Report on Patient Privacy Volume 19, Number 7. July 10, 2019 Scrutinize Your Subcontractors Closely, Security Experts Warn Following Massive AMCA Breach

By Jane Anderson

Covered entities (CEs) and business associates (BAs) need to re-examine their relationships with subcontractors and implement more stringent security protocols where necessary in the wake of the massive American Medical Collection Agency (AMCA) data breach revealed last month, security experts warn.

Details of the breach aren't completely clear—AMCA filed for Chapter 11 bankruptcy protection on June 17, and its bankruptcy petition includes a description of the breach. However, it is clear that health care industry consolidation, combined with outsourcing, means the size of potential breaches is increasing.

"Large data breaches will be more frequent, given the volume of IT outsourcing" and the amount of electronic protected health information (ePHI) held by health industry contractors, says Brian NeSmith, CEO and co-founder of Arctic Wolf Networks.

Roger Shindell, president and CEO of Carosh Compliance Solutions, adds that breaches aren't inevitable. "But a better job must be done in vetting of business associates," Shindell tells *RPP*. "The regulations actually require a covered entity to terminate their relationship with their business associate if the CE uncovers a pattern of non-compliance with the regulations and the non-compliance is not cured. This rarely happens, though."

The AMCA breach, which may have involved more than 20 million patients, hit the clinical laboratory industry hard: Quest Diagnostics Inc. reported that it had nearly 12 million patients involved; competitor Laboratory Corporation of America Holdings (LabCorp) had 7.7 million patients involved; and BioReference Laboratories Inc., a subsidiary of OPKO Health, had nearly 425,000 patients involved.

The breach went undetected for more than eight months—from last August until late March—and then wasn't immediately reported. The affected companies first alerted stockholders in filings with the Securities and Exchange Commission.

In its bankruptcy filing, AMCA stated that it first became aware of a potential problem when it received a series of common point of purchase (CPP) notices. When credit card fraud is detected, banks analyze the data to identify the "point of purchase" the cards have in common, since that business could be the source of the data breach generating those stolen credit card numbers.