BATTLING BREACHES

RULES, REGULATIONS & REINING IN THE PLAYERS

BY BETH WALSH

When it comes to the privacy and security of personal health information, there is always room for improvement, says Cris V. Ewell, PhD, chief information security officer for Seattle Children's Hospital. And the final privacy omnibus rule could easily put those providers that haven't kept up with the requirements even further behind.

ASSUME A COMPROMISE

Seattle Children's has a mature privacy and security program that Ewell operates under the assumption that a breach is going to happen. "I assume that our environment is going to be compromised." Developing a privacy and security program around that assumption helps determine how to best allocate resources, he says.

"Many hospitals rely on protection mechanisms for perimeter control, much like a drawbridge or moat around the castle, but it doesn't work. It's good because you have to have that, but it's not going to protect you 100 percent." Ewell runs a risk-based program to help make protection decisions. "You can't protect 100 percent of your assets 100 percent of the time."

Assuming a breach will happen at some point also is the viewpoint of Doug Copley, chief information security officer for Beaumont Health System, which serves metro Detroit. "It's not a question of if a breach will happen, but when."

To prevent a breach, Beaumont uses a tool specifically designed for its EHR system to conduct user activity audits. The tool reports on user activities within the EHR. For example, parameters can be set to report unusual activity. "We terminate people who access records inappropriately. We have caught people looking at their manager's record even though we tell employees that it is a surefire way to get fired."

Beaumont currently is deploying data loss prevention software, another monitoring tool that allows the IT department to set up triggers for certain data transactions. For example, if someone attempts to upload a file of thousands of patient records to his or her email account as


Source: Seattle Children's Hospital

Cris V. Ewell, PhD, Chief Information Security Officer for Seattle Children's Hospital, operates under the premise that a breach will happen.

an attachment, a pop-up message will question the activity. "The tool allows flexibility about what we want to do with the alert," Copley says. They could silently report activity to the IT department, establish a pop-up message for high-risk activities or block the ability to perform an activity. "To me, it's one of the best tools out there to prevent data loss."

Monitoring user activity is key because staff training, in general, is lacking, Copley says. He has worked in other industries and found that all companies can improve in this area. "It's a shame because raising people's awareness is a very inexpensive control to reduce the repercussions to both them and the company." The problem, he says, is that training is viewed as disruptive and a nuisance. But, "the more you can do, the better off you are."

At Seattle Children's, staff awareness begins with an optimal governance structure, says Ewell. He has the ability to audit anything. He also reports to both the board of directors and the general counsel, an unusual reporting structure in healthcare "that helps set the tone that privacy and security is important and we take it very seriously."

Seattle Children's staff members are required to take annual training for privacy and security, which Ewell says is helpful, "but we're constantly out there talking to people and conducting random audits. All of this is necessary for individuals to understand it." He also teaches a course to the hospital's leadership.

ONGOING EFFORTS

Aside from staff training and awareness, providers need to continuously monitor privacy and security threats, says Ewell. "You need a process to do that because if you're not consistently and constantly looking at issues on a daily or weekly basis, you'll fall behind on threat factors in your environment. You have to know where your problems are to fix them."

To fight off threats, more and more healthcare organizations are encrypting their devices. Back in 2006, Beaumont had a stolen laptop, which was encrypted, but the password was on a sticky note attached to the computer, Copley says. The laptop was recovered and a forensic analysis revealed that a breach did not occur, but the incident already had made the front page of the local newspaper. In general, he says all computers, devices and USB drives should be encrypted.

Encryption is part of the solution, Ewell says, but without password protection, "encryption does absolutely nothing. All controls go together to strengthen your ability to protect information."

Another issue of growing importance is bring-your-own-device policies and procedures. "You need a strategy around what you're going to do when people want to bring in their devices," says Ewell. For example, Seattle Children's maintains a private network just for personal devices that links to no other information systems. Access is tightly controlled and users must go through middleware to connect to the hospital's network.

Source: Seattle Children's Hospital

Seattle Children's Hospital has a private network for clinicians to connect their personal mobile devices that doesn't link to any clinical information systems.

Recent settlements by the government have emphasized the importance of addressing various threats through a comprehensive risk analysis. Adam H. Greene, JD, partner at Davis Wright Tremaine law firm in Washington, D.C., says the rule indicates high expectations in this area. Organizations need to include tailored, detailed elements rather than a checklist of controls. They should look at their organization and determine the biggest risk, which will differ between covered entities. Not all hospitals, for example, are at a high risk of an earthquake. And, organizations should evaluate the risk of an employee putting protected health information on a personal device, Greene says. "Just because you have a policy that says don't do it does not mean there's not a significant risk. The U.S. Department of Health and Human Services [HHS] is looking for a high level of detail."

Privacy and security audits, which the Office of Civil Rights began conducting in 2012, provide another reason to refocus on risk analysis and business associates (BAs). Greene has seen the first 20 audit reports that indicate more security problems than privacy problems. For example, a big issue was organizations improperly using user activity monitoring by not turning on audit logs or regularly reviewing reports.

Risk analysis was another significant area revealed through the audits, Greene says, so don't wait until you have an incident or get an audit notice to make sure yours is up to date. While it's not clear what form the audits will take in the future, Greene is confident they are not going away.

The Omnibus Rule also raises numerous questions about BAs. "This is an area that needs attention," says Ewell. Twenty to 30 percent of his time is spent on contract negotiations. "I get involved if anybody wants to change a BA agreement and the security and privacy language. That's my way of making sure they understand their responsibility. It takes that level of involvement." While vendors and BAs are becoming more aware, he says, "sometimes we're still informing them of the law. It's an educational process, and we have a long way to go."

Covered entities should revisit their BA agreements, says Greene. "It's more important than ever

before for covered entities to understand their BAs and whether they have good practices in place.

FINAL RULE PRESENTS CHALLENGES

The Omnibus Rule, which HHS issued in January, revises a significant number of HIPAA requirements. For example, the rule moves the concept of a breach from significant risk of harm, which was a solid and respectable harm threshold, to a presumption that there's been a breach unless the covered entity can demonstrate low probability the data have been compromised, says Lisa Sotto, JD, managing partner at the New York City office of Hunton & Williams law firm. That change requires covered entities and BAs to prepare a formal risk assessment, so they can later demonstrate to HHS why they didn't believe they needed to conduct a notification in a particular instance.

> Many subcontractors will have no earthly idea that they interact with HIPAA unless they are told via BA agreement.

The final rule defines subcontractors as BAs, which is "really difficult to manage," says Sotto. Subcontractors are just as responsible for compliance as BAs, and that follows subcontractors down the line all the way to the end of the data stream. A covered entity could have 30,000 BA agreements and every single one will require amendment.

Unfortunately, "many subcontractors will have no earthly idea that they interact with HIPAA unless they are told via BA agreement," says Sotto. If there is a failure of communication, subcontractors will have direct liability under the new privacy rule, but they won't even know it.

The rule also finalizes the breach notification timeframe, which could be very challenging for many organizations. While the requirement to conduct your breach notification within 60 days was in the 2009 interim rule, Ewell points out the final rule's preamble includes strong language on the topic. Sixty days is not a lot of time to "assimilate, analyze and make a determination of breach and then make the notification," he says. "You need a very mature process to manage that."

HHS says that 60 days to notify is "the outer limit," says Sotto. "In some cases, even waiting that long will be considered an unreasonable delay." Based on her experience helping organizations manage breaches, "a number of breaches are not susceptible to notification within 60 days. It can take months to determine the scope of a breach, but there is no flexibility in this standard."

Aside from the new and long-standing rules and regulations governing privacy and security, determining the very scope of a data breach presents further challenges. "The term covers such a broad spectrum of activity from the most innocuous, like a stolen laptop, to the most malicious, so it's hard to put your arms around any kind of fix." The laws increase awareness so that more and more companies are taking basic data security measures but human error is always at play, she says. Deep awareness and a strong incident response team are critical components of a hospital's privacy and security program.

"You need a strong framework of policies and procedures and compliance with those policies and procedures. They need to be updated constantly in the never-ending battle to protect data." CI+T