COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 32, Number 14. April 10, 2023
As a BA of Hospitals, Law Firm Settles HIPAA Case Over Attack That Exposed Patient Data

By Nina Youngstrom

A New York City law firm that's a business associate (BA) of its hospital clients has agreed to pay $200,000 in an agreement with the New York State Office of Attorney General (OAG) over alleged violations of HIPAA and New York state business law.[1]

The law firm, Heidell, Pittoni, Murphy & Bach LLP (HPMB), which represents hospitals and hospital networks in litigation, is also required to implement reforms. They include appointing a chief information security officer, encrypting data and patching software in the context of maintaining an information security program.

The OAG alleged the law firm's "poor data security measures made it vulnerable to a 2021 data breach that compromised the private information of approximately 114,000 patients." For example, the law firm left its server vulnerable to attack by failing to timely apply Microsoft software patches when they were released in the spring of 2021, according to the Assurance of Discontinuance, which has the OAG's investigative findings and the relief agreed to by the law firm.[2]

"Third-party vendors are really where health care organizations, such as hospitals and health systems, are vulnerable," said Walter Johnson, assistant privacy officer at Inova Health System in Fairfax, Virginia. A small or midsize BA "doing a heavy lift for a specific area for the covered entity is an easy target for threat actors. Any gap identified by threat actors allows them a back door to the covered entity." Johnson noted that some covered entities (CEs) are requiring BAs to cover the costs associated with a breach they're responsible for. Their business associate agreements (BAAs) would include a liability provision to that effect.

As fiduciaries, law firms, accounting firms and some benefit vendors have a higher threshold for protecting client data, said attorney Iliana Peters, former acting deputy director of the HHS Office for Civil Rights. "A fiduciary has additional obligations to their clients—many of them ethical—to protect the best interests of their clients. They are entities with their own ethics and other compliance obligations besides requirements pursuant to HIPAA and any state law that might be applicable," said Peters, with Polsinelli in Washington, D.C. She said hospitals have a different relationship with a fiduciary than they do with other types of BAs, such as software vendors. "Some software vendors or other infrastructure vendors may only be concerned with their business. Many of them are very good data stewards but some are not." In theory, covered entities have less to worry about when data is in the hands of fiduciaries because "there are fewer concerns about redisclosure versus other vendors who might specialize in, for example, artificial intelligence, social media or other software technologies" and possibly reuse or sell aggregated and anonymized data, Peters said.