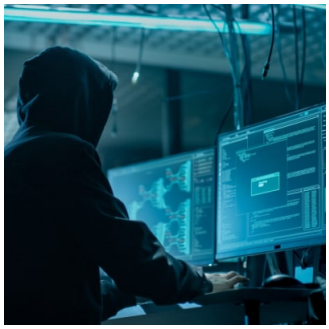
HealthManagement
Promoting Management and Leadership

U.S. Department of Health and Human Services Launches Probe into Change Healthcare Ransomware Attack



The U.S. Department of Health and Human Services (HHS) has initiated an investigation into the recent ransomware attack on Change Healthcare, following weeks of disruptions to healthcare and billing operations nationwide. The announcement comes after a meeting between White House officials, medical industry representatives, HHS Secretary Xavier Becerra, and Andrew Witty, CEO of UnitedHealth Group, Change Healthcare's parent company.

HHS will investigate possible health information leak and accountabilities

In a letter published by the HHS Office for Civil Rights (OCR) on Wednesday, Director Melanie Fontes Rainer stated the need for an investigation "given the unprecedented magnitude of this cyberattack, and in the best interest of patients and healthcare providers." The probe will focus on whether protected health information was compromised and if Change Healthcare and UnitedHealth Group (UHG) complied with Health Insurance Portability and Accountability Act (HIPAA) rules. Fontes Rainer clarified that while other entities associated with Change Healthcare and UHG are of secondary interest, reminders have been issued regarding regulatory obligations and responsibilities, including the necessity for business associate agreements and timely breach notifications.

Consequences of the attack are still ongoing

The incident has incurred significant financial losses, estimated at over $100 million daily, impacting hospitals, clinics, and pharmacies across the country. Change Healthcare, responsible for processing roughly half of all medical claims in the U.S., detected the ransomware attack by the AlphV/BlackCat gang on February 21, prompting the shutdown of its systems. Despite allegedly paying a ransom, the company struggled to restore its platform, severely affecting healthcare providers' ability to file and receive insurance payments. The American Hospital Association termed it "the most significant and consequential incident of its kind against the U.S. healthcare system in history." Biden administration officials expressed frustration with UnitedHealth's handling of the situation. Becerra urged insurance companies to assist providers in ensuring timely care delivery. While some systems have been restored, the broader payments platform is not expected to resume until March 15, with medical claims technology testing to follow through March 18.

Recent attack reignites concerns about market concentration

The incident has rekindled concerns raised by the Justice Department over UnitedHealth's acquisition of Change Healthcare, initially contested in 2022. Despite the lawsuit's failure, the consolidation of significant portions of the healthcare system under one company has drawn criticism. Ransomware attacks targeting the healthcare industry have surged by 256% over the past five years, with breaches affecting over 134 million individuals in 2023 alone, as highlighted by HHS.

In response to these escalating cyber threats, industry stakeholders and government agencies are under mounting pressure to fortify cybersecurity measures and ensure regulatory compliance to safeguard patient data and critical healthcare operations. The investigation into the Change Healthcare ransomware attack underscores the urgency of addressing cybersecurity vulnerabilities within the healthcare sector to mitigate the risks posed by malicious actors.

Source: The Record Media

Image Credit: iStock

Published on : Fri, 15 Mar 2024