HHS opens investigation into UnitedHealth cyberattack

March 14 2024, by Robin Foster

Following a cyberattack on one of the nation's largest health insurers that's thrown health care payments into disarray and likely exposed reams of private patient data, the U.S. Department of Health and Human Services said Wednesday it has begun an investigation into the incident.

In a statement, the HHS Office for Civil Rights (OCR) said it plans to focus on assessing the extent of the breach and whether UnitedHealth Group and its affected subsidiary, Change Healthcare, took adequate steps to protect patient data under the Health Insurance Portability and Accountability Act (HIPAA).

"Given the unprecedented magnitude of this cyberattack, and in the best interest of patients and health care providers, OCR is initiating an investigation into this incident," the statement said.

Still, the OCR acknowledged the problem is not unique to UnitedHealth.

"Ransomware and hacking are the primary cyber-threats in health care," the statement noted. "Over the past five years, there has been a 256% increase in large breaches reported to OCR involving hacking and a 264% increase in ransomware... The large breaches reported in 2023 affected over 134 million individuals, a 141% increase from 2022."

Health care companies can be penalized for those breaches: In 2020, Anthem paid a $16 million settlement following a 2015 data breach that exposed the protected health information of 79 million people, the Washington Post reported.

UnitedHealth told the Post that it will cooperate with the HHS investigation.

"Our immediate focus is to restore our systems, protect data and support those whose data may have been impacted," the company said in a statement. "We are working with law enforcement to investigate the extent of impacted data."

One health care expert applauded the HHS move.

HHS is "doing the right thing by investigating the root cause and location of the fallout from this serious hack while letting providers focus on getting back on track and ensuring that patient care doesn't suffer," Chip

Kahn, CEO of the Federation of American Hospitals, told the Post.

Meanwhile, health care providers are still scrambling 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.

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.

"We are committed to providing relief for people affected by this malicious attack on the U.S. health system," UnitedHealth CEO Andrew Witty said in the update. "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 lingers.

"This is by far the biggest ever cybersecurity attack on the American health care 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.

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.

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

Citation: HHS opens investigation into UnitedHealth cyberattack (2024, March 14) retrieved 27 April 2024 from https://medicalxpress.com/news/2024-03-hhs-unitedhealth-cyberattack.html