COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 23, Number 2. February 09, 2023 FBI Breach Alert Helped Spur New Path for Owensboro Health

By Jane Anderson

For the chief information security officer (CISO) of Owensboro Health, a 2015 breach—notice of which came courtesy of the FBI—served in part as a wakeup call that the organization needed to take a more global approach to risk management.

"No one wants the dreaded FBI call telling them that they've detected suspicious network activity involving a third party on their network," said Jackie Mattingly, CISO for the Owensboro, Kentucky-based health system. "However, that's what happens."

Owensboro Health, with more than 4,800 employees, serves an 18-county area in western Kentucky and southern Indiana and includes a centrally located hospital with 477 beds, three outpatient locations and a health park.

In September 2015, the FBI notified Owensboro that it had identified suspicious activity on the health system's network involving third parties at Muhlenberg Community Hospital in Greenville, Kentucky, which Owensboro had acquired about two months prior to the attack notification, Mattingly told a webinar audience in an event sponsored by Clearwater Compliance.[1]

The forensic investigation indicated that cyberattackers had used a keystroke logger to capture and transmit patient data as it was entered into certain computers, Mattingly said. "We discovered that we had several computers that were affected with a keystroke logger." The infection may have dated as far back as 2012, long before Owensboro purchased the Muhlenberg facility.

Potentially compromised information included: patient names, addresses, telephone numbers, birth dates, Social Security numbers, driver's license numbers, medical and health plan information, financial information, payment card information and information about people responsible for paying patients' bills. The breach impacted some 85,000 patients.

"Of course, this put us on the dreaded OCR [Office for Civil Rights] Wall of Shame, and consequently led us right into an OCR investigation," Mattingly said, adding that the organization brought in Clearwater to help Owensboro conduct risk analysis and mock OCR audits. "We did gap assessments against the HIPAA Security Rule as well as the privacy and breach rule."