COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 24, Number 4. April 11, 2024
Hackers Increasingly Leveraging Threats to Patients to Pressure Health Organizations to Pay Ransom

By Jane Anderson

Cyberhackers—potentially frustrated by their limited 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 even with other forms of harassment, such as multiple spam emails or threats to send law enforcement to their homes, 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."

One of the most recent attacks 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, to webinar attendees. "In December, criminals started emailing Integris patients. The email 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.' And by the way, they sent this on Christmas eve."

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

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]