Is Your Data Secure? HHS Opens Investigation into Change Healthcare Cyberattack

March 26, 2024

PRACTICES Employee Benefits and Executive Compensation

The HHS's Office for Civil Rights (the ***"OCR"***) issued a "Dear Colleague" letter (***"Letter"***) on March 13 addressing a massive cybersecurity incident impacting Change Healthcare, a unit of UnitedHealthcare Group (***"UHG"***) that handles payment processing. This cyberattack impacted many other health care entities, disrupted health care and billing information operations nationwide and threatened the security of patients' health information. A ransomware group was responsible for this attack.

The HIPAA Privacy, Security, and Breach Notification Rules (***"HIPAA Rules"***) set forth the requirements that "covered entities" (such as most health care providers, health plans and health care clearinghouses) and their "business associates" must follow to protect the privacy and security of PHI, including required notifications to HHS and affected individuals following a breach of PHI.

The OCR administers and enforces the HIPAA Rules, and safeguarding PHI is a top priority of the OCR.

As noted in the Letter, over the past five years, there has been a 256% increase in large breaches reported to the OCR involving hacking and a 264% increase in ransomware attacks. The OCR reports that in 2023 hacking accounted for 79% of the large breaches reported to the OCR, and these breaches affected over 134 million individuals, a 141% increase from 2022.

Although the OCR stated it is not prioritizing investigations of health care providers, health plans or business associates that were impacted by this cyberattack, the OCR did remind entities that have partnered with Change Healthcare and UHG of their regulatory obligations and responsibilities, including ensuring that up-to-date business associate agreements are in effect, and that timely breach notifications to HHS and the affected individuals are provided. The OCR encouraged all entities subject to the HIPAA Rules to review their cybersecurity measures to ensure that health information is properly protected in compliance with the HIPAA Rules.

Employers should (i) ensure they have current business associate agreements in effect with service providers to the plan, (ii) review business associate agreements to determine whether the employer or the service provider is responsible for making required notifications under HIPAA and state law in the event of a breach, and (iii) ensure they are documenting breaches in accordance with the HIPAA Rules and the plan's HIPAA policies and procedures. It is always a good idea to have the plan's legal counsel review all agreements, including business associate agreements, before they are signed by the plan or plan sponsor.

The Letter is available here.