COSMOS
Navigate the Compliance Universe

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.

The $100,000 penalty was also significantly higher than DMS felt it should pay. OCR, however, wanted to impose a higher fine—DiBona said he couldn't recall the exact amount. He counteroffered $30,000, but $100,000 was the lowest the agency would go, DiBona said.

According to OCR, the "unauthorized party" entered DMS' network on April 1, 2017, and "deployed ransomware" a year later on Christmas Eve, when the staff discovered it, as DiBona also described to *RPP*.[2]

DiBona said the hacker got in through a "remote desktop connection," which was an area where DMS actually tightened up access, coincidentally, in 2018, before it knew the perpetrator was already inside.

"We had already cancelled the VPN [virtual private network], but they had already started jumping from computer to computer. It took them [time], but once they got to our server, that's when they shut everything down," DiBona said, relaying what forensic investigators told him.

Announced Oct. 31, OCR Director Melanie Fontes Rainer said the agreement "highlights how ransomware attacks are increasingly common and targeting the health care system. This leaves hospitals and their patients vulnerable to data and security breaches. In this ever-evolving space, it is critical that our health care system take steps to identify and address cybersecurity vulnerabilities, along with proactively and regularly review risks, records, and update policies. These practices should happen regularly across an enterprise to prevent future attacks."

In the announcement, OCR shared data about ransomware, stating that "in the past four years, there has been a 239% increase in large breaches reported to OCR involving hacking and a 278% increase in ransomware. This trend continues in 2023, where hacking accounts for 77% of the large breaches reported to OCR. Additionally, the large breaches reported this year have affected over 88 million individuals, a 60% increase from last year."

OCR didn't discuss how DMS handled the attack—such as the fact that no ransom was paid and disruption to the business was minimal. DiBona also told *RPP* there have been no reports of fraud, identity theft or other misuse of DMS's records.

"We were very happy about that because there was certainly…the potential, but I don't think this perpetrator really knew what they had in their possession at the time." DiBona added that he's always been a "big hawk" about medical privacy, even making YouTube videos for organizations like his because "HIPAA education typically is much more focused on hospitals and medical practices."

OCR Alleged Four Violations

OCR's announcement "makes it seem like we were fumbling, and that was never the case. It wasn't the case before this. And it's never been what we've been about. We've always been very respectful and focused on the safety of the patient data," DiBona said.

So much time has passed since the attack that there's now free decryption software available to recover from GandCrab—though, as noted, DMS had backups and didn't need to decrypt its data. Moreover, through a four-year, global operation involving 17 countries—codename: Operation Quicksand—seven individuals affiliated with the ransomware were arrested, and their network was disrupted.

OCR accused DMS of four violations of the Security Rule—the first being access into its systems and the deployment of ransomware. Secondly, "DMS failed to conduct an accurate and thorough risk analysis that assesses technical, physical, and environmental risks and vulnerabilities associated with handling" electronic protected health information (ePHI).

Further, DMS "failed to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports," OCR said, and "failed to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule."

DiBona told *RPP* he disagreed with these findings and that his firm provided OCR with documentation to verify its actions.

Over the years since OCR initiated the investigation—which the agency said began April 22, 2019—three or four different officials were in contact with DMS, DiBona said. Some requested documents he had already sent or

similar ones but for different date ranges. There were also periods where there was no correspondence from the agency for months; then communication would start again. DiBona lamented that he wasn't able to meet or talk on the phone with anyone from OCR; the entire investigation was conducted via email, he said.

DMS supplied OCR—at its request—its financial records so it could assess the company's ability to pay a fine. In the past, former OCR directors have said penalties are meant to be an appropriate sanction but not designed to close a business or practice.

DMS: OCR Asked About Insurance

It wasn't until "at the very end...probably just shy of five years of going back and forth with them, showing them what we're doing, showing them what we're continuing to do, and trying to explain what had happened in the past," he said when OCR officials said, "there's going to be a fine, and this is the amount that we're looking for."

OCR officials asked him if he had an insurance policy that might cover a fine, and if so, how much coverage was left, DiBona said.

"I'm not saying we were perfect, but a six-figure hit for a small business was certainly significant," DiBona said. "If we didn't have coverage, we would have been put right out of business with that."

He said he expected, if there was a sanction, that it would be "more of a slap on the wrist or a strong censure or... oversight for three years" related to the kind of activities spelled out in the CAP.

"It would be one thing if we were being defiant or criminal [but] that wasn't really the case. We were very responsible prior to this and through this" investigation," DiBona said. "It was surprising not only that it was dragged on for five years but also that we got hit with a massive fine. When all was said and done, [it] was very difficult to deal with, especially as a small company."

DiBona said he "did request for us to work together [with OCR], but they just ended up giving us the [CAP]. It seemed like they weren't familiar even after five years with what we're actually doing right now and what's appropriate for our version of health care management."

As OCR summarized, under the three-year CAP, DMS must:

- "Review and update its Risk Analysis to identify the potential risks and vulnerabilities to Doctors' Management Services data to protect the confidentiality, integrity, and availability of electronic protected health information.
- "Update its enterprise-wide Risk Management Plan (strategy to protect the confidentiality, integrity, and availability of ePHI) to address and mitigate any security risks and vulnerabilities found in the updated Risk Analysis.
- "Review and revise, if necessary, its written policies and procedures to comply with the Privacy and Security Rules.
- "Provide workforce training on HIPAA policies and procedures."

Long Process Spurred Fear

DiBona said some CAP requirements "might be difficult from a financial perspective" but added that DMS has the "drive to work on this and make sure we satisfy it."

Now that the settlement has been finalized—despite being unhappy with the $100,000 payment—DiBona feels some relief.

"It's been an extremely stressful five years. [DMS is] very much like a family. We all just got done doing pumpkin carvings and a Halloween costume contest. It's a very tight crew here. Whenever you're facing a situation where someone could potentially lose their jobs for, on their side, not doing anything wrong, it's scary," DiBona said. "You're not only responsible for your own livelihood, but also the livelihood of your employees. This whole time, you're worried at any moment you're just gonna get that email that says, 'You're gonna get this nasty fine and you have to close your doors.' It's a terrifying experience."

He also has concerns that OCR's "heavy-handed" approach sends a "disincentive message" to other entities to not report breaches. In his view, OCR "beat somebody up who was really the victim of somebody else's assault."

1 U.S. Department of Health and Human Services, "HHS' Office for Civil Rights Settles Ransomware Cyber-Attack Investigation," news release, October 31, 2023, https://bit.ly/3slY2Bi.
2 U.S. Department of Health and Human Services, "Doctors' Management Services, Inc. Resolution Agreement and Corrective Action Plan," content last reviewed October 31, 2023, https://bit.ly/3SoxmdR.