Dec. 15, 2016.
- "Enter into business associate agreements with three of its business associates, Quest Records LLC, Total Technology Solutions, and SRS Software LLC"; compliance began Aug. 17, 2017.
- "Provide its entire workforce with HIPAA training"; compliance began Jan. 15, 2018.
- "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by" Athens.
- Implement "security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level."

Athens Accused of Mishandling Breach

As OCR noted, the involvement of The Dark Overlord became known through some detective work published on databreaches.net. In an interview exclusive to *RPP*, the journalist, who blogs anonymously but whose identity *RPP* confirmed, said she was unaware that OCR had pursued this case (or that it would mention her) until she saw the settlement.

She said she was "surprised" to see her website mentioned but found it satisfying, particularly because in her 11 years of running the site and contacting the owners of data that have been breached, she has not always been taken seriously—some accuse her of being the perpetrator of a leak or hack.

Perhaps more gratifying is the fact that a patient whose data was breached contacted her after the settlement was

announced to offer thanks for her efforts.

She also noted that Athens officials drew the ire of patients—and a class-action lawsuit that is still ongoing—when they refused to offer credit monitoring after the breach, saying they could not afford to do so. This statement stands out now that the practice is paying $1.5 million to OCR.

In her view, Athens officials failed to address the hack appropriately after she alerted them to it, saying they were "playing games" and angered the hackers—which she saw herself when the hackers provided her their correspondence with Athens.

Not only was Athens' identifiable data being offered for sale on the dark web, some of it was "dumped" on a public website. What was most "disturbing," the journalist said, was that she personally requested that the data site remove the PHI. Athens, she said, stopped communicating with her after initial contacts.

"Had they talked to me, they might have found out some things sooner and locked down their data sooner," she said.

Multiple Tasks Required Under CAP

Under the terms of the settlement, Athens is required to "review and revise its written policies and procedures," and to specifically address the following:

- "Technical access controls for any and all network/server equipment and systems to prevent impermissible access and disclosure of ePHI,
- "Technical access control and restriction for all software applications that contain ePHI to ensure authorized access is limited to the minimum amount necessary,
- "Technical mechanisms to create access and activity logs as well as administrative procedures to routinely review logs for suspicious events and respond appropriately,
- "Termination of user accounts when necessary and appropriate,
- "Appropriate configuration of user accounts to comply with the Minimum Necessary Rule,
- "Required and routine password changes,
- "Password strength and safeguarding,
- "Addressing and documenting security incidents,
- "Conducting routine, accurate, and thorough risk analyses and implementing corresponding security measures to sufficiently reduce identified risks and vulnerabilities to a reasonable and appropriate level,
- "Workforce training,
- "Documentation of workforce training,
- "Identification of business associates,
- "Engaging in compliant business associate agreements,
- "Breach notification content requirements."

As with other CAPs, Athens must also train workers on policies, submit period implementation reports to OCR and alert it to any HIPAA breaches during the two-year period.

Contact Dissent at breaches@databreaches.net.

1 Theresa Defino, "New Agreements Signal OCR's Impatience With Thwarted Access to Patients' Records," *Report on Patient Privacy* 20, no. 10 (October 2020).
2 Jane Anderson, "Failure to Plug Security Gaps Leads to Large OCR Settlements for Premera, CHSPSC," *Report on Patient Privacy* 20, no. 10 (October 2020).
3 HHS, "Athens Orthopedic HIPAA Resolution Agreement and Corrective Action Plan," resolution agreement, July 7, 2020, https://bit.ly/34sLdoJ.
4 Dissent, "Athens Orthopedic Clinic incident response leaves patients in the dark and out of pocket for protection," August 15, 2016, https://bit.ly/30nQixx.