Eli's Hospice Insider

HIPAA: Expect a HIPAA Compliance Crackdown -- Are You Ready?

Tip: You're not off the hook if the breach is your vendor's fault.

If you've jumped on board the electronic health records bandwagon, you're probably experiencing benefits such as reduced costs and errors. But if your patients' protected health information (PHI) data isn't secure, you could be headed for compliance headaches.

The American Recovery and Reinvestment Act (ARRA) intensified HIPAA requirements, and Congress has allocated more HIPAA security compliance enforcement dollars to the Centers for Medicare & Medicaid Services and the HHS Office of Inspector General, points out **Wayne J. Miller**, a health care attorney with the Compliance Law Group in Los Angeles.

Use this breakdown of the new HIPAA regulations to update your policies and procedures:

Stricter notifications: Under ARRA's HITECH provisions, you must notify patients "without unreasonable delay" and in no case later than 60 calendar days after you discover that unsecured electronic health information was improperly "accessed, acquired or disclosed."

But don't wait 60 days to get the word out, warned attorney **Michael Hale** with Poyner Spruill in Raleigh, NC during his presentation at the National Association for Hospice and Home Care's annual meeting. Your hospice is deemed to have discovered the breach when anyone other than the person who caused the breach recognizes the potential problem -- and that includes volunteers. Be sure to train staff so they know who to tell when they suspect a breach, Hale said.

Unsecured PHI is data that wasn't secured through the use of technology as defined by the Department of Health.

Good news: Breaches of secured PHI have no reporting requirements, Hale said. So PHI that is rendered unusable, unreadable or indecipherable and PHI that meets National Institute of Standards and Technology (NIST) standards and is encrypted, shredded, cleared, purged, or destroyed aren't subject to reporting.

Safe bet: Ask your IT staff to carefully review the NIST guidelines to make sure you are storing and destroying PHI accordingly, Hale said.

Plan the Notification

You are required to notify affected patients by first class mail. If you have no address, you'll need to use a substitute form such as a Web site, major publication, or newspaper, Hale said. However, if the patient affected is deceased, and you have sent notification to next of kin or another responsible party, there is no need to notify by a substitute form.

If the data breach affects more than 500 people, you must also notify prominent media outlets in your state or jurisdiction and report the incident immediately to the Department of Health and Human Services. The notification should include the following, Hale said:

• A description of the breach including the date it occurred

• The types of unsecured PHI involved such as social security number,date of birth, diagnoses

• The steps affected individuals should take to protect themselves

• A description of what your hospice is doing to investigate, mitigate harm, and make sure such a breachdoesn't happen again

• The appropriate contact information for the affected individual to use

Keep a record: Make sure you document all unsecured PHI breaches of any size in your hospice. The Dept. of Health and Human Services may ask to review this information on an annual basis, Hale said.

Enforcement shift: For the first time, ARRA extends liability for HIPAA violations directly against business associates and forces them to comply with the same security standards as providers,explains Miller.

You will likely need to modify your business associate agreements as a result, he suggests. Not everyone you do business with, however, qualifies as an associate -- for instance, a credit card company that processes your transactions would not be a business associate under ARRA. But a billing company or any other entity that keeps records for you would qualify, explains attorney **Michael C.Roach** of Meade and Roach and the Aegis Compliance & Ethics Center in Chicago.

Eye on disclosures: In addition,you are required to restrict all thirdparty protected health information (PHI) disclosures to a "limited data set" or the "minimum necessary," including those disclosures you make to health plans, said attorney **Steven J. Fox** at Post & Schell in Washington, D.C., during a recent Fierce Live webinar.

"Limited data set" and "minimum necessary" are defined in the original HIPAA regulations, so providers should look to the law's text when setting disclosure guidelines,Fox tells Eli. Also, expect to account for all disclosures you make from EHRs, including those for treatment, payment, and health care operations.

Marketing crackdown: The stimulus bill places new restrictions on the sale of PHI and marketing practices as well, added Fox.