Part B Insider (Multispecialty) Coding Alert

Take 3 Steps to Avoid Punishing HIPAA Penalties

Look for compliance clues in two new government reports.

Recent HIPAA reports mandated by the HITECH act may seem like jumbles of depressing statistics, but you can actually learn quite a bit from them.

Here are three key lessons you can glean from these reports:

1. Ratchet up your theft-prevention efforts. Theft didn't merely rank number one on the list of breach causes, it blew all other causes out of the water. Theft accounted for half of the breaches in both years (50 percent in 2011 and 53 percent in 2012), according to a blog post from health law attorney Leah Roffman with Cooley.

"The statistics in both reports clearly show that the most breaches still come from 'older' sources of PHI, such as paper records, desktop computers, and network servers," note attorneys Stephanie Willis and Dianne Bourque in an analysis for Mintz Levin Cohn Ferris Glovsky and Popeo, published in The National Law Review. But "in addition to updating and monitoring security protocols for older PHI sources, covered entities should address security problems with newer storage media," according to Willis and Bourque.

And specifically, the breach report shows a large increase in the number of breaches involving laptops, say Willis and Bourque. "Because theft was the primary cause of breaches in 2009 to 2012, ensuring that laptops and other portable devices are secured in accordance with standards acceptable under HIPAA will become even more important as organizations adopt more 'bring your own device' policies to ensure the mobility and convenience of health care delivery."

2. Keep a close eye on your BAs. Although Business Associates accounted for only 26 percent of the breaches in the reporting period, these breaches affected 59.3 percent of the total individuals affected by all the breaches reported. And the large number of affected individuals in breaches involving BAs likely reflects the reality that BAs may house PHI for multiple CEs, Willis and Bourque point out.
Action point: "Based on these statistics, health care organizations must impose standards for using BAs and subcontractors," Willis and Bourque urge. You must also ensure that your BAs and subcontractors understand their obligations under the HIPAA Privacy and Security Rules.

3. Beware of the cumulative effects of small breaches. Although small breaches those involving fewer than 500 individuals may seem like a far cry from mega breaches affecting millions of people, they can still seriously hurt your organization.

Reason: "The problem with small breaches for organizations is that they can occur more frequently than large ones," warn Willis and Bourque. "The occurrence of repeated small breaches can be indicative of a systemic compliance problem, and may suggest to a regulator that the organization has not taken steps to identify and remedy the problem."

That's why it's crucial for your organization to determine its breach risk profile, and identify and correct any compliance gaps, Willis and Bourque stress. "All covered entities should ensure that they account for the likelihood of small breaches as much as they do for large breaches when doing their security risk assessments."

Note: For help with your risk assessment, check out the **HHS Office of the National Coordinator's** Security Risk Assessment Tool for small and medium-sized health care providers at www.healthit.gov/security-risk-assessment.