American Hospital Association™
Advancing Health in America

Special Bulletin

March 12, 2024

Change Healthcare Cyberattack Prompts Breach Notification Questions

Following the Change Healthcare cyberattack on Feb. 21, the AHA has received questions from hospitals and health systems about their obligations for breach notifications and other requirements regarding data privacy and patient information. Please note that to date, neither Change Healthcare nor its parent company UnitedHealth Group has publicly indicated that the cyber adversaries responsible for this attack have taken any data, including protected health information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

The AHA has worked with its outside counsel at Jones Day to address questions on this issue. The information contained herein does not constitute legal advice. Hospitals should consult their organization's legal counsel and other leadership when assessing these issues.

With those caveats in mind, at this initial stage, hospitals should consider the following:

1. Assess Relationship with Change Healthcare

Change Healthcare Products Utilized. Change Healthcare offers over 400 solutions for its customers. Hospitals should consult with their business and IT teams now to determine, specifically, which Change Healthcare products are utilized. Hospitals using Change Healthcare products should then assess whether it acts as a business associate or as a covered entity clearinghouse under HIPAA, as the relationship may impact the investigation and notice obligations.

Business Associate Agreements (BAA) and Underlying Service Agreements. Hospitals should review BAAs and underlying service agreements with Change Healthcare for provisions relating to security incidents and breach notification obligations (e.g., delegation of breach notification functions, timing for notices, etc.) and indemnification, limitation of liability, insurance coverage, arbitration of disputes, etc.

2. Assess Initial Regulatory Obligations

Duty to Investigate. Regardless of any notification (or lack thereof) from Change Healthcare as to whether PHI was impacted, hospitals should assess the facts and investigate credible information and evidence of any potential data breach impacting their data, including by seeking status updates from Change Healthcare directly. HIPAA regulations treat breaches as "discovered" as of the date a covered entity knew, "or, by exercising reasonable diligence" would have known of the breach. The date of discovery of a breach triggers breach notification timing requirements.

Requirements Upon Notice of Breach. If Change Healthcare, acting as a business associate, provides notice of a breach of unsecured PHI, hospitals should conduct a HIPAA risk assessment to determine whether there is a low probability that PHI has been compromised. This risk assessment must consider, at least, the following four factors: (i) the nature and extent of PHI involved (e.g., type of identifiers); (ii) the unauthorized person who used or received the PHI (e.g., threat actors); (iii) whether PHI was actually acquired or viewed (e.g., exfiltration); and (iv) the extent to which risk to PHI has been mitigated. If Change Healthcare provides notice of a breach of personal information that does not constitute PHI, a HIPAA risk assessment may not be necessary, but state law and other requirements may still apply.

3. Assess Business Considerations

Review of Privacy and Security Policies. Hospitals should review internal privacy and security policies to facilitate and ensure compliance with a hospital's own procedures for purposes of potential future government audits. Hospitals also should review their public-facing privacy policies for provisions relating to arbitration, class action waivers, etc., to assess data breach class-action litigation risks, particularly because litigation has already been initiated related to the incident.

Timely Insurance Notice. Importantly, hospitals should review insurance policies, identify and review notice provisions and requirements, and contact applicable carriers (e.g., cyber and business interruption) to notify of potential incidents as the situation develops.

Continued Monitoring and Assessment. Hospitals should continue to monitor and assess internal IT systems for suspicious activity or inconsistent outcomes and maintain logs/documentation of such assessments. They also should continue regular conversations with Change Healthcare to stay updated on progress of its internal assessments and, ideally, broader communications before a hospital's potential involvement is publicized by Change Healthcare or otherwise. Apart from cyber and privacy matters, hospitals also may consider obligations, risks and available flexibilities including in the health care, civil litigation and insurance recovery spaces.

BACKGROUND

The widespread repercussions from the Change Healthcare cyberattack continue to make it harder for many hospitals and doctors to provide patient care, submit insurance claims and receive payment for the essential health care services they provide.

Throughout the last few weeks, the AHA has been urging UHG to take action to minimize disruption to patient care and hospital operations resulting from this attack. In addition, AHA has urged Congress and the Department of Health and Human Services to support hospitals and providers impacted by the attack.

FURTHER QUESTIONS

If you have further questions on these announcements, please contact Chad Golder, AHA general counsel, at cgolder@aha.org, and Julie Schenker, AHA deputy general counsel for advocacy, at jschenker@aha.org.