Part B Insider (Multispecialty) Coding Alert

Patient Privacy: Report: Data Breaches Increase in Early 2015

Breaches rose by 10 percent in first half of this year versus last year's numbers.

The United States is home to about 320 million people, which may sound like a high number—until you hear that nearly 246 million records were compromised in the first half of this year. That staggering number came as the result of 88 data breaches in early 2015, most of which occurred in the healthcare field, said digital security company Gemalto in its report, "2015: First Half Review—Findings from the Breach Level Index."

Anthem Leads Breaches

Among the many breaches was the hack into Anthem Insurance's servers, which compromised 78.8 million records that included protected health information (PHI). Because the Anthem breach was so massive, the leading source of data breaches in the first half of this year was malicious outsiders, which remains a growing threat, Gemalto said in its report.

Some 22 percent of breaches were attributed to accidental loss—a commonly-seen problem within Part B practices. This could include misplacing a laptop with medical records on it, losing an external hard drive that contains patient social security numbers or losing track of a box of papers with patient names on it.

The report underscores the fact that healthcare organizations should constantly be finding new ways to secure PHI. "It's apparent that a new approach to data security is needed if organizations are to stay ahead of the attackers and more effectively protect their intellectual property, data, customer information, employees and their bottom lines against data breaches in the future," the report notes.

Prep Now for HIPAA Audits

With HIPAA breaches growing despite continued education and regulations, the government is getting ready to institute its HIPAA audits, which will allow the feds to determine exactly what practices are doing wrong. But the problems could lie in the fact that HIPAA has been an ever-evolving bundle of regulations that practices have trouble following.

Although the initial HIPAA laws have been in place since 1996, the first privacy regulations covering PHI didn't come into play until 2003, followed by the security rule in 2005, said **Paul Hales, Esq.,** a healthcare attorney in St. Louis, MO. Unfortunately, not every medical entity was on board with the law at that point.

"I've found that the only people who were really paying attention were big organizations like health plans, hospitals, etc., and they already had the compliance, IT staffs and attorneys to handle it," Hales says. "The dentists, doctors, chiropractors, podiatrists and other small practices just didn't have the resources to comply, and the Department of Health and Human Services (HHS) didn't really enforce it, so breaches were occurring."

However, HHS prepared modifications during the Bush administration that were passed into law as part of the Stimulus Act in 2009. HIPAA now covers not only Business Associates who handle PHI, but even subcontractors working for those Business Associates. In addition, the Breach Notification Rule came into effect, HIPAA penalties skyrocketed, and HHS did a pilot audit of HIPAA programs in anticipation of a nationwide audit plan, Hales said. The HIPAA audits will likely start late this year or early next year, he added.

If the pilot audit results are any indication, the nationwide audit program could spell trouble for unprepared practices. "In 2012, HHS conducted a pilot HIPAA compliance audit in preparation for the mandatory, random HIPAA compliance audits that will begin soon," Hales says. "HHS found 80 percent of the providers had not conducted a risk analysis although it

had been mandatory since 2005. HHS also found that small providers have serious HIPAA compliance issues and 'struggle' with compliance."

Even Baby Pictures Could Violate HIPAA

Many practices fall victim to HIPAA violations due to keeping unencrypted PHI on portable devices. "Encryption is an algorithmic process that scrambles the drive and scrambles electronic data that is being transmitted," Hales says. "You need the key in order to unscramble it. So if you have a laptop that's encrypted in a way that meets the federal standard and it's stolen and it contains the PHI of 50,000 patients, that's not a breach because the encryption makes it impossible to read the information." Encryption is very inexpensive and simple to do, so practices that don't take advantage of that feature could be putting themselves at risk of a breach.

Other, less obvious issues could lead to a breach as well. For instance, if you hire a marketing company to create a website for your practice, chances are that you're going to include patient testimonials on it. "But what many people don't realize is that the patient must execute a HIPAA-compliant authorization for that testimonial," Hales says.

In the same vein, you can't paper your practice in patient photos which is particularly common with obstetricians. "A fertility specialist in Manhattan had to remove photographs of babies that his patients had conceived, and HHS said in order to post these, you have to have a HIPAA-compliant authorization," Hales says. "A picture of a face is one of the 18 identifiers that constitutes PHI."

Create Authorization Forms

In addition to your standard HIPAA lingo, your practice should create additional authorization forms such as those for patient testimonials to put on your website or on social media like your Facebook page. You might also need authorization forms for unexpected reasons. "Let's say a patient is in a car accident and there's a lawsuit involved the doctor has to have an authorization to release the information to the lawyer," Hales says.

To alleviate the problem for smaller practices, Hales created the HIPAA E-Tool on the internet to make HIPAA compliance affordable, accessible and complete. It has all required forms, policies and procedures and interactive step-by-step risk analysis to help a practice comply with the law.

"The E-Tool also includes sample Business Associate agreements as well as state health privacy and breach notification laws, which are more stringent than the national standards," Hales adds.

Resource: To read Gemalto's complete report, visit www.gemalto.com/brochures-site/download-site/Documents/Gemalto_H1_2015_BLI_Report.pdf.