Report on Patient Privacy Volume 19, Number 5. May 08, 2019 Managing Vendors, Possible Breaches As OCR, State-Level Scrutiny Increases for BAs and CEs

By Jane Anderson

The HHS Office for Civil Rights (OCR) and state attorneys general (AGs) are honing in on vendor management in the wake of breaches involving business associates (BAs), and covered entities (CEs) and BAs that contract with other BAs need to be prepared, three privacy and security experts say.

Out of 503 reported breaches in 2018, 30% involved a BA, noted David Holtzman, executive director at CynergisTek. BA-related breaches often involve multiple CEs and commonly affect more individuals when compared to a single CE, he told attendees at the March HIPAA Summit in Washington, D.C.

In fact, the largest breach in 2018—the September breach involving more than 2.65 million patient records from Atrium Health and Baylor Scott & White Medical Center—originated with a BA, AccuDoc Solutions Inc., a billing vendor ("Vendor Hack Results in 2.65M Records Breached for Atrium Health, Baylor," *RPP* 18, no. 12).

Thora Johnson, chair of the healthcare practice at Venable LLP, added that OCR guidance has evolved on breaches involving BAs. The OCR guidance on cloud computing implies that a CE has a role in managing a BA, she said. The guidance states: "A covered entity (or business associate) that engages a CSP [cloud services provider] should understand the cloud computing environment and solution offered by a particular CSP so that the covered entity (or business associate) can appropriately conduct its own risk analysis and establish risk management policies, as well as enter into appropriate BAAs [business associate agreements]."

Johnson said that while guidance specifically states that CSPs are not required under HIPAA to provide documentation, or allow auditing, of their security practices, it notes: "Customers may require a CSP through the business associate agreement, service level agreement or other documentation to provide documentation of safeguards or audits, based on the customer's own risk analysis and risk management or other compliance activities."

"We are seeing more due diligence and more additional requirements placed on BAs," Johnson said. Holtzman added, "What we are seeing, is organizations are more actively assessing BAs' security. As we share more data and outsource more of the day-to-day functions of IT, your BA poses a quantifiable risk."