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."