COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 32, Number 8. February 27, 2023
BAAs Have 'Become Almost Noise,' But BAs Were Implicated in Almost Half of 2022 Breaches

By Nina Youngstrom

When a hacker spoofed the email of an employee at a health care consulting firm, it set in motion a notification to clients that was mostly met with a shrug. The hacker had sent emails to the employee's clients with the intention of infiltrating their email accounts and gathering more contacts, but one of them recognized it was phishing and tipped off the consulting firm. Although the hacked email was shut down immediately, the consulting firm was concerned because some clients send unsecured protected health information (PHI) through email. As their business associate (BA), the consulting firm sent letters to clients who were potentially affected and explained the details of the security incident, said Regina Alexander, who worked for the consulting firm at the time. The response was surprising: about a third of the clients ignored the letter, another third asked one question about it and the rest were attorneys who wanted a meeting to discuss it, said Alexander, now a principal with BerryDunn.

The relative indifference was emblematic of the attitude toward business associate agreements (BAAs), Alexander said. "The key point is it's a document that has become almost noise. It's one of those check-the-box compliance items that people sign without reading," she explained. That's unfortunate because covered entities (CEs) pay the price when things go wrong with their BAs, Alexander said at a Feb. 9 webinar sponsored by the Health Care Compliance Association. Alexander noted that BAs were implicated in about 51% of the HHS Office for Civil Rights' (OCR) reportable breaches in 2022 affecting 500 or more people. More powerfully, about 89% of people affected by breaches last year were attributable to the cases involving BAs.