WHA WISCONSIN HOSPITAL ASSOCIATION
ADVOCATE. ADVANCE. LEAD.
The Valued Voice

Vol. 68, Issue 9 Thursday, February 29, 2024

Kaufman Hall: UnitedHealth Group Security Breach Causing "Significant Cash Flow Issues" for Providers

AHA is providing regular updates and advocacy to address impacts on hospitals

Change Healthcare, a health care technology company that is part of Optum and owned by UnitedHealth Group, announced on Feb. 21 that it experienced a cyberattack that has resulted in continued disconnection of its systems. Systems impacted include claims processing, prior authorization and eligibility determinations. At this time, there is no timeline regarding when Change Healthcare's systems will be back online.

Initially reported in national media as primarily impacting prescription orders and military clinics and hospitals, the outage at Change Healthcare is also significantly impacting other providers and payers that utilize its platform. Those impacts include inability to send claims, receive payments and process prior authorizations.

"My understanding is Change/Optum touches almost every hospital in the United States in one way or another," said National Advisor for Cybersecurity and Risk for the American Hospital Association (AHA) John Riggi.

Kaufman, Hall & Associates, LLC, a health care financial services consultant, reported on Feb. 28 that "lack of access to Change's platform is causing significant cash flow issues for many provider organizations," and warned that "this can be a particularly significant issue for organizations that are approaching a March 31 fiscal year end or a test of bond covenants, especially if they had less robust balance sheets preceding the cyberattack [on Change Healthcare]."

"The most significant impact of the shutdown of Change's platform is that provider organizations are no longer able to send claims information through Change's clearinghouse platform and are no longer able to receive claim information back from payers through the platform," said Kaufman Hall's Geoff Stenger and Zech Decker. "Cash posting has also been affected because provider organizations do not have the data needed to match with any funds deposited by payers in bank accounts."

"The outage of United Healthcare's Change Healthcare claims processing systems has a potential to have significant financial impacts on 24/7/365 hospitals in Wisconsin and nationwide that are already facing historic fiscal pressures," said WHA President and CEO Eric Borgerding. "In addition to direct impacts of delayed payments and patient care disruptions, implementation of alternatives to the Change Healthcare system will require the diversion of hospital expenditures, resources and expertise to develop and appear to not be easily implemented in the short-term."

AHA has been actively responding to and providing information to its members throughout the incident, including an initial alert on Feb. 22 and a nationwide member call on Feb. 23 with representatives from the Department of Health and Human Services, Cybersecurity and Infrastructure Agency, and Federal Bureau of Investigation.

AHA is posting its updates and bulletins on the Change Health care Cyberattack at https://www.aha.org/cybersecurity/change-healthcare-cyberattack-updates.

AHA is also communicating with policymakers in Washington, D.C. regarding the impacts of the security breach at Change Healthcare. On Feb. 26, AHA President Rick Pollack sent a letter to U.S.
Department of Health and Human Services Secretary Xavier Becerra regarding the implications of the cyberattack and requested efforts from HHS to help minimize the fallout from the outage at Change Healthcare.

Included in AHA's request to HHS was to offer guidance to providers about how they may request Medicare advanced and accelerated payments to help assist hospitals and health systems that may need immediate federal support as the disruption persists.

AHA also sent out a bulletin to members on Feb. 26 reporting information published by cyberintelligence firm RedSense that Change Healthcare's Feb. 21 security breach was caused by an exploitation of vulnerabilities with the ConnectWise ScreenConnect software that were reported by ConnectWise to its users on Feb. 19. AHA's bulletin reports that the ScreenConnect software is utilized in many businesses across the nation and that all users should follow ConnectWise' advisory to its customers to its immediately update the ScreenConnect software to address the identified vulnerability.

AHA and others are exploring alternatives for claims submissions to address the disruption to Change Healthcare's system. However, multiple challenges have been identified to quickly changing claims processing systems.

Kaufman Hall also highlighted those challenges. "Organizations should expect, however, a lag of weeks or even months before these alternatives could become functional," said Kaufman Hall's Stenger and Decker.

For members seeking additional information relating to the Change Healthcare security breach, contact WHA's Matthew Stanford or Joanne Alig.

Other Articles in this Issue