Report on Medicare Compliance Volume 32, Number 42. November 20, 2023

Business Associate Settled Case Over Ransomware, Said OCR Was 'Heavy Handed'

By Theresa Defino

Tim DiBona clearly remembers Christmas Eve 2018 when the staffers of his small firm—Doctors' Management Services (DMS)—arrived at their West Bridgewater, Mass., office to find their computer system down. "We realized right away what was happening—that it was a ransomware attack," he recalled. The demand for $20,000 was uncovered, but with backup records, no payment was necessary.

"We kicked the perpetrator out, we restored our backups," said DiBona, CEO of the business his mother, Barbara, founded in their garage 35 years ago. "The following day was Christmas. The day after that, we were back in the office. Everything was fine." DMS, a business associate (BA), hired forensic experts to investigate the attack, later learning it had been infiltrated in 2017, apparently one of the first U.S. victims of "GandCrab" ransomware.

DMS, whose CFO is Tim's brother, Rich, notified some 290,000 patients whose records it held as part of its billing, practice management, provider credentialing and related services firm. It set up a call center, offering patients credit monitoring services. In April 2019, DMS also filed a breach report with the HHS Office for Civil Rights (OCR). Thus began a saga that became public when OCR announced Oct. 31 that DMS had agreed to pay $100,000 and implement a three-year corrective action plan (CAP) to resolve alleged HIPAA violations.[1]

OCR portrayed DMS as the poster child for the dangers of ransomware, and noted the settlement "marks the first ransomware agreement OCR has reached."