HIPAA Business Associates are Not Immune from HIPAA Penalties



9/1/2025

A New York public accounting, business advisory, and management consulting firm recently agreed to settle alleged HIPAA violations, including paying a $175,000 civil penalty, implementing a corrective action plan, and undergoing two years of monitoring by the Department of Health & Human Services, Office for Civil Rights (OCR). In the provision of its accounting and financial services to its single covered entity client, the firm receives protected health information.

The OCR initiated an investigation after receiving a breach report filed by the business associate, in which it reported its discovery that part of its network was infected with ransomware, impacting the PHI of its health care client. Through its investigation, the OCR determined that the business associate "failed to conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of [electronic] PHI held by" the business associate. The settlement mark's OCR's 15th Ransomware Enforcement Action and 10th Enforcement Action in its Risk Analysis Initiative.

This settlement underscores OCR's emphasis on HIPAA Security Rule compliance, including the performance of periodic risk analyses and the development or risk management plans to address identified risks and vulnerabilities to IT systems that house PHI. Importantly, it also emphasizes that the amount of PHI held by a business associate or the fact that it serves only a single covered entity client does not make that business associate immune from compliance, or from prosecution.

If you need assistance with your HIPAA compliance program, an OCR investigation, or a data breach incident, please contact:
Lani M. Dornfeld, CHPC | 973.403.3136 | ldornfeld@bracheichler.com

Authors

The following attorneys contributed to this insight.



Lani M. Dornfeld

CHPC, Member
Healthcare Law

973.403.3136 · 973.618.5536 Fax

ldornfeld@bracheichler.com