COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 28, Number 31. September 09, 2019
After FBI Detects Spyware, Health System Faces OCR, Adds Controls

By Nina Youngstrom

The FBI broke the bad news to University of Virginia (UVA) Health in Charlottesville two days before Christmas two years ago: One of its computers was among the thousands infected by malware called Fruitfly. It wasn't a whodunit because the FBI knew 28-year-old Ohio hacker Phillip Durachinsky had targeted the Mac computers through spyware that enabled him to open a microphone and camera and observe computer screens, download images and log keystrokes. "It was basic spyware. It was insidious," said Regina Verde, chief compliance officer and privacy officer at UVA Health, which includes a medical center, school of medicine and university physicians group. But how?

So began an internal forensic investigation and risk assessment, with privacy and security working hand in hand to unravel the hack, followed by breach notification and an OCR privacy and security investigation. When the dust settled, UVA Health strengthened its safeguards, which was a learning experience. Recovery from Fruitfly was "truly a joint effort," Verde said.

The first part of the big reveal came from the FBI, which determined that Durachinsky got inside UVA Health's network through a virtual private network (VPN). The notification was sent to UVA Health's chief information security officer (CISO), who passed the information to Verde and Erin Trost, UVA Health's information security manager. VPNs offer employees and physicians remote access to UVA Health computers. "We allow personal devices to connect to our network, and at that point we were able to take an IP address and host name and tie it to an individual," said Trost, who spoke with Verde at the Health Care Compliance Association's Compliance Institute in April. "That started our initial investigation."

The individual turned out to be a UVA Physician Group surgeon who was also an attending physician at the medical center. It was not the most comfortable situation; "try asking a busy surgeon" to turn over four of his Macs without being able to fully explain why, Verde said. "We met with a great deal of resistance" until the chief medical officer intervened. "We got all his devices sequestered." The surgeon also was interviewed (e.g., "Were there any indications you had malware on your machines?"), Trost said.