American Hospital Association™
Advancing Health in America

Cybersecurity Advisory

February 22, 2024

UnitedHealth Group's Change Healthcare Experiencing Cyberattack that Could Impact Health Care Providers and Patients Across the U.S.

Change Healthcare, which is one of the largest health care technology companies in the United States, Feb. 21 was hit with a cyberattack that began disrupting a number of its systems and services, according to published reports and a statement posted on Change Healthcare's website.

"Change Healthcare is experiencing a cyber security issue, and our experts are working to address the matter," according to the latest Change Healthcare statement posted on its website at 11:32 a.m. ET on Feb. 22. "Once we became aware of the outside threat, in the interest of protecting our partners and patients, we took immediate action to disconnect our systems to prevent further impact. At this time, we believe the issue is specific to Change Healthcare and all other systems across UnitedHealth Group are operational."

In 2022, UnitedHealth Group completed its merger of U.S. healthcare services company Optum and Change Healthcare. Optum provides services in technology, data, pharmacy care and direct health care.

The AHA has been in communication with the FBI, Department of Health and Human Services, and the Cybersecurity and Infrastructure Security Agency regarding this incident.

WHAT YOU CAN DO

Due to the sector wide presence and the concentration of mission critical services provided by Optum, the reported interruption could have significant cascading and disruptive effects on revenue cycle, certain health care technologies and clinical authorizations provided by Optum across the health care sector. Based upon the statements from Change Healthcare that they became aware of an "outside threat" and disconnected "in the interest of protecting our partners and patients," **we recommend that all health care organizations that were disrupted or are potentially exposed by this incident consider disconnection from Optum until it is independently deemed safe to reconnect to Optum.** It also is recommended that organizations which utilize Optum's services prepare related downtime procedures and contingency plans should Optum's services remain unavailable for an extended period.

Please send any technical, financial and/or clinical impact or related technical threat intelligence on a confidential basis to Riggi at jriggi@aha.org.

In addition:

- Organizations should use this opportunity to test the security, redundancy and

resiliency of their network and data backups ensuring they remain offline. AHA recommends backup technology which renders the backups “immutable” — unable to be deleted, altered or encrypted.

- Ensure that all high criticality, known and exploited vulnerabilities have been patched, especially any which are internet facing.
- Review and test cyber incident response plans, ensure they are well coordinated and integrated with emergency management plans. Test callout for activation of incident command structure and backup communications plans should email and VoIP communications fail.
- Review business and clinical continuity downtime procedures to ensure mission critical and life critical functions could sustain a loss of information, operational and medical technology for up to 30 days.
- Consider designating clinical downtime “coaches” and “safety officers” for each shift. These would be individuals who are experienced and adept at working with downtime, manual procedures should there be a loss of access to the EMR and other medical technology, and who could guide and lead other less experienced staff in the implementation of downtime procedures to ensure continuation of safe and quality care.
- Increase threat hunting and monitoring tools and techniques. Although no specific threat actor has been identified, the joint government agency advisory regarding “living off the land” cyber technique serves as a good general guide.

ADDITIONAL RESOURCES

- For further information on ransomware preparedness see the Stop Ransomware guide.
- Other resources and alerts may be found at stopransomware.gov.
- For the latest cyber threat information and alerts visit cisa.gov.
- To contact local FBI Offices to report suspicious cyber activity visit fbi.gov or ic3.gov.
- For emergency cyber issues such as ransomware attacks in progress, call 24/7 FBI Cyber Watch command center at (855) 282-3937. Define patient care/safety impact such as ambulance diversions in progress, canceled surgeries, etc. CISA may also be contacted at https://www.cisa.gov/cisa-central. CISA 24/7 Cyber Watch Center is (888) 282-0870. Define same patient care/safety impact protocol as above.

FURTHER QUESTIONS

If you have further questions, please contact Riggi at jriggi@aha.org. For the latest cyber threat intelligence and resources, visit www.aha.org/cybersecurity.