American Hospital Association™
Advancing Health in America

Special Bulletin

March 1, 2024

UnitedHealth Group's Change Healthcare Launches Temporary Funding Assistance Program, E-prescribing Service in Relation to Ongoing Cyberattack

See AHA's resources on the ongoing cyberattack

Change Healthcare, a health care technology company that is part of Optum and owned by UnitedHealth Group, today announced a "Temporary Funding Assistance Program" webpage and a new instance of its Rx ePrescribing service for customers affected by the ongoing cyberattack on Change Healthcare. Optum says the funding will be for certain providers "who receive payments that were processed by Change Healthcare." See the webpage for more details. *Please note, the AHA has not evaluated the terms of Optum's temporary funding program and is providing this to our membership for informational purposes only.*

BACKGROUND

Change Healthcare announced Feb. 21 it was experiencing a cyberattack and this week acknowledged the attack was perpetrated by threat actor ALPHV Blackcat. See the Feb. 26 AHA Advisory for details on the indicators of compromise associated with the attack and a Feb. 27 updated joint federal advisory #StopRansomware: ALPHV Blackcat.

CONNECTION TO SYSTEMS

UnitedHealth Group continues to say that based on its ongoing investigation, there's no indication that Optum, UnitedHealthcare and UnitedHealth Group systems have been affected by this issue. The AHA continues to recommend that all health care organizations maintain disconnection from applications specified by Change Healthcare that **remain unavailable due to this cyberattack** as identified on the Change Healthcare application status page.

Each health care organization should 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 systems, each health care organization should weigh possible clinical disruptions and business impacts caused by severing the connection to nonimpacted Optum, Change Healthcare, UnitedHealthcare and/or UnitedHealth Group systems.

There is still currently no timetable for recovery of all Change Healthcare systems.

BE MINDFUL OF POTENTIAL FRAUD

© 2024 American Hospital Association | www.aha.org

High profile health care cyberattacks create a ripe environment for all types of fraudsters and cyber adversaries to target hospitals and patients. Be cautious of any email or phone call seeking to obtain personally identifiable information, health insurance information, passwords, financial information or seeking change of payment instructions. Be on heightened alert for phishing emails. If you believe payments have been diverted to unauthorized accounts immediately contact your financial institution and the FBI at www.ic3.gov. If staff or patients have become a victim of identity theft, resources are available at www.identitytheft.gov. Report health insurance fraud to https://tips.oig.hhs.gov/**.**

AHA RESOURCES

Visit AHA's Change Healthcare cyberattack webpage (https://www.aha.org/cybersecurity/change-healthcare-cyberattack-updates) for the latest advisories and advocacy to support hospitals and health systems and ensure patient access to care.

FURTHER QUESTIONS

If you have further questions, please contact John Riggi, AHA's national advisory for cybersecurity and risk at jriggi@aha.org. For the latest cyber threat intelligence and resources, visit www.aha.org/cybersecurity.

© 2023 American Hospital Association | www.aha.org