Report on Patient Privacy Volume 19, Number 6. June 05, 2019
New OCR Fact Sheet on Business Associates' Liability Part of Move to Dismiss Suit Against HHS

By Theresa Defino

It wasn't the first settlement the HHS Office for Civil Rights (OCR) has had with a business associate (BA) over allegations of HIPAA violations. It's also safe to predict it won't be the last. But one day after announcing a $100,000 agreement with a medical records firm, OCR issued a short "fact sheet on direct liability" of BAs under HIPAA.

Said OCR Director Roger Severino: "We want to make it as easy as possible for regulated entities to understand, and comply with, their obligations under the law."

The settlement with Medical Informatics Engineering (MIE), announced May 23, was triggered by a May 2015 cyberattack that exposed the protected health information (PHI) of 3.5 million individuals. OCR said MIE, among other things, had not conducted a "comprehensive" risk analysis, a requirement that applies equally to it as a BA and to covered entities (CEs) (see story above and "After Settlements, MIE CEO Shares Lessons Learned," *RPP* 19, no. 6).

The settlement was the second OCR announced last month. The first was for $3 million with Touchstone Medical Imaging LLC of Tennessee (see story above and "$3 Million Settlement Demonstrates Need for Quick Breach Management," *RPP* 19, no. 6).

On May 24, OCR issued the fact sheet, which it said "provides a clear compilation of all provisions through which a business associate can be held directly liable for compliance with certain requirements" of the various HIPAA rules. It did not make reference to the Touchstone settlement, but various media reports linked the two.

But *RPP* has learned the fact sheet is playing a prominent role in HHS' attempt to win dismissal of a lawsuit filed against it last year by Ciox Health LLC, the nation's largest medical records retrieval firm. Ciox filed suit against HHS 18 months ago, seeking relief from enforcement actions it said OCR was threatening to take against it ("Medical Records Firm Sues HHS Over Access Fees, Seeks Return to System Under State Laws," *RPP* 18, no. 2).

OCR was granted the authority to pursue direct enforcement action against BAs as a result of the 2009 HITECH Act, which OCR codified in a 2013 final rule. But BAs are not required to comply with some provisions in the security, privacy and breach notification rules.