Healthcare IT News

CIO Spotlight: Ed Ricks on managing business associates and third-party privacy risk

With about 200 subcontractors to deal with, “that’s a lot of people that we’re trusting to do the right thing with our patients’ data,” says the Beaufort Memorial Hospital CIO. “We want to stay on top of it.”

By Mike Miliard March 27, 2017

Ed Ricks, CIO of Beaufort Memorial Hospital

Speaking at HIMSS17 this past month, security consultant Kevin Johnson made the point that far too many health organizations still “don’t truly understand” the array of security threats they face. It’s not just nefarious hackers, he said. The privacy risk posed by negligence from trusted third-parties such as vendors and other business associates is “astronomical.”

Ed Ricks, chief information officer of Beaufort Memorial Hospital in Beaufort, South Carolina, is one IT leader who does appreciate the threat that third parties pose to patient data.

That’s not to say, however, that it’s an easy threat to manage.

Beaufort Memorial deals with about 200 business associates, said Ricks. “And we’re not gigantic. We’re a 200-bed community hospital. But that’s a lot of people we’re trusting to do the right thing with our patients’ data. That is a lot, and we want to stay on top of it.”

The HIPAA Omnibus Final Rule of 2013 broadened the definition of business associates and upped the stakes for potential financial penalties when they mishandle patient data. That means managing business associate agreements and keeping apprised of their status is imperative.

“Our biggest challenge was just making sure we knew who was really a business associate,” said Ricks. “People struggle with that.”

Ricks uses software to track business associates status across the organization. The Partner Risk Manager tool from Iatric System helps with due diligence, he says, offering capabilities such as vendor tracking and screening to spot potential risks, and the ability to send alerts if contractors associated with terminated BAA access ePHI. That, combined with rigorous internal access audits, gives him and his team visibility into where and when electronic protected health information is accessed, whether inside the hospital or out of it.

“For lack of a better way to say it, it’s an electronic filing cabinet with a good tickler system,” said Ricks. “Things don’t fall through the cracks, things don’t expire. Any time we contract with any vendor on any of the relationships, then we go through the analysis: Are they a business associate or not?”

A dashboard to keep IT teams posted about the status of dozens or hundreds of BAAs is a valuable tool in an era where OCR enforcement is both more widespread and more pointed.

“We set the software up so we knew who the business associates were, who we were working with, who all our contacts were,” said Ricks. “We need to have that information now. So if we do get audited – before, without it, we would have been lost. Even though we felt like we had the right documents somewhere on file. This makes it much easier to get the information together.

“There’s sometimes a lot of mystery around that: are they a business associate, or are they a covered entity? Are they really going to have ePHI of ours? So we go through that algorithm,” he added. “Some people are good with what our attorneys have drawn up to be a sort of standard. Some companies want to doctor it up a bit, so there’s some back and forth on that. We make sure we get the right elements in the BAA.”

The technology has helped free up enough time, said Ricks, that he and his team are able to focus on more robust risk prevention.

“Now what we’re actually talking about doing – I don’t know if we’ll be able to pull off, but we may get someone to help us – is doing audits: Doing real, technical audits, which is something (our business associates) agreed to. We can go in and treat them like we treat ourselves, hold them to the highest standards of technology and process. We want to go in and at least do a tabletop exercise.

“Iatric always understands that there are all these small niches that people don’t really fill for you that make sense,” he said. “Whether it’s around security, or just making you a little more efficient.”

Ricks also uses the company’s Security Audit Manager, for instance – a machine learning technology that helps manage privacy by homing in when inappropriate activity is detected with patient data. Its tracking tool enabling easier data collection, analysis, breach risk assessment and incident response.

“It takes a lot of the complexity out of just doing the easy audits,” said Ricks. “We have a small staff – I have just one engineer who’s cybersecurity focused, and he’s got to do a lot of things. So if we can just have this stuff running in the background, bringing the appropriate alerts forward to us, we can manage those.”