What Home-Based Care Providers Should Learn from Change Healthcare, Ascension Cyberattacks

By **Joyce Famakinwa**

When news of the Change Healthcare cyberattack became public, it rocked the broader health care sector. Months later, it serves as a major lesson for home-based care providers.

In February, Change Healthcare – the largest U.S. billing and payment system in the country, and a subsidiary of UnitedHealth Group (NYSE: UNH) – was brought to a screeching halt as the result of a cyberattack.

Change Healthcare works with payers, providers and patients — delivering revenue and overseeing payment cycle management. The ransomware attack made it difficult for thousands of providers to bill, significantly impacting cash flows in the process.

UnitedHealth Group would go on to pay the cyber hackers roughly $22 million, according to reports from WIRED.

In March, UnitedHealth Group rolled out a Temporary Assistance Funding Program for providers.

During the same month, Senator Mark Warner (D-Va.) introduced the Health Care Cybersecurity Improvement Act of 2024. The legislation gives providers financial incentive to keep up with cybersecurity standards.

“I’ve been sounding the alarm about cybersecurity in the health care sector for some time. It was only a matter of time before we saw a major attack that disrupted the ability to care for patients nationwide,” Warner said in a press statement. “The recent hack of Change Healthcare is a reminder that the entire health care industry is vulnerable and needs to step up its game.”

In April, Axios reported that the Change Healthcare hackers had begun to leak parts of the stolen data.

More recently, Ascension Healthcare Network revealed that it was the victim of a cyberattack in May. The health system noticed “unusual activity” in its network systems which lead to the unavailability of electronic health records systems, patient portals and more, Ascension stated in a press release.

As one of the largest private health systems in the U.S., Ascension has 140 hospitals across the country.

In the aftermath of these major cyberattacks, the Department of Health and Human Services’ (HHS) research funding agency announced that it would throw more than $50 million behind hospital cybersecurity.

Overall, the department noted that there's been a 256% hike in large breaches, and a 264% increase in ransomware reported to its Office for Civil Rights.

One major takeaway for home-based care providers is that any organization can be the victim of a cyberattack.

"No entity is immune to cyberattacks, no matter how sophisticated their firewalls or software are," Barbara B. Citarella, the founder of the health care consulting firm RBC Limited, told Home Health Care News in an email.

Further compounding matters, hackers have become more aggressive.

"[Cyberattackers] are getting more bold, and even going after what I call critical systems, or patient safety organizations, which is very concerning for all of us," Ben DeBow, founder of Fortified, told HHCN. "It's potentially impacting a person's life, or the safety of others. It's very alarming to us."

DeBow pointed out that providers that are most vulnerable to cyberattackers are the ones with outdated legacy systems with old codes and processes. He noted that this places patients and personal data at risk.

"A lot of these players only need to find one hole in the boat to get in," he said. "Once they're in, they can navigate around. If you're running on an unsupported legacy platform, then that is not under support anymore. That is a common way into a lot of organizations. Some recent ones came in on a company that were running Windows Server 2003. That's a very old platform."

Sometimes smaller home-based care providers don't earmark funds in their budget that will allow them to compete with sophisticated cyber attackers.

DeBow believes that investing in cyber security should be a priority.

"You have to really enable security service providers in the technology space to be able to really stand a chance of competing and keeping your infrastructure secure," DeBow said. "Health care is good at health care, security services are going to be good at security. That's why you want to buy their service versus trying to build that out."

Citarella emphasized the importance of conducting annual cybersecurity assessments and educating staff.

She also noted that providers should be frequently updating passwords, have multi-factor authentication in place and perform exercises and drills to test backup systems. Providers should also implement clear policies and procedures of what to do when a cyber event occurs.

"People will share what type of attacks are going on around the globe, as they're happening, from the FBI and all these other organizations," DeBow. "They're sharing and collating that information together. Make sure you're watching what the next attack is because the play that I did today on the football field, I'm not going to do that same play tomorrow. I'm going to create another play, and then we have to be ready for that."

Ultimately, DeBow believes that a mixture of people and technology-based processes and policies will help lower risk.

"A lot of times when we think about cyber, we think of all Star Wars and all of these advanced things, but it goes back down to the basics," he said.