COSMOS
Navigate the Compliance Universe

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.

In response to the CPP notices, AMCA reports in its bankruptcy filing that it "shut down its web portal to prevent any further compromises of customer data, and engaged outside consultants who were able to confirm that, in fact, [AMCA]'s servers (but not [AMCA]'s mainframe) had been hacked as early as August 2018." This hack led directly to the bankruptcy filing, the petition said, as LabCorp, Quest, Conduent Inc., and CareCentrix Inc., the company's four biggest clients, either terminated or substantially curtailed their business relationships with AMCA.

AMCA said in its petition that IT consultants cost it $400,000 to determine the source of the breach. In addition, breach notification cost it "in excess of $3.8 million," which "required more liquidity than [AMCA] had

available."

The company faces additional legal trouble. Two state attorneys general—Connecticut Attorney General William Tong and Illinois Attorney General Kwame Raoul—have opened formal investigations into the breach, and a third—Michigan Attorney General Dana Nessel—has asked for additional information from the company.

Also, multiple class action lawsuits have been filed against AMCA and its clients, including LabCorp and Quest Diagnostics. The class action lawsuits claim that the company delayed notifying victims of the data breach, and failed to implement security that could have prevented the breach.

Do Companies Properly Vet Contractors?

It's not clear exactly what might have caused the breach. AMCA has not provided details publicly beyond what it wrote in its bankruptcy filing. But HIPAA security experts say there are specific steps CEs and BAs should take in the wake of this breach.

Shindell acknowledges that he's speculating on the cause of the AMCA breach, but he notes that "in my experience, credit card processing firms tend to rely on PCI [payment card industry] as their go-to security protocol. Adding a HIPAA-focused privacy and security program would be beneficial."

Generally speaking, Shindell says, "most organizations do an inadequate job of evaluating their business associates for their HIPAA compliance. Spending more time in this kind of evaluation would have a significant impact in mitigating the possibility of a breach occurring."

David Harlow, principal at the health care law and consulting firm The Harlow Group LLC, also declines to speculate on what the companies involved could have done to prevent this particular breach. But he did offer some general guidance.

"I believe that a certain percentage of breaches are in fact inevitable, because not [all] vulnerabilities known to black hat hackers are known to white hat hackers or security professionals in advance of exploits, and not all known vulnerabilities are patched," Harlow tells *RPP*.

"However, many significant breaches over the years have been due to poor data hygiene, including the failure to prioritize sufficiently the preventive measures necessary to frustrate bad actors." These include patching systems as soon as they are made available, and auditing the compliance capabilities and practices of BAs, he says.

Harlow adds, "Implementing best practices consistently may not necessarily have avoided this latest breach, but doing so would have prevented many of the breaches we've seen in the headlines."

Specific Steps Urged to Manage Vendors

Obviously, a CE that uses BAs is dependent on those BAs to safeguard protected health information. But that doesn't mean there's no role for the CE to play, NeSmith says.

"This is a matter of vendor risk management and ensuring that the people you are doing business with have adequate security controls to protect your sensitive data," says NeSmith. "If someone has outsourced IT services, it is incumbent on them to ensure that they have decent security in place. While there is no way to absolutely guarantee security in someone else's environment, vetting and auditing your vendors can minimize the risk."

Shindell adds that CEs and BAs should ask their subcontractors very specific questions, which should include: "Did the BA conduct a risk assessment" as per the National Institute of Standards and Technology (NIST) *Guide*

for Conducting Risk Assessments—NIST SP 800-30 Rev. 1 (2012)? "Did they generate a remediation plan? Is there a policy and procedure manual developed through the remediation process? Do they conduct adequate training? Can they provide documentation attesting to the above?"

NeSmith points out that businesses have different appetites for risk, which will affect security protocols and how they choose their vendors. "Covered entities and business associates need to arrive at their risk appetite and make the investments to meet that goal. Covered entities need to ensure they are properly vetting their business associate supply chain and auditing that supply chain." NeSmith adds that he has seen some CEs and BAs using the Standardized Information Gathering (SIG) and SIG Lite questionnaires to qualify their subcontractors.

BAs and subcontractors need to undergo "comprehensive review" before they are entrusted with data, Harlow says. "This includes requiring them to complete comprehensive questionnaires and assessments." Regular audits also are essential, he says, adding, "this is not a 'set it and forget it' kind of function."

Look for vendors who have taken steps to earn certification, Harlow recommends. "The best indication of vendor preparedness to deal with known and unknown security vulnerabilities and breaches [is] internal or third-party attestation of compliance with broadly accepted standards—e.g., NIST Cybersecurity Framework or HITRUST CSF."

Automated processes that limit key human factor vulnerabilities also are important, he says, noting that "reducing in a responsible manner the number of human touches required for all functions of the BA or subcontractor will likely increase the security of the data in question."

NeSmith points out that companies should actively monitor systems and have a plan they can implement instantly if a breach occurs. "Contractors need to have adequate security that includes protective measures and detection so you can slam shut the window of vulnerability once something gets compromised," he says. "Having adequate monitoring can mean the difference between a compromise and a catastrophic data breach."

Regular review of data minimization and data segmentation practices also is critical, Harlow says. "Does your BA need to have all of the data? Could it be segmented or anonymized or de-identified in a manner that still allows the BA to discharge its functions? Some level of inconvenience and expense is worthwhile if it can help minimize the chance of a significant data breach."

Finally, it's important to perform real-world tests, such as those involving fake phishing emails, to see where security is lax or could be improved, Harlow says. "If they click where they shouldn't, they get re-education rather than triggering a breach." Humans often are the weakest link in the entire security infrastructure, he points out. Real-world tests should include simulated cyberattacks in the form of penetration testing, he says, as "these are a critical component of any robust data security system."

Security requires CEs and BAs to take multiple steps in a variety of systems, experts say. "Most breaches are not terribly high-tech," Shindell says. "Most breaches are caused by a series of small mistakes that grow. Training is the cornerstone of a robust security and privacy program. OCR suggests that almost all breaches can be tracked back to inadequate training being a contributing factor."

The AMCA data breach shows that CEs and BAs need to "up their game" to protect ePHI, which includes monitoring their environment to detect threats that might slip through, NeSmith adds. "Covered entities will probably be imposing more rigorous vetting and auditing for their IT outsourcing relationships. Business associates can expect to spend more time and resources demonstrating to their partners that they are following cybersecurity best practices."

Contact Shindell at rshindell@carosh.com, Harlow at david@harlowgroup.net or via his blog HealthBlawg, and

NeSmith via spokesperson Melanie Ford at ford@merrittgrp.com. ✧