COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 18, Number 5. May 31, 2018 HIPAA Compliance Must Take Center Stage in Mergers and Acquisitions

By HCCA Staff

Firms involved in mergers and acquisitions involving covered entities (CE) and business associates (BAs) run the risk of acquiring HIPAA liabilities along with another company's assets. In order to manage that risk, they need to know exactly what they're buying, even if that means asking time-consuming and difficult questions as part of transaction due diligence.

That's the word from attorneys involved in mergers and acquisitions, who say that the purchaser needs to incorporate HIPAA-related due diligence early in the process. BAs in particular may warrant extra scrutiny in mergers and acquisitions, depending on how they're set up and on how much of their business involves protected health information (PHI).

"Problems are ubiquitous," says Kate Hardey, an attorney with McGuireWoods LLP in Virginia. "Companies are certainly trying. But in a higher percentage of deals we look at, there is some type of HIPAA concern that we want to correct."

According to Hardey, the most common concerns found in health care mergers and acquisitions include whether the merger or acquisition target has conducted security risk assessments, and whether the target has proper HIPAA policies and procedures.

HIPAA issues figure into "so many different types of deals," Hardey tells *RPP*. "It's not just health systems purchasing physician practices." For example, issues frequently arise when a BA buys or merges with another BA, and when a CE buys a BA, she says.

BAs Have OCR's Attention

The HHS Office for Civil Rights (OCR) showed it was serious about policing BAs in a $650,000 settlement reached in 2016 with Catholic Health Care Services, a division of the Archdiocese of Philadelphia that was a BA (*RPP 7/16, p. 1*). The settlement was prompted by the theft of an unencrypted iPhone that involved PHI of fewer than 500 nursing home patients.

For BAs, "HIPAA enforcement has been evolving, as has overarching data privacy and security in general," Hardey says. "Enforcement has shifted, and now we're certainly seeing more enforcement and agencies looking at business associates."

BAs—and of course, CEs—vary in the attention they pay to HIPAA issues, Hardey says. Some have excellent written policies but ignore those policies in practice, while some barely have anything written down, but have a strong culture of privacy and security in practice.

For an organization seeking to acquire a BA, the key is to determine how faithfully the company follows HIPAA rules, she says. "If you're a business associate, what are you doing to evaluate the security of the data you have? What are your policies and procedures? What are you doing with your data? You've got to have the basic

provisions."

In one recent deal, Hardey reports, a BA was acquiring another company that operated primarily as a BA. "Neither company really had the robust policy and training they should have had as a business associate," she says, but the purchaser actually had a weaker privacy and security program compared to the company being acquired. The purchasing BA planned to review the other BA's policies and procedures with an eye toward upgrading its own, she says.

That strategy—to take the best practices from one of the parties in an acquisition or merger deal and apply them to the combined entity—can work well in many transactions, Hardey says.