A large US health care tech company was hacked. It's leading to billing delays and security concerns

March 1 2024, by Devna Bose

Pages from the United Healthcare website are displayed on a computer screen in New York on Thursday, Feb. 29, 2024. On Thursday, Change Healthcare, a massive U.S. health care technology company owned by UnitedHealth Group, announced a ransomware group claimed responsibility for a cyberattack and is assessing the impact of the attack, which it first acknowledged on Feb. 21 and says has affected billing and care authorization portals. Credit: AP Photo/Patrick

Health care providers across the country are reeling from a cyberattack on a massive U.S. health care technology company that has threatened the security of patients' information and is delaying some prescriptions and paychecks for medical workers.

The hack could also disrupt discharging people from the hospital, a major hospital association said.

Change Healthcare announced Thursday that a ransomware group that had claimed responsibility for the attack was at fault. Change Healthcare also said it is assessing the impact of the attack, which it first acknowledged on Feb. 21 and has affected billing and care-authorization portals across the country.

"Patient care is our top priority and we have multiple workarounds to ensure people have access to the medications and the care they need," Change Healthcare said in a statement.

Owned by UnitedHealth Group, Change Healthcare manages health care technology pipelines, processing 14 billion transactions a year. The company said its investigation determined that Change Healthcare, Optum, UnitedHealthcare and UnitedHealth Group systems have been affected. Change also confirmed Thursday that ransomware group ALPHV, or Blackcat, made the breach. The company didn't respond to a question about whether it paid or negotiated a ransom.

One of the most immediate impacts is that people are seeing delays in getting prescriptions, American Hospital Association spokesperson Ben Teicher said. Change Healthcare said most affected pharmacies are

using workarounds like writing things down.

But the severity of the situation may still be unfolding, the American Hospital Association said in an email to The Associated Press. Hospitals are having issues with processing claims, billing patients and checking insurance coverage for care, the AHA said, but the attack also could affect the ability to pay workers and buy medicine and supplies.

"The impact to hospitals is just now really starting to crystallize and as a result has been underreported," Teicher said. "As a result we can't really speak to the longer term aftermath, but it can result in hospitals not being able to make payroll or patients still waiting for services to be approved."

Health systems told the Healthcare Association of New York State that they've had trouble with various things, including "an inability to verify patient eligibility and coverage … communicate pharmacy prescriptions, file claims … and receive normal cash flow to support operations, among other issues," association president Bea Grause said.

Several major health care providers that serve multiple states did not respond to requests for comment.

Cybersecurity experts say ransomware attacks have increased substantially in recent years, especially in the health care sector. This one comes on the heels of an attack last month on a children's hospital in Chicago, which had to take phone, email and medical records systems offline.

An FBI spokesperson in Tennessee said he could not confirm or deny whether the FBI is investigating. The FBI also said it's "aware of this incident" but didn't have anything else to provide because the incident "is ongoing."

"As far as we can tell, the attack is being contained," said Allan Liska, a threat intelligence analyst at Recorded Future. "We don't think it's going to get worse. But when you have a critical system like this that's down for an extended period … the longer it's down and the longer that recovery takes, the more impact it's going to have on patient care."

© 2024 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed without permission.

Citation: A large US health care tech company was hacked. It's leading to billing delays and security concerns (2024, March 1) retrieved 9 May 2024 from https://techxplore.com/news/2024-03-large-health-tech-company-hacked.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.