Cyberattack leaves health care providers reeling weeks later

March 13 2024, by Robin Foster

Following a cyberattack on the largest health insurer in the United States last month, health care providers continue to scramble as insurance payments and prescription orders continue to be disrupted and

physicians lose an estimated $100 million a day.

That estimate was generated by First Health Advisory, a cybersecurity firm that specializes in the health industry, according to the American Medical Association (AMA).

"This massive breach and its wide-ranging repercussions have hit physician practices across the country, risking patients' access to their doctors and straining viability of medical practices themselves," AMA President Dr. Jesse Ehrenfeld said in a news release.

"Against the backdrop of persistent Medicare cuts, rising practice costs and spiraling regulatory burdens, this unparalleled cyberattack and disruption threatens the viability of many practices, particularly small practices and those in rural and underserved areas," he added. "This is an immense crisis demanding immediate attention."

How did the crisis begin?

The security breach was first detected on Feb. 21 at Change Healthcare, part of Optum Inc., which is in turn owned by UnitedHealth Group.

In a report filed that day with the U.S. Securities and Exchange Commission, UnitedHealth Group told government officials that it had been forced to sever some of Change Healthcare's vast digital network from its clients. It hasn't yet been able to restore all of those services.

In its latest update on the attack, Change Healthcare said the company is working to get the provider payment systems back up by the middle of March.

"UnitedHealth Group continues to make substantial progress in mitigating the impact to consumers and care providers of the

unprecedented cyberattack on the U.S. health system and the Change Healthcare claims and payment infrastructure," the company said in a statement.

"We are committed to providing relief for people affected by this malicious attack on the U.S. health system," UnitedHealth CEO Andrew Witty added in the statement. "All of us at UnitedHealth Group feel a deep sense of responsibility for recovery and are working tirelessly to ensure that providers can care for their patients and run their practices, and that patients can get their medications. We're determined to make this right as fast as possible."

Until then, the effects on patients and doctors alike continues.

"This is by far the biggest ever cybersecurity attack on the American healthcare system ever," Dr. Céline Gounder, an editor-at-large for public health at KFF Health News and a *CBS News* medical contributor, said Tuesday. "This is a system, Change Healthcare, that processes medical payments and touches one out of every three patients in this country. So the magnitude of the scope of this attack is really quite large."

Gounder explained that a provider's ability to bill and process things like prior authorizations have been hampered since the cyberattack.

"Can you get those medications? Can you get an estimate, say, on a surgery that you want to schedule? What is that going to look like in terms of your insurance coverage, and so on. All of those kinds of things are being affected," she told *CBS News*.

It's also affecting patients' ability to fill their prescriptions at some hospitals.

"Here, for example, we're only able to give some patients only two weeks of refill," Gounder said. "So, it means that they may need to come back over and over again. And some patients are even having to pay out of pocket for their refills."

Two weeks after the attack, the federal government stepped in to help.

On March 5, the U.S. Department of Health and Human Services announced several assistance programs for health providers who have been affected.

"The government is trying to create some supports for health care systems—not directly supporting patients, but the systems," Gounder explained. "This is because without revenue coming in through the billing process, you don't have money to make payroll to be able to pay your doctors and your nurses and your janitors and all the staff that you need to run a health care system."

The attack is also interfering with the ability to order needed medications and supplies, she adds.

"So the idea is to try to help support health care systems through this, but especially Medicaid providers, those who have less of a buffer, so to speak, financially—they're really in deep trouble here," Gounder said.

Unfortunately, this cyberattack will likely not be the last: Federal officials estimate that large breaches of health care data have nearly doubled from 2018 to 2022.

More information: Visit HealthIT.gov for more on health information security.