Low-Tech Threats in a High-Tech World

By Genna Rollins

Despite the rise of health IT, healthcare providers still face daily privacy and security risks of the mundane variety—paper records are misplaced, improperly disclosed, or released without confidential information redacted. No matter the opportunities and risks that technology brings to securing health information, often the hardest element of a privacy program to control is the human one.

This was clear last February when Massachusetts General Hospital reached a settlement with the US Department of Health and Human Services in a case involving potential violations of the HIPAA privacy rule.

Though Massachusetts General has been a pioneer in the development and implementation of health IT and bioinformatics, the incident that precipitated the settlement was decidedly low-tech: an employee commuting to work left paperwork on the subway.

Among the lost documents were billing encounter forms that included patient names, dates of birth, medical record numbers, health insurer and policy numbers, and diagnoses. The documents never were recovered.

The lapse is a sobering reminder of how challenging it can be for any institution to safeguard patient privacy, even an era of dramatic technological innovation, says Peg Schmidt, RHIA, chief privacy officer at Aurora Healthcare in Milwaukee, WI.

"When you hear of an Office for Civil Rights investigation like this and see what it involves, you can't help but think, 'That could be my organization,'" she says.

In addition to a $1 million fine, Massachusetts General entered a corrective action plan in which it agreed to develop, implement, and train staff on a comprehensive set of policies and procedures designed to ensure that protected health information remains private when removed from the institution's premises.

Like the incident, the solution is also decidedly low-tech. And that reflects a foundation of privacy programs, say experts: understand the risks, create policies and procedures to mitigate those risks, and educate staff on following the rules—provide a high-touch effort for low-tech situations.

Trend It Closely

Understanding your weaknesses, Schmidt says, is a first step in reducing them. Collecting data on the facility's privacy breaches enables critical assessment of the problems.

"You have to know what's wrong in order to educate people. We try to track violations with enough granularity that we can pinpoint groups of problems. That way we know what to focus on and what we need to educate staff about," she explains.

Judi Hofman, CAP, CHSS, is a privacy and information security officer at St. Charles Health System in Bend, OR. Her facility uses software to make tracking as easy for staff as possible.

"We use an event management system to track a number of things, like sentinel events, and our staff is used to using it as a tool. We encourage them to use it to report any ethical or privacy concerns, and having this tool empowers them to do so," she says.

Hand-in-hand with robust reporting mechanisms is the need to recalibrate expectations around what to report, according to Schmidt.

"In the old days we might not have thought it was a big deal if a staff person misdirected a fax to someone outside the organization. It would have been addressed at that time, and that would have been it," she says. "But now we expect employees to report something like that."

Federal breach notification laws enacted in 2010 play some part in that. Organizations must report certain breaches of unsecured, protected health information to the Department of Health and Human Services.

A misdirected fax "may seem like a little thing," Schmidt says, "but it's still a disclosure, and we have to review it to see if it's a notifiable violation."

Trend information detailing the leading departments and types of violations helps focus education and remediation efforts, Schmidt says, both narrowly and broadly.

"Of course we address individual events, but if you do one-on-one counseling or training, you teach one individual. That person's peers could have the same problem, so we try to take the next step and discuss expectations within that department," she says.

Trend data also serve as the backbone for Schmidt's annual privacy education plan, a multipronged approach to reinforce privacy topics in a variety of forums. In addition to required annual training, which takes the form of an online, scenario-based module, she places monthly reminders on Aurora's Intranet, often tied to news of incidents at other organizations or unauthorized disclosures that have taken place at Aurora.

"We try to come at them in different ways, and not just present the same old HIPAA basics," she says of her education efforts. "We're trying to build a culture of privacy, so all staff see it as theirs to own, not just the privacy officer's responsibility."

Spell It out in Policy

In addition to educating employees upfront and counseling them when mistaken disclosures occur, Hofman closely scrutinizes contractors as well.

"You could have a mom-and-pop courier service, for example, that is licensed and bonded, but they might subcontract to someone who isn't," she says.

Hofman and Schmidt also regularly review policies and tighten them when it seems prudent to do so.

"We're trying to be a little more proscriptive and make stronger policy statements," Schmidt says. "So instead of a general statement about protecting records when an employee is transporting protected health information, we're going to make more definitive statements around that, such as that the information must be locked in the employee's trunk."

Once adopted, policies must be applied fairly and uniformly, she adds. This holds true for individuals, roles and functions, and facilities within the enterprise. Organizations that apply their policies inconsistently—terminating a clerk for a violation but only warning a surgeon, for example—send a damaging message to staff, suffer a loss of credibility should the event become public, and increase their liability in the event of an investigation. (For more, see "Sanction Guidelines for Privacy and Security Breaches.")

Deliver It Personally

John Jenson, CHPS, CIPP, makes a pitch for privacy in person with as many people as he can. In fact, he considers himself somewhat of an internal consultant at the University of Minnesota, where he is assistant director of privacy and security.

"I strive to have clear and constant communication. Whatever committee I can get before, I try to get my name on the agenda," he says. "It's not sexy, but this enables staff to ask questions of me they might not otherwise, and I get the chance to ask questions that [are beyond the] traditional HIM [scope of practice] but help us improve privacy."

Jenson has been known to question managers about recruiting and hiring practices as well as work requirements. For example, he may ask, “Have we made demands on our employees that lead them to make decisions they otherwise wouldn’t?”

Jenson, also a proponent of tracking and assessing lapses, says that thorough analyses of even a single breach can reveal opportunities to make system-wide changes for the better. “When you combine poor data collection practices or other low-tech lapses with a bad technical decision, then you end up with a worse incident,” he says.

In his consultant role, Jenson seeks to understand a department’s needs and then find a way to meet them in the framework of privacy requirements.

People still think of HIPAA in terms of those things it prevents them from doing, he says. “But I always ask, ‘What is it that you’re trying to do without having considered HIPAA?’ Once I hear that, I’ll explain what HIPAA allows, and then there’s always a better result. We structure something that is compliant and still helps them with their business,” he explains.

As an example, Jenson points to the research studies taking place at the university. Many of the hospital’s clinical research coordinators wanted to maintain participants’ Social Security numbers so that they could track down those who drop out of studies. Jenson had an alternate suggestion.

“I suggested that they let my office take over finding people and that we keep the patients’ Social Security numbers,” he says. The idea was to get researchers into the habit of keeping as little patient information as possible—only the information they required to conduct their actual research.

The personal connection is essential in helping departments tighten up everyday security, Jenson stresses. “Many people don’t want to come to me until there is a problem—the privacy officer is to be avoided. But I want to get people out of that mindset,” he says.

“I want them to realize there’s a better way to do healthcare and HIPAA. No one is here just to do HIPAA. We’re here to provide care, perform research, educate clinicians, and to do it in ways that protect privacy.”

Genna Rollins is a freelance writer specializing in healthcare.

Original source:
Rollins, Genna. "Low-Tech Threats in a High-Tech World" (Journal of AHIMA website), April 2011.
