

Report on Patient Privacy Volume 23, Number 11. November 09, 2023 BA Depicted by OCR as Example of Ransomware Dangers Recovered Quickly, Didn't Expect Fine

By Theresa Defino

Tim DiBona clearly remembers Christmas Eve 2018 when the staff of his small firm—Doctors' Management Service (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 on 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, noting it is a "type of malware (malicious software) designed to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid." OCR noted the settlement "marks the first ransomware agreement OCR has reached."

But, in an extensive interview with RPP, Tim DiBona disputed OCR's depiction of DMS and expressed shock, as well as disappointment, that OCR took formal enforcement action against DMS. He described the nearly five-year process of getting to the resolution as "frustrating" and, at times, "terrifying." OCR did not respond to RPP's questions about the investigation and settlement.

DiBona felt so strongly that DMS—which has eight employees—had acted appropriately in response to the breach and its prior compliance efforts that he asked OCR not to mention the company name in the settlement announcement—something the agency obviously did not agree to.

This document is only available to subscribers. Please log in or purchase access.

[Purchase Login](#)