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

OCR Settlement Includes Vendor Breach of ePHI in Absence of Business Associate Agreement

Article By:

Drinker Biddle & Reath LLP

Oregon Health & Science University (OHSU) has agreed to a $2.7 million settlement with the ***Office for Civil Rights (OCR)*** at the Department of Health and Human Services. This settlement follows the theft of unencrypted laptops and an unencrypted thumb drive that exposed the electronic personal health information (ePHI) of thousands of patients. Through further investigation, OCR found that OHSU stored over 3,000 individuals' ePHI in Google Drive and Google Mail, a cloud-based service provider. OHSU did not have a business associate agreement in place with Google. OCR's settlement agreement in this case reinforces OCR's previous statements that a business associate relationship arises as a matter of law, and not just when a business associate agreement is in place. The settlement also suggests that simply providing PHI to a business associate without an appropriate Business Associate Agreement (BAA) in place –without further third-party disclosure – can lead to a conclusion that the PHI was breached.

OCR's investigation revealed that OHSU failed to obtain a BAA from Google when it stored ePHI in Google's cloud-based services. Google held a variety of sensitive ePHI, including credit card and payment information, diagnoses, procedures, photos, driver's license numbers, and Social Security Numbers. OCR's investigation also revealed a number of other concerns. For example, the security risk assessment conducted by OHSU failed to cover all ePHI in its possession, and the documented risks were not addressed in a timely manner. Additionally, OHSU failed to implement policies and procedures to prevent, detect, contain, and correct security violations. OHSU also failed to implement encryption and decryption standards or equivalent alterative measures, as required by HIPAA. OCR Director Jocelyn Samuels stated that "from well-publicized large scale breaches and findings in their own risk analyses, OHSU had every opportunity to address security management processes that were insufficient."

Importantly, for companies that work with covered entities and receive or maintain PHI on their behalf, the OCR settlement suggests that mere access to ePHI without a BAA can be a "breach" that requires OCR notification. OCR is likely drawing on language in the definition of "breach" that requires notification upon any violation of the Privacy Rule. However, OCR did not explain why the use of a service provider without a BAA in place would necessarily pose a risk that the PHI had been "compromised." Although not necessarily indicative of OCR's thinking, OSHU's press release issued at the time of the breach pointed to language in Google's terms and conditions that allows Google to use data stored in its services for the purpose of improving Google's own products. If this

language was the basis for OCR’s conclusion that PHI was “compromised” by being stored in a Google product, the settlement demonstrates OCR’s very low threshold for risk of compromise.

Health care companies should review relevant relationships with vendors to assess the need for a BAA. Covered entities should implement BAAs with any company that has access to ePHI, even if the company does not view the information, but merely holds it. Per their terms, BAA requires vendors to provide written assurances that information will be protected according to the required physical and security safeguards. Even if cloud providers never view or actually access the ePHI, companies that receive ePHI are still considered business associates.

National Law Review, Volume VI, Number 216