DORSEY
DORSEY+WHITNEY LLP

HHS OCR Settles HIPAA Investigation with Business Associate for $350,000

May 19, 2023 – Dorsey Health Law
by Alissa Smith and Seamus Taylor

Over the past decade, the number of health care data breaches reported to the U.S. Department of Health and Human Services' Office for Civil Rights ("OCR") has increased dramatically. From 2009 to 2022, over 5,000 data breaches affecting 500 or more records were reported to OCR, accounting for the exposure of over 380 million health care records. More and more often, these breaches have involved business associates performing third-party services for covered entities. This year, some of the largest business associate breaches have involved Cerebral, Inc. (> 3 million individuals affected), NationsBenefits Holdings, LLC (> 3 million individuals affected), and NextGen Healthcare (> 1 million individuals affected). The latest business associate settlement with OCR, involving MedEvolve, Inc., provides important lessons for both business associates and covered entities.

The HIPAA Fundamentals

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") creates rules for the privacy and security of individually identifiable health information held by covered entities and business associates (the "HIPAA Rules"). A "covered entity" is a health plan, a health care provider that electronically transmits health information in connection with certain financial and administrative transactions, or a health care clearinghouse. A "business associate" is a person or entity that provides services to a covered entity that involve creating, receiving, maintaining, or transmitting protected health information ("PHI"). Any subcontractor of a business associate that creates, maintains, or transmits PHI on behalf of that business associate is also a business associate. All arrangements between covered entities and business associates, including between business associates and

Related People

- Alissa Smith

Related Capabilities

- Healthcare & Life Sciences
- Healthcare Transactions & Regulations
- Healthcare Litigation
- Medical Devices

subcontractors, must involve a business associate agreement (BAA) which outlines each party's obligations to protect PHI and report any data breaches.

OCR is the office tasked with enforcement of the HIPAA Rules. Under the HIPAA Rules, covered entities are required to notify affected individuals, OCR, and in some cases, the media, following the discovery of a breach of unsecured PHI. Business associates are also required to notify covered entities following the discovery of a breach. OCR investigates written complaints and conducts compliance reviews and audits to enforce the HIPAA Rules. If violations of HIPAA are discovered, OCR can enter into a resolution agreement with the violating entity. Resolution agreements often require the entity to complete a corrective action plan (CAP) and pay a settlement amount.

OCR's Settlement with MedEvolve, Inc.

On May 16, OCR announced a settlement of potential violations of the HIPAA Rules with MedEvolve, Inc. (MedEvolve), a business associate that provides practice management, revenue cycle management, and practice analytics software services to covered health care entities. The alleged HIPAA violations occurred in 2018, when MedEvolve suffered a data breach exposing the PHI of more than 200,000 individuals. Specifically, one of MedEvolve's servers containing PHI such as patient names, billing addresses, and phone numbers was reported as openly accessible to the internet. As OCR investigated the breach, it determined that MedEvolve had failed to: (i) conduct a risk assessment to determine vulnerabilities to PHI, and (ii) enter into a BAA with a subcontractor.

Pursuant to the resolution agreement, MedEvolve has paid a $350,000 penalty to OCR and agreed to implement a corrective action plan (CAP) to address potential violations of the HIPAA Rules. As part of the CAP, MedEvolve has agreed to:

- Conduct a risk analysis to determine vulnerabilities;
- Implement a risk management plan;
- Revise its written HIPAA policies and procedures; and
- Provide HIPAA training for employees with access to PHI.

Additionally, OCR will monitor MedEvolve for a period of two years to ensure compliance with the HIPAA Rules.

Lessons for Covered Entities and Business Associates

While covered entities have historically reported the largest number of data breaches, the number of business associate data breaches continues to increase. Hacking/IT incidents accounted for 79% of the large data breaches reported to OCR in 2022, and

network servers were the most common targets in these incidents. Thankfully, both covered entities and business associates can take precautions to strengthen their cybersecurity practices and lower the risk of a breach. Steps that should be taken include:

- Covered entities should conduct due diligence on any vendor that will handle PHI. This should include investigating the vendor's: (i) IT security measures employed to protect data, (ii) employee training used to ensure staff understands how to protect PHI; and (iii) processes in place for responding to incidents.
- Covered entities and business associates should have a BAA in place and understand their reporting obligations under the BAA. The BAA should govern a business associate's reporting obligations to the covered entity. When a breach is reported to the government, OCR will have questions about the BAA and the parties' reporting obligations.
- Employees pose the biggest risk to an employer's security. Employees should be trained to recognize and avoid phishing attempts and to report concerns immediately when they suspect a breach has occurred.

When it comes to cybersecurity, an ounce of prevention is worth a pound of cure. Dorsey's health care attorneys strongly recommend regularly reviewing your HIPAA compliance and updating your policies and procedures to reflect current best practices.