Provided by National Insurance Services

LEGAL UPDATE

HHS Updates HIPAA FAQs Regarding Change Healthcare Cybersecurity Incident

On May 31, 2024, the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) updated its frequently asked questions (FAQs) regarding HIPAA and the recent cybersecurity incident involving Change Healthcare, a unit of UnitedHealth Group. OCR enforces the HIPAA Privacy, Security and Breach Notification Rules (HIPAA Rules), which require covered entities and their business associates to protect the privacy and security of protected health information (PHI) and notify HHS and affected individuals following a breach.

FAQ Updates

The updates to the FAQs address the **responsibility for providing breach notification to HHS, affected individuals and, where applicable, the media.** Specifically, the FAQs provide that:

- Covered entities affected by the Change Healthcare breach may delegate to Change Healthcare the task of providing the required breach notifications on their behalf;
- Only one entity (which could be the covered entity or Change Healthcare) needs to provide breach notifications; and
- If covered entities ensure that Change Healthcare provides the required breach notifications in a manner consistent with the HIPAA Rules, they will not have additional HIPAA breach notification obligations.

Cybersecurity Measures

In connection with the Change Healthcare cybersecurity incident, OCR has encouraged HIPAA-covered entities (e.g., health plans, health insurance issuers and healthcare 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.

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 Webinar on HIPAA Security Rule Risk Analysis Requirement
- HIPAA Security Risk Assessment Tool
- Fact Sheet: Ransomware and HIPAA

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.

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.