Provided by National Insurance Services

LEGAL UPDATE

NIS
National Insurance Services

HHS Encourages Urgent Review of HIPAA Compliance Following Health Care Cyberattack

The U.S. Department of Health and Human Services (HHS) recently issued a letter addressing the cybersecurity incident impacting Change Healthcare, a unit of UnitedHealth Group. Given the "unprecedented magnitude" of this cyberattack, HHS' Office for Civil Rights (OCR) is investigating whether these entities comply with the HIPAA Privacy, Security and Breach Notification Rules (HIPAA Rules), including whether a breach of protected health information (PHI) occurred.

OCR is also encouraging HIPAA-covered entities (e.g., health plans, health insurance issuers and health care providers) and their business associates to **review their cybersecurity measures "with urgency"** to ensure that health information is protected.

While many employers do not have access to PHI from their health plans, employers that use third-party vendors, such as third-party administrators (TPAs) and pharmacy benefit managers (PBMs), should investigate and verify these vendors' cybersecurity measures during the selection process. Employers should also ensure they have business associate agreements in place that include adequate security protections for electronic PHI.

ACTION STEPS

Given OCR's focus on safeguarding electronic PHI, employers should consider the following steps:

- Employers that have access to PHI from their health plans should review their current cybersecurity measures and make any appropriate updates.
- Even if an employer does not have access to PHI, it should review a prospective TPA's or PBM's cybersecurity practices during the selection process.
- Employers should also ensure their business associate agreements include adequate security protections.

Health Care Cyberattacks

On Feb. 21, 2024, Change Healthcare, one of the largest platforms for managing health insurance billing and payments in the United States, experienced a large-scale cyberattack. This attack affected millions of health care providers and patients across the country. Cybersecurity experts have deemed the incident one of the most disruptive attacks in history.

According to OCR, ransomware and hacking are the primary cyberthreats in health care. Over the past five years, there has been a 256% increase in large breaches reported to OCR involving hacking and a 264% increase in ransomware. In 2023, hacking accounted for 79% of the large breaches reported to OCR.

Compliance Resources

Safeguarding PHI is a top priority for OCR. To help covered entities and business associates protect their systems from cyberattacks, OCR has provided a variety of resources, including:

- HIPAA Security Rule Guidance Material
- OCR Video – How the HIPAA Security Rule Protects Against Cyberattacks
- OCR Webinar on HIPAA Security Rule Risk Analysis Requirement
- HIPAA Security Risk Assessment Tool
- Fact Sheet: Ransomware and HIPAA

This Legal Update is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel for legal advice.
©2024 Zywave, Inc. All rights reserved.