Report on Patient Privacy Volume 19, Number 5. May 08, 2019 Easy Win for MD Anderson? OCR Drops Annual Caps, Issues Warning on Right-of-Access Denials

By Theresa Defino

Some in the HIPAA compliance community are surely breathing a sigh of relief now that the HHS Office for Civil Rights (OCR) has significantly reduced the amount of penalties it will impose for all but the most serious violations.

But they may have missed a warning OCR Director Roger Severino expressed along with the April 26 announcement that could mean greater legal jeopardy based on a pervasive problem the agency now plans to tackle. Severino stressed during a call with *RPP* and a few other reporters that OCR is serious about sanctioning covered entities (CEs) that don't comply with patients' requests to access their medical records.

And Severino said some access rights violations fall into the "willful neglect" category, the maximum penalty that remains unchanged at $1.5 million per year per violation. OCR has reduced the other three penalty categories significantly.

OCR's decision to use its "enforcement discretion" to lower the annual penalty maximums—in some cases to $25,000 from $1.5 million—follows by just a few weeks a lawsuit the University of Texas MD Anderson Cancer Center filed against HHS. MD Anderson has appealed the imposition of a $4.358 million fine by OCR for breaches in 2012 and 2013 that collectively exposed information about approximately 35,000 individuals. OCR also alleges MD Anderson failed to implement enterprise-wide encryption. In its suit, MD Anderson said the maximum cap should not be the same for all levels of violations, among other arguments ("Should 'State' Agencies Be Exempt From HIPAA? MD Anderson Says Yes," *RPP* 19, no. 5).

In a statement issued to *RPP*, MD Anderson officials acknowledged OCR's turnaround mimics their legal contention and signaled a hope the new penalty calculations could be applied to them.

For OCR's part, Severino said the new penalties reflect "numbers that Congress provided in the HITECH Act itself."

Since an interim final rule was issued in 2009, and then confirmed via a final rule in 2013, OCR has negotiated settlement agreements with CEs and business associates over HIPAA violations based on penalties provided for in the 2009 HITECH Act, but with an interpretation OCR now says was essentially flawed. At the time, HHS said applying a $1.5 annual cap for all four types of violations was "logical" and "appropriate."

Then, as now, penalties are based on the level of knowledge an organization had that there was a violation, and whether it acted to correct the problem within 30 days (referred to as "timely corrected"). The HITECH Act established a range of penalties per violation and annual maximums. The law refers to a "person" being the recipient of the fine, which includes organizations.