February 24, 2024

UPDATE: UnitedHealth Group's Change Healthcare's Continued Cyberattack Impacting Health Care Providers and Patients Across the U.S.

AHA cybersecurity update as of Feb. 24, 7 p.m. ET

Change Healthcare, a health care technology company that is part of Optum and owned by UnitedHealth Group, announced Feb. 21 they were hit with a cyberattack that disrupted a number of its systems and services, according to a statement posted on its website. Change Healthcare indicated it had disconnected its systems "in the interest of protecting our partners and patients." Due to its sector-wide presence and the concentration of mission critical services it provides, the reported interruption could have significant cascading and disruptive effects on the health care field within revenue cycle, pharmacy, certain health care technologies, clinical authorizations and other services.

The AHA continues to recommend that all health care organizations that were disrupted or are potentially exposed by this incident consider disconnection from applications specified by Change Healthcare that remain unavailable due to this cyberattack, as identified on the Change Healthcare application status page. In our Feb. 22 Cybersecurity Advisory we also recommended that organizations which use Change Healthcare impacted services prepare related downtime procedures and contingency plans should those services remain unavailable for an extended period. **As of this date, Change Healthcare has not provided a specific timeframe for which recovery of the impacted applications is expected.**

In addition, open-source statements and press reports have identified exploitation of the ConnectWise vulnerability as a factor in this cyberattack. **The U.S. government had previously recommended that all organizations immediately patch this vulnerability.**

The AHA remains in direct contact with Change Healthcare and requested clarification on its confidence level of nonimpacted systems' security. As of Feb. 23 at 2:40 p.m. ET, Change Healthcare began including the following statement in their regular updates, "We have a high-level of confidence that Optum, UnitedHealthcare and UnitedHealth Group systems have not been affected by this Issue."

We are encouraged by this public statement. **However, the AHA recommends that each health care organization continue to monitor and independently evaluate information provided by Change Healthcare to inform its own risk-based decisions regarding nonimpacted systems.** When considering connectivity to nonimpacted Change Healthcare systems, each health care organization should weigh

connection or reconnection against possible business and clinical disruptions caused by severing the connection to nonimpacted Change Healthcare systems.

In addition, we recognize that the hospitals and health systems may be experiencing challenges with obtaining care authorizations for their patients, as well as delays in payment. **We are in communication with the Department of Health and Human Services, including the Centers for Medicare & Medicaid Services, about options to support patients' timely access to care and provide temporary financial support to providers.** We also are having these discussions with Optum. We will provide more information as it becomes available.

The AHA will continue to keep you updated on this situation. Please send any technical, financial and/or clinical impact or related technical threat intelligence on a confidential basis to John Riggi, AHA's national advisor for cybersecurity and risk, at jriggi@aha.org. The AHA maintains close contact with the FBI, Department of Health and Human Services, and the Cybersecurity and Infrastructure Security Agency and will share cyber threat intelligence with them without attribution to your organization, unless you specify permission to be identified, or contact your local [FBI field office](#).

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.