Hacking at UnitedHealth unit cripples a swath of the US health system: What to know

March 4 2024, by Darius Tahir, KFF Health News

Credit: Pixabay/CC0 Public Domain

Early in the morning of Feb. 21, Change Healthcare, a company unknown to most Americans that plays a huge role in the U.S. health system, issued a brief statement saying some of its applications were

"currently unavailable."

By the afternoon, the company described the situation as a "cyber security" problem.

Since then, it has rapidly blossomed into a crisis.

The company, recently purchased by insurance giant UnitedHealth Group, reportedly suffered a cyberattack. The impact is wide and expected to grow. Change Healthcare's business is maintaining health care's pipelines—payments, requests for insurers to authorize care, and much more. Those pipes handle a big load: Change says on its website, "Our cloud-based network supports 14 billion clinical, financial, and operational transactions annually."

Initial media reports have focused on the impact on pharmacies, but techies say that's understating the issue. The American Hospital Association says many of its members aren't getting paid and that doctors can't check whether patients have coverage for care.

But even that's just a slice of the emergency: CommonWell, an institution that helps health providers share medical records, information critical to care, also relies on Change technology. The system contained records on 208 million individuals as of July 2023. Courtney Baker, CommonWell marketing manager, said the network "has been disabled out of an abundance of caution."

"It's small ripple pools that will get bigger and bigger over time, if it doesn't get solved," Saad Chaudhry, chief digital and information officer at Luminis Health, a hospital system in Maryland, told KFF Health News.

Here's what to know about the hack:

Who did It?

Media reports are fingering ALPHV, a notorious ransomware group also known as Blackcat, which has become the target of numerous law enforcement agencies worldwide. While UnitedHealth Group has said it is a "suspected nation-state associated" attack, some outside analysts dispute the linkage. The gang has previously been blamed for hacking casino companies MGM and Caesars, among many other targets.

The Department of Justice alleged in December, before the Change hack, that the group's victims had already paid it hundreds of millions of dollars in ransoms.

Is this a new problem?

Absolutely not. A study published in *JAMA Health Forum* in December 2022 found that the annual number of ransomware attacks against hospitals and other providers doubled from 2016 to 2021.

"It's more of the same, man," said Aaron Miri, the chief digital and information officer at Baptist Health in Jacksonville, Florida.

Because the assaults disable the target's computer systems, providers have to shift to paper, slowing them down and making them vulnerable to missing information.

Further, a study published in May 2023 in *JAMA Network Open* examining the effects of an attack on a health system found that waiting times, median length of stay, and incidents of patients leaving against medical advice all increased—at neighboring emergency departments. The results, the authors wrote, mean cyberattacks "should be considered a regional disaster."

Attacks have devastated rural hospitals, Miri said. And wherever health care providers are hit, patient safety issues follow.

What does it mean for patients?

Year after year, more Americans' health data is breached. That exposes people to identity theft and medical error.

Care can also suffer. For example, a 2017 attack, dubbed "NotPetya," forced a rural West Virginia hospital to reboot its operations and hit pharma company Merck so hard it wasn't able to fulfill production targets for an HPV vaccine.

Because of the Change Healthcare attack, some patients may be routed to new pharmacies less affected by billing problems. Patients' bills may also be delayed, industry executives said. At some point, many patients are likely to receive notices their data was breached. Depending on the exact data that has been pilfered, those patients may be at risk for identity theft, Chaudhry said. Companies often offer free credit monitoring services in those situations.

"Patients are dying because of this," Miri said. Indeed, an October preprint from researchers at the University of Minnesota found a nearly 21% increase in mortality for patients in a ransomware-stricken hospital.

How did it happen?

The Health Information Sharing and Analysis Center, an industry coordinating group that disseminates intel on attacks, has told its members that flaws in an application called ConnectWise ScreenConnect are to blame. Exact details couldn't be confirmed.

It's a tool tech support teams use to remotely troubleshoot computer problems, and the attack is "apparently fairly trivial to execute," H-ISAC warned members. The group said it expects additional victims and advised its members to update their technology. When the attack first hit, the AHA recommended its members disconnect from systems both at Change and its corporate parent, UnitedHealth's Optum unit. That would affect services ranging from claims approvals to reference tools.

Millions of Americans see physicians and other practitioners employed by UnitedHealth and are covered by the company's insurance plans.

UnitedHealth has said only Change's systems are affected and that it's safe for hospitals to use other digital services provided by UnitedHealth and Optum, which include claims filing and processing systems.

But not many chief information officers "are jumping to reconnect," Chaudhry said. "It's an uneasy feeling."

Miri says Baptist is using the conglomerate's technology and that he trusts UnitedHealth's word that it's safe.

Where's the Federal Government?

Neither executive was sanguine about the future of cybersecurity in health care. "It's going to get worse," Chaudhry said.

"It's a shame the feds aren't helping more," Miri said. "You'd think if our nuclear infrastructure were under attack the feds would respond with more gusto."

While the departments of Justice and State have targeted the ALPHV group, the government has stayed behind the scenes more in the aftermath of this attack. Chaudhry said the FBI and the Department of

Health and Human Services have been attending calls organized by the AHA to brief members about the situation.

Miri said rural hospitals in particular could use more funding for security and that agencies like the Food and Drug Administration should have mandatory standards for cybersecurity.

There's some recognition among officials that improvements need to be made.

"This latest attack is just more evidence that the status quo isn't working and we have to take steps to shore up cybersecurity in the health industry," said Sen. Mark Warner (D-Va.), the chair of the Senate Select Committee on Intelligence and a longtime advocate for stronger cybersecurity, in a statement to KFF Health News.

If you're caught in a cybersecurity breach, here are steps to take:

- Monitor the notices and bills you receive from insurers and providers. Contact them immediately if anything seems suspicious.
- If a medical provider requests your Social Security number on intake forms, leave the space blank, and politely push back if they insist.
- If your health plan offers free credit or identity theft monitoring following a breach, take it.

If you're concerned your data has been compromised:

- Go to the Federal Trade Commission's identity theft site to file an identity theft report, if appropriate.
- If someone used your name to get medical care, contact every provider who may have been involved and get copies of your

medical records. Correct any errors.
- Notify your health plan's fraud department and send a copy of the FTC identity theft report.
- File free fraud alerts with the three major credit reporting agencies.