Insights

Business Associate Fined Under HIPAA For Maintaining PHI on Unsecured Server

June 6, 2023

By: Robert A. Anderson and Stacy Walton Long

The U.S. Department of Health and Human Services, Office for Civil Rights ("OCR"), recently concluded its investigation into MedEvolve, a business associate ("Business Associate") of a covered health care entity. Business Associate self-reported a data breach to OCR that exposed the Protected Health Information ("PHI") of more than 230,000 individuals on the Internet. The PHI was accessible on the Internet for at least seven months due to Business Associate's use of an unsecured firewall on its computer server. OCR settled with Business Associate for $350,000 and imposed a Corrective Action Plan to resolve potential HIPAA violations and ensure the security of electronic Patient Health Information going forward. OCR's **investigation** is a significant reminder that business associates of covered entities can be directly liable for failures to maintain adequate IT safeguards with respect to PHI. Business associates are subject to the same privacy and security rules as covered entities under HIPAA.

HIPAA requires all business associates to comply with the HIPAA Security Rule as well as provisions of the Privacy and Breach Notification Rule. Although HIPAA is regularly understood to require covered entities take the necessary steps to follow privacy and security regulations, there is an equal necessity for business associates to actively protect PHI received through the contractual relationships with the covered entities. Under HIPAA's Rules, business associates are required to self-report any information breaches. As this case illustrates, these breaches can include something as basic as failing to maintain a firewall to protect the information. Thus, it is essential for Business Associates to understand and implement the HIPAA privacy and security rules. Not only can it lead to liability to OCR, adverse publicity, and an onerous Corrective Action Plan, but significant breaches will most likely seriously damage the relationship between the business associate and the covered entity.

Business Associate's settlement requires monitoring by OCR for the next two years. It also requires Business Associate to conduct a risk analysis and implement a risk management plan addressing and mitigating security risks. Business Associate's **Corrective Action Plan** also requires it to develop, maintain, and revise written policies and procedures in compliance with HIPAA. Moreover, all Business Associate workforce members with access to PHI must take part in a HIPAA Privacy and Security Training Program. If any member of Business Associate's workforce fails to comply with the HIPAA Rules, Business Associate must report the failure to Health and Human Services within sixty days and mitigate the harm.

Contact **Robert A. Anderson** or **Stacy Walton Long** with any questions regarding the implications of the HIPAA privacy and security rules applicable to business associates.