COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 33, Number 14. April 15, 2024
Hackers Increasingly Go After Patients to Try to Get Entities to Pay Ransom

By Jane Anderson

Cybercriminals—potentially frustrated by their ability to extort ransom from health care entities in attacks—have started extorting the patients themselves, threatening them with the release of information or embarrassing photos online, or other forms of harassment, experts said.

The tactics cropped up in multiple attacks in late 2023 and likely will accelerate this year, said Michael Hamilton, co-founder of Critical Insight and former City of Seattle chief information security officer. "This tactic doesn't seem to be going away," Hamilton said during a recent webinar.[1] "This seems to be a new business model."

A recent attack took place at Oklahoma City-based Integris Health. In that incident, some patients were contacted in December by apparent hackers who claimed to have stolen their personal information and threatened to post it on the dark web.[2]

"In November, Integris Health, based in Oklahoma, had a ransomware attack," said Jake Milstein, chief marketing officer for Critical Insight, at the webinar. He said the hackers sent an email to Integris patients on Christmas eve that said: "We've contacted Integris Health, but they refuse to solve this issue. We give you the opportunity to remove your personal data from our databases before we sell the entire database to data brokers on January 5th, 2024."

Patients were told they could pay $3 to view the information and $50 to remove it, Milstein said.

Patients Threatened With Swatting

Hamilton said that this represented "double-dipping" by those conducting the ransomware attack: first, the bad actors exfiltrate the data and then they can install malware on the system. "So, having that data is an ace in the hole, right? If you have a ransom that you refuse to pay, now you can extort the entity whose data was stolen. Now, of course, they're going one step further and leaning into the people whose data was stolen themselves."

In an incident that occurred during the same general time frame at Fred Hutchinson Cancer Center in Seattle, patients received emails purportedly from the alleged hackers stating that their data had been stolen and "will soon be sold to various data brokers and black markets to be used in fraud and other criminal activities," according to emails seen by *The Seattle Times*, which broke the story.[3]

The email said those responsible for the ransomware attack had already been in contact with Fred Hutchinson, but the cancer center "refused to make a deal." Fred Hutchinson said it had emailed patients urging them not to send any money to the cybercriminals and report the emails to the FBI's internet crime center.

Ultimately, some patients also received swatting threats, in which the purported hackers warned people that they needed to pay a fee or they would be swatted, Hamilton said. In swatting, bad actors call the authorities with a fake report of a bomb threat or shooting at the victim's location in the hope that heavily armed law enforcement

officers will show up at the victim's door.

Bad actors also leverage nude photos of patients to extort CEs, Milstein said. For example, Lehigh Valley Health was hit by ransomware in February 2023, and "the criminals then released photos of nude female cancer patients to try to get the organization to pay," he said.[4]