Report on Medicare Compliance Volume 29, Number 15. April 20, 2020

Hackers Exploit Pandemic With COVID-Specific Phishing; 'Humans Are the Weakest Link'

By Nina Youngstrom

When hordes of employees headed home to work as the coronavirus spread, there was a hospital surge of another kind: a sudden increase in the number of employees who needed laptops and/or licensing of software and training on how to use the technology. The potential for security lapses is greater, especially for employees who use home computers, at least temporarily.

"For some organizations, having employees working remotely can be a nightmare for security," said the director of information security at a health system, who preferred not to be identified. The health system, which includes a hospital and physician clinics, has addressed that a couple of ways, he said. Employees who received a company laptop are directly connected through a virtual private network (VPN) to the network when they log in, which is preferable. Not enough laptops were available for the entire virtual workforce, however, so some employees use their own computers. To access the network, they must use a Citrix Gateway client, which gives employees a secure connection to the network to access applications or virtual desktop instances. "It creates a tunnel to our [system]," the information security director said. "It only allows employees to run certain programs, and they can't grab files from their personal computer." Ultimately, however, computer systems are only as secure as the people using them. "Humans are the weakest link," he noted. "All we can do is educate, hope it sinks in and monitor."