Published on *The National Law Review* https://natlawreview.com

A $31,000 Mistake: Failing To Manage Business Associate Agreements Proves Costly For Providers

Article By:

Kim T. Le

The Center for Children's Digestive Health (CCDH), a small, for-profit pediatric subspecialty practice that operates seven clinics in the Chicago area, has paid the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) $31,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

On August 13, 2015, OCR initiated a compliance review of CCDH to determine whether CCDH's disclosure of protected health information (PHI) to FileFax, Inc. (FileFax), a Northbrook, Illinois-based vendor that stores paper records, was permissible under the Privacy Rule. OCR found that, beginning in 2003, CCDH contracted with FileFax to store inactive patient medical records containing protected health information—however, neither party could produce a signed business associate agreement (BAA) prior to Oct. 12, 2015. CCDH had "failed to obtain satisfactory assurances from Filefax, in the form of a written business associate agreement, that Filefax would appropriately safeguard the PHI" that was in the company's possession. Despite not having a BAA in place, the provider shared the records of at least 10,728 people, according to OCR. In a related suit, the Illinois Attorney General alleged that FileFax's employees had tossed thousands of paper medical records into an unlocked dumpster.

In addition to the $31,000 settlement, CCDH must (i) enter into a corrective action plan to develop policies and procedures in compliance with federal privacy and security standards, (ii) educate its employees about proper handling of PHI, and (iii) provide HHS a list of all its business associates, and produce a duly-executed BAA for each.

Many of the obligations set forth under the HIPAA Privacy, Security, and Breach Notification Rules apply directly to business associates pursuant to the 2013 HIPAA Omnibus Rule; notwithstanding, covered entities are still obligated to have a BAA in place with each of their business associates. **CCDH's settlement should serve as a reminder to providers that they do not need a data breach to trigger a HIPAA violation and the stiff penalties that follow. An essential part of any provider's contract management process must include a keen eye towards BAA management.**

The most common types of provider entities that have had to take corrective action to achieve voluntary compliance are, in order of frequency:

- Private Practices
- General Hospitals
- Outpatient Facilities
- Pharmacies

Given this increased exposure, providers should examine their business associate relationships and take the following actions to avoid HIPAA penalties:

1. Tighten-Up Existing Business Associate Agreements. A good BAA should spell-out a business associate's privacy and security obligations—less-savvy business associates may need added guidance regarding HIPAA compliance requirements. Additionally, where the underlying vendor service agreement does not contain a provision for indemnification, providers should ensure that the BAA contains an indemnification provision, as HIPAA breach liability can be extremely costly. The business associate should be obligated to indemnify the provider where the business associate caused the data breach (e.g., through negligence).

2. Follow the Use and Disclosure Rules. Generally, covered entities may use or disclose PHI for purposes of treatment, payment, or certain health care operations; however, they may not use or disclose more than is minimally necessary for the permitted purpose. Providers should ensure that they disclose to business associates only the minimal amount of PHI necessary for the business associate's intended purpose.

3. Ensure Timely Patient Access. HIPAA grants patients certain rights over their PHI, including the right to obtain copies, request amendments to their information, and obtain an accounting of disclosures. Providers should ensure that any patient-facing business associate promptly responds to patient requests to access their PHI, in accordance with the terms of its BAA—or, ensure that such business associate is obligated to promptly notify the provider of the request so that the provider may directly respond.

4. Maintain Written Policies and Procedures. HIPAA requires covered entities to develop and maintain written policies and procedures that effectuate the privacy and security rule requirements, including policies concerning business associate oversight and BAA management. According to OCR, a provider that maintains the required written policies may be able to avoid heavy penalties imposed for "willful neglect."

National Law Review, Volume VII, Number 117