Newsbytes

Tips for averting and halting security issues in the lab

December 2021—Like death and taxes, cyberattacks targeting health care organizations are a certainty, but taking proactive breach mitigation measures and developing a thorough response plan can lessen, or even prevent, a devastating blow.

“You’re never going to prevent every security attack,” says Emily A. Johnson, JD, member at the business advisory law firm McDonald Hopkins, “but having the right safeguards in place will go a long way.” In a webinar presented by Dark Daily and a recent interview with CAP TODAY, Johnson, who focuses on proactive breach prevention and regulatory compliance, described the measures that pathology labs, and health care organizations in general, can take to protect themselves from a breach of health care information or to address a security incident.

The most common error smaller organizations make is neglecting to implement security policies and procedures and perform annual security risk assessments—both of which are HIPAA requirements—until a breach has happened and a government investigation is underway, Johnson says. “Regulators are increasingly coming down on providers who don’t have those,” she notes. The hospital-based laboratory may be able to rely on the hospital’s security risk assessments if the lab isn’t housing protected health information, but a standalone lab “absolutely must do them.”

While an in-house information technology department can perform such assessments, it’s best to engage a third-party vendor, Johnson says. “IT usually implements the safeguards, so they might not come at it with as unbiased of an approach when trying to evaluate weaknesses and vulnerabilities,” she explains. The vendor will “assess your policies and procedures, look at your system, determine what controls you have in place, and perform penetration testing to see how easy it is to access your network.” While the assessment can be costly, insurance may cover it.

Johnson

To protect itself, the hospital-based laboratory should institute security policies and procedures, even if it isn’t housing PHI, Johnson adds, a critical component of which is describing the lab’s processes in the event of a security incident. “At the end of the day, you’re a separate entity,” Johnson says, and if the incident was caused by the lab, the hospital may turn to the lab as the responsible party even though the lab is located in the hospital. Therefore, the lab should work with hospital administration to ensure it’s following the hospital’s security protocols.

Formulating an incident response plan is another HIPAA requirement. An incident response team should include C-level decision-makers in the IT, legal, risk management, human resources, public relations, compliance, and physical security departments, as well as third-party response services, such as cyber liability carriers and cyber forensics specialists, Johnson says. Personnel from the hospital-based laboratory may not be involved with the hospital’s response team unless a security incident affects the laboratory information system.

Health care entities should test their incident response plans at least annually, Johnson adds. “I recommend a tabletop breach exercise,” in which an attorney poses a hypothetical incident scenario to the incident response team, providing an opportunity for the team to discuss the decision points in addressing a potential attack. Cyber liability carriers often partner with law firms to perform these exercises, which are often covered under cyber liability insurance. It’s important for health care entities to check with their cyber carrier to make sure such exercises are covered via their insurance plan, she notes. If the exercise isn't covered, the hospital or lab may want to hire a law firm to lead it.

"The scenario we use," says Johnson, "is a worst-case scenario, but it's one our clients have been through: The FBI shows up, there's a threat to go public with the information through the media, employees are involved and they're posting on Facebook, the phones are shut down, email's shut down." The exercise identifies potential communication breakdowns and other vulnerabilities in the organization's response plan. If the email goes down, for instance, "do you have backup phone numbers, home numbers, email addresses?" she says.

An additional mitigation measure, says Johnson, is to vet all potential business associates. If a business associate has a breach, "as a covered entity, your name will be mentioned in the notifications" to affected parties. Therefore, it's important to ask potential business associates about their security policies and procedures, how often they perform security risk assessments and audit assets, and if they offshore data, since the latter may pose additional risks. In the business associate agreement, include an indemnity clause and obligate the other party to carry cyber liability insurance, she says, in case the business associate can't cover the indemnity obligations.

Most security incidents are caused by human error, Johnson says, so train employees annually, if not more frequently. And use news events about cyberattacks as opportunities to retrain employees. "Say, 'How would this have impacted our organization?'" In addition, when employees leave the organization, terminate access to protected health information immediately.

If a security incident does happen, alert your cyber liability carrier right away, Johnson advises, so the carrier can engage its affiliated legal firm and cybersecurity forensic services to carry out an investigation immediately. The cost of the investigation should be partially covered by the carrier, she adds.

"Immediately start working with your incident response team," Johnson continues. "Make sure everyone is aware of the incident and is working off the same set of facts." And preserve all evidence from a cyber perspective. "Don't leave things up to IT," she says, because the information technology department may wipe everything clean and rebuild, "and then we have no evidence of the variant responsible for the attack, if it's capable of data exfiltration," or the attack's overall scope. While an incident doesn't always rise to the level of a breach, without that evidence, it can be difficult to rule it out. The laboratory may have to perform a time-consuming and costly manual document review to see what information has been exposed and notify patients because a breach is assumed unless there is evidence to refute it.

The incident response team should control the messaging, Johnson says. "Sometimes attacks cause panic among employees, or the threat actors will contact employees. So make sure the messages conveyed to workforce members and customers are consistent" with what decision-makers, such as the HR department, want to share. And call it a security incident. "Don't use the word 'breach' until your lawyers say you have a breach," even in private emails or other communications, she says. If the incident does rise to the level of a breach, the organization is obligated to notify the affected individuals within a set period, and calling the incident a breach before it's official could start the notification clock early. Furthermore, she says, the words "incident" and "event" are better received by the public than "breach."

Under HIPAA, the window for notifying patients of a breach is within 60 days of discovery, Johnson says. And the Office of Civil Rights, too, must be notified under HIPAA rules, although the timeline varies based on the number of patients affected by the breach. State laws also mandate that organizations notify the affected individuals and, in certain circumstances, the state attorney general. Some states, such as Colorado, have shorter notification timelines than does HIPAA, so it's important that laboratories be aware of their state laws, Johnson notes. The affected individual's residence determines which state's laws apply, regardless of where the organization is located. Therefore, a pathology lab operating in multiple states must determine where each affected individual resides and follow the state notification laws in each case.

Many states have instituted HIPAA exemptions, "which means if you notify the impacted individuals pursuant to HIPAA, you are considered to be in compliance with state law notification obligations," Johnson says. But even states with a HIPAA exemption may obligate organizations to notify the state attorney general.

Some states, such as Massachusetts, require organizations to submit a written information security plan to the state attorney general in the event of a breach. A WISP is a document that describes the organization's security policies and procedures and how that entity is safeguarding its systems. A WISP "can be similar to certain security policies and procedures" under HIPAA, Johnson says.

Hospitals and pathology labs also may have contractual notification obligations based on the terms of a contract between the organization and a payer, grant provider, or other entity. Under some grant contracts, the lab will be obligated to notify the grant provider when PHI housed by the lab has been exposed by a breach, Johnson says. Other times, the notification obligations apply only when data supplied by the grant provider is exposed.

Contractual notification obligations also may apply in a relationship with a vendor or client, she says. Labs usually are a covered entity, "but sometimes they function as a business associate, depending on the services they're providing, so they could have a business associate agreement obligation" to notify an upstream covered entity of a breach. The laboratory would notify the entity and then work with it to determine the entity's notification obligations.

Research contracts, Johnson says, tend to lay out notification obligations in greater detail than many other types of contracts, "so you want to look at that type of contract [closely] in the event that research participants were impacted by an incident."

The notification letter for any health care data breach should include a description of the incident and information exposed, the dates of occurrence and discovery, and "what you're offering to the impacted individual. Do you have a toll-free number they can call? Do you offer credit monitoring? Do you offer identity theft insurance?" Johnson says.

Consider having a lawyer draft the letter, she advises. "Data privacy regulations, at least at the state level, are changing on what seems like a daily basis. The last thing you want is to have to send two letters to the same individual because the first wasn't accurate. So make sure you have the most current information, and I would leave that up to the professionals."□

—Charna Albert

Lighthouse releases AI-based RCM software

Lighthouse Lab Services has introduced RCM Spotlight, cloud-based software that uses artificial intelligence to provide business insight and improve revenue cycle management.

"By using a copy of the standard claim and remit data labs already exchange with their payers, RCM Spotlight analyzes data using its proprietary AI engine to compare reimbursement and denial results across payers and similar providers," according to a company press release. "Users also have the opportunity to pair feedback with professional implementation guidance from our dedicated team of RCM consulting specialists at Vachette Pathology."

The software allows pathology laboratories and health care billing companies to detect changes in denial patterns, perform fast denial root-cause analyses, prioritize recoverable denials, compare payment performance with peers, and receive a monthly scorecard and analysis reports.

Lighthouse Lab Services, 844-789-4874

Xifin introduces latest version of RCM system

Xifin has launched Xifin RPM 14, the latest iteration of its flagship revenue cycle-management solution.

Xifin RPM 14 features a suite of updated capabilities, including workflow automation through Web services that supports two-way real-time data exchange. This enables digital “conversations” between client and patient portals, lab information systems, electronic medical record systems, computerized physician order-entry applications, and other systems.

Diagnostic providers can share test results with patients through the patient portal and send them text notifications or emails with a link for viewing test results. In addition, referring physicians and their staff can review interactive statements, dispute pricing, or rebill insurance via the client portal. Diagnostic providers receive notifications when invoices are available.

The software also offers additional dashboards to support executive, financial, and operational analyses and enhance decision-making.

Xifin, 866-934-6364

New QR code in CGM LIS transmits COVID-19 patient test results

Clinical laboratories using CompuGroup Medical’s CGM LabDaq or CGM SchuyLab laboratory information systems can now provide patients with a QR code that links to their COVID-19 test results.

“This new QR code feature helps our laboratories deliver real-time access to results while ensuring the highest degree of patient safety,” said Derek Pickell, CEO of CompuGroup Medical US, in a company press release.

Laboratories can link COVID-19 test results to a QR code on the patient report. For privacy purposes, the laboratory generates a special report in CGM SchuyLab containing only the desired results or a split group in CGM LabDaq that separates the desired information from other test results generated through the same order.

Laboratories using all versions of CGM LabDaq except version four, which does not support the new functionality, provide results via the CGM LabNexus laboratory outreach solution. Labs using CGM SchuyLab provide results through the CGM SchuyNet Web portal.

CompuGroup Medical, 800-359-0911

Dr. Aller practices clinical informatics in Southern California. He can be reached at raller@usc.edu. *Dennis Winsten is founder of Dennis Winsten & Associates, Healthcare Systems Consultants. He can be reached at* dwinsten.az@gmail.com.