Ensuring HIPAA compliance among inpatient, outpatient docs
Kyle Murphy, PhD | June 3, 2014

The continuum of care continues to expand and is forcing integrated delivery networks and health systems to reconsider their health data privacy and security practices after addressing the features unique to inpatient and outpatient clinical settings.

Over the past several years, one of the largest non-profit health systems in New Jersey has increased the size of its organization through the acquisition of physician practices and taken upon itself the task of making these ambulatory providers as HIPAA- and HITRUST-compliant as their inpatient counterparts.

“From a hospital perspective, we’ve been doing information security risk assessments since 2004 — third-party, outside — that includes penetration testing and all kinds of things,” says Atlantic Health System Vice President and CIO Linda Reed, MSN, RN, MBA. “A couple years after that, we started performing annual HIPAA assessments in which we run through what would happen if a HIPAA auditor came in. A few years ago, we extended this process to the physician practices because as we acquired more and more of them we had to make sure that they could also pass.”

Ensuring privacy and security on the inpatient side

Consisting of four medical centers, one children’s hospital, and a growing number of physician practices, the various settings have different health information technology in place and therefore differing perceptions of what best practices in health data security and privacy entail.

On the inpatient side, a trend toward mobility and virtualization has help eliminate potential gaps data security and privacy and increase access for clinicians. Recently, the New Jersey health system implemented a secure clinical communication tool called Imprivata Cortext to complement its virtualized desktop and single sign on functionalities.

“We’ve had something called mobile rounding in place for a long time and the physicians got used to it, but what happened is that you had to have a piece of software on your device and it didn’t let them to talk to each other,” explain Reed. “As texting became more ubiquitous and easier to use, they began using that and very quickly we all knew that that’s not a secure medium to do that, especially if you’re going to use PHI.”

The decision to implement the secure texting tool came about as a means of safeguarding even well-intentioned providers against themselves in a convenient way.
Ensuring HIPAA compliance among inpatient, outpatient docs

“Telling them not to doesn’t help because they are going to do it anyway,” Reed continues. “Everybody puts the same policies in place — we did just like everybody else — no texting allowed and it promptly gets ignored. We figured that we had to put something in place as an alternative so if you are going to talk to someone or if something does happen, we do have the secure texting tool.”

According to Reed, physicians sometimes cannot help themselves when working to improve the outcomes of their patients despite mandatory training about vulnerability and breaches. “So even though they know, they need to get something done. Physicians are the ultimate pragmatist. Sometimes there is that mentality — it won’t happen to me,” she reveals.

**Ensuring privacy and security on the outpatient side**

In her dealings with physician practices and extending the health system’s health data security and privacy practices there, Reed quickly realized that a different kind of approach was necessary to bring these outpatient settings into a compliant state. “It is still a concern when we acquire physician practices. Some of them are not hosted and running their own little servers sitting in an unlocked office somewhere under a desk,” she maintains.

The New Jersey health system has taken a direct approach to mitigating risk by putting boots on the ground.

“We go into the offices and do a walkthrough,” Reed explains. “We take a look at where their screens are placed, where all the technology is, where the printing winds up. We’ve also done a bit of social engineering testing — calling the office and seeing if you can work a password out of somebody. And it does happen at times. Having the HIPAA audit, having all the HITRUST stuff documented — we put that all in place.”

The process is particularly important for eligible professionals in the EHR Incentive Programs for whom meaningful users for whom the risk analysis is required and a major focus of auditors.

“As you look at meaningful use many folks skipped that piece,” argues Reed. “I don’t know if it just didn’t occur to them or they didn’t know what it meant. They had checked it off as doing it, but they never did. It’s fascinating.”

For these physicians, working with a regional extension center has paid off, says Reed. However, the risk is still there for those practices looking for a quick or cheap fix.

“It depends on who is doing meaningful use for some of these offices,” she observes. “Some of them were working with our regional extension center and got some good direction and tools from it, but the ones who were doing it on their own found it a little difficult. There are lots of people out there selling info-sec security assessments you can do yourself — that’s a little frightening.”

To reduce risk the Atlantic Health System has worked to move practices from an onsite to hosted EHR system before ultimately making one system available to these providers in the long run. “If we can
move them to a hosted version, that’s probably the best option for us temporarily until we can start rolling everyone on to the single EMR,” adds Reed.

Until then, the onus is on providers in both settings to be trained and tested on their health data privacy and security practices.