Newsbytes, 7/16

Raymond D. Aller, MD, and Hal Weiner

How to minimize cybersecurity risks from business associates

Like parents, through the decades, telling their teenagers, "It isn't all about you," cybersecurity firms are sending health care organizations a similar message: It isn't all about you—it's about your business associates too.

To protect their data, health care organizations have to do more than secure their own information technology systems, explains James Christiansen, vice president of information risk management at Optiv Security, a provider of end-to-end cybersecurity solutions. They also need to scrutinize the security programs of current and prospective business associates, point out their vulnerabilities, and insist those vulnerabilities be remediated.

In a presentation at the Healthcare Information and Management Systems Society's annual conference earlier this year, Christiansen outlined a step-by-step approach to managing business associate risk, including a number of measures health care organizations, including pathology labs, should take when negotiating a business associate agreement. First, "make sure you spell out the security safeguards you expect the associate to adhere to, such as HIPAA 164.308," he said. And consider placing restrictions on whether a business associate can outsource a service that it provides for you to a subcontractor, a point, Christiansen told CAP TODAY in an interview, that is often overlooked. "Can the business associate outsource your service? If you don't say anything, that means yes. You can say in the contract, 'Yes, on the condition that you get our approval first.' Make sure your contract addresses this."

A contract should also allow the health care organization to perform security audits, Christiansen said. "If you do notice something amiss, give them a set time—say, 60 days or 90 days—to get it fixed. And you need to check back; that's where I often see people fall down." High-risk vulnerabilities, he noted, obviously should take priority, and the time frame for fixing them should be spelled out in the contract, as should all steps for addressing them. "What are the penalties if they don't fix them? Is it treated as a breach of contract? Will you receive a refund of service? You probably have performance service-level agreements, but maybe not in this area."

Determining how a business associate would handle a breach of health care information is paramount: "If they have a breach, you want to make sure you're notified quickly so that you can minimize the impact to you," Christiansen said. On average, more than 230 days pass before a breach is detected, he added.

Furthermore, business associates should have cybersecurity insurance, he told the audience at HIMSS. And if a breach of the associate's IT system would pose a significant risk to your health care organization, "I would make sure they name you as an additionally insured."

Once the contract is in effect, "at least every year you should go back and re-review their security and make sure they maintain their security program," Christiansen said. If a security vulnerability is found, both parties need to agree on how to address it. And, "make sure you have an exit strategy" that includes the business associate destroying your institution's data if the partnership ends, he added.

Assessing the cybersecurity risk of current or prospective business associates can be broken down into a five-step process, Christiansen explained. First, thoroughly examine the business relationship, including the service the business partner performs and the terms of all contracts with the partner. Second, take a close look at the stability of the associate. “Are they two guys in a garage? Are they a very large company or a small one? What is the risk of actually doing business with them?” The larger risks often lie with smaller vendors, he added, because “large companies have big IT staffs and security staffs and spend a lot of time putting security in. A smaller organization simply doesn’t have those resources.” Third, look at how the business associate protects information. It should be working from a standard such as HIPAA and, for cloud-based providers, the Cloud Security Alliance’s STAR (Security, Trust, and Assurance Registry) program. Fourth, validate the security controls the business associate says are in place. “I always recommend to ask them first, ‘What are you doing?,’ then come back and say, ‘Show me,’” Christiansen said. Fifth, monitor the business associate for changes that could affect security. “If a company has only one security guy part time, and he leaves, their risk goes up very quickly,” he noted. “Nobody’s managing IDs, nobody’s watching logs, and so on. What if suddenly they go bankrupt? That just changed the profile risk.”

Based on the size and complexity of a business associate’s business, laboratory IT personnel should expect to devote 20 to 40 hours, before signing a contract, to thoroughly assessing the security controls of the vendor with which it wants to partner, writing a report for management documenting their findings, and creating a remediation plan to correct any deficiencies, Christiansen said.

Yet, because even the most thorough safeguards might not prevent a data breach, it’s critical that health care organization IT staff maintain “visibility” within their computer networks, Christiansen concluded. “Whoever is running the system should have the tools, people, and processes to monitor system activity and watch for intruders.” *—Jan Bowers*

Medical societies urge feds to alter interoperability measures

Thirty-six medical societies, including the CAP and AMA, have petitioned the Centers for Medicare and Medicaid Services and the Office of the National Coordinator for Health Information Technology to change how the government measures interoperability of electronic health records.

The organizations voiced their concerns in a letter to the agencies that it sent last month in response to requests from the ONC and CMS for information about assessing interoperability for the Medicare Access and CHIP Reauthorization Act, or MACRA.

The medical societies expressed their concern that many health information technology vendors’ claims of systems interoperability are really “little more than digital faxing.” Meaningful use measures “are a poor metric for interoperability, being too focused on the quantity of information moved and not the relevance of these exchanges or the underlying business case for transmitting data,” they continued.

The coalition requested that CMS focus on the “usefulness, timeliness, correctness, and completeness of data, as well as the ease and cost of information access. This requires measures that do more than count how many times voluminous documents are sent back and forth.” The medical societies further suggested that the ONC and CMS target specialty-specific interoperability use cases instead of focusing on the quantity of data exchanged.

The coalition concluded the letter by emphasizing its concern that failure to change the objectives of interoperability will “undermine advances in health care and will hinder a successful implementation of MACRA.”

Optra debuts digital pathology system in subscription model

Optra Systems has launched an on-demand, pay-per-usage model for its OptraScan whole slide imaging system and end-to-end digital pathology solution. Users will have access to all digital pathology components via a monthly subscription.

As part of the new model, Optra will provide its customers with an OptraScan cloud-enabled, compact, high-resolution scanning device with a 20× or 40× objective lens and 10-slide or 150-slide scanning capacity at no upfront cost. The monthly subscription will allow users to choose customizable slide-scanning packages dependent on their lab's monthly slide throughput. The complete digital pathology solution, for research use only, also includes cloud-based storage and around-the-clock service and support.

Also available on a monthly subscription basis are the Web-based OptraAssays image-analysis solutions; OptraCards system, which detects and highlights regions of interest based on OptraAssays' morphometric assays and algorithms; and OptraTelepath telepathology product.

***Optra Systems**, 408-524-5300*

Contracts and installations

- UniConnect has sold its Precision Molecular Diagnostics laboratory management system to Clinical Genomics, a developer of diagnostic tools for colorectal cancer. Clinical Genomics plans to implement the PMDx system in its molecular diagnostics laboratories in Bridgewater, NJ, and Sydney, Australia. ***UniConnect LC***, 801-428-1700
- Pathagility has installed its Pathagility laboratory information management system and reporting software at Advanced Genomics, a San Antonio-based commercial lab specializing in pharmacogenetic testing. *Pathagility*, 888-222-2792

[hr]

Dr. Aller teaches informatics in the Department of Pathology, University of Southern California, Los Angeles. He can be reached at raller@usc.edu. Hal Weiner is president of Weiner Consulting Services LLC, Eugene, Ore. He can be reached at hal@weinerconsulting.com.