CYBERATTACK ON OPTUM UNIT DISRUPTS PRESCRIPTION ORDERS

**By Reed Abelson**

A cyber attack on a unit affiliated with UnitedHealthcare, he nations’ largest insurer, has disrupted drug prescription orders at thousands of pharmacies for nearly a week.

The assault on the unit, Change Healthcare, a division of United’s Optum, was discovered last Wednesday. The attack appeared to be by a foreign country, according to two senior federal law enforcement officials, who expressed alarm at the extent of the disruption on Monday.

UnitedHealth Group, the conglomerate, said in a federal filing that it has been forced to disconnect some of Change Healthcare’s vast digital network from its clients, and as of Monday, had not been able to restore all of those services.

Change handles some 15 billion transactions a year representing as many as one of three U.S. patient records and involving not just prescriptions but denial, clinical and other medical needs. The company was acquired by UnitedHealth Group for $13 billion in 2022.

This latest attack underscores the vulnerability of health care data, especially patients’ personal information, including their private medical records. Hundreds of breaches at hospitals, health plans and doctors’ offices are being investigated, according to federal records.

In this case, the disturbance has been widespread, including for U.S. military overseas. Change acts as a digital intermediary to help pharmacies verify a patient’s insurance coverage for their prescriptions, and some reports indicate that people have been forced to pay in cash.

Last week, after UnitedHealth found what it described as “a suspected nation-state associated cybersecurity threat actor” targeting Change, the company shut down several services, including those allowing pharmacies to quickly check what a patient owes for a medication. Some hospitals and physician groups that rely on Change for billing to get paid may also be affected.

Large drugstore chains like Walgreens say that the effects have been limited, but many smaller outfits say that they rely on Change whenever they handle a prescription for someone with insurance.

“For the last week, it has been hit or miss about whether we can take care of patients,” said Dared Price, who operates seven pharmacies in Kansas. While patients can pay cash if the medication is inexpensive, he says that some of his customers have been unable o obtain more costly treatments for flue or Covid because heir insurance status is unclear.

“It’s a debate,” he said.

Tricare, which covers the U.S. military, said its pharmacies in the United States and abroad are being forced to fill prescriptions manually. It continues to warn people this week of possible delays in getting medications.

Details about the attack, including whether any personal patient information has been stolen, are limited. Change has been making brief periodic updates on its website. On Monday, the company reiterated that the affected services would likely be unavailable for at least another day. It also emphasizes that it had a “high-level of confidence” that other parts of United’s businesses were not targeted in the attack.

But there’s little question that United, whose sprawling businesses touch nearly every aspect of health care, made for a particularly rich target.

“If you’re going to go after stealing records, you want to go after the biggest pot of record you can get,” said Fred Langston, the chief product officer for Critical Insight, a cybersecurity firm. “You’re literally hitting the jackpot.”

The motives of the attacker are not yet known, Mr. Langston said.

It may involve ransomware, allowing culprits to demand some sort of ransom. The intent may also have been to throw the healthcare system into disarray by making it harder to fill prescriptions or to bill for care in a timely manner.

“You have a concentration of mission-critical services for the entire sector, which represents a concentration of risk,” said John Riggi, the national adviser for cybersecurity and risk for the American Hospital Association. It has been advising hospitals to be careful about connecting to Change or affiliated businesses.

“The industry has seen an increasing number of these kinds of assaults”, said Cliff Steinhauer, director of information security and engagement at the National Cybersecurity Alliance, a non-profit group.

According to federal officials large breaches of health care data have nearly doubled from 2018 to 2022, including a spike in the number involving ransomware. Patients have had to go to different facilities, resulting in delays in care, according to a recent report.

Under federal law, patients must eventually be notified if their information is the subject of some sort of breach, Mr. Steinhauer said. People will be alerted even if their information does not appear to have become publicly available.

“It is worse if we find out that information is for sale on the dark web,” he said.