Health Information Compliance Alert

HIPAA: Prepare Now For Heightened Privacy And Notification Protections

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

Making the electronic health record transition may cut costs and reduce errors, but you also are bound to face increased compliance risks -- and increased federal scrutiny.

Wake-up call: You are accountable for compliance even if a third party installs and maintains your system. Physicians will still be responsible for ensuring the same privacy protections as if they did have their own IT dept, points out **Jim Sheldon-Dean,** founder and director of compliance services at Lewis Creek Systems in Vermont.

What's more: The American Recovery and Reinvestment Act (ARRA) just intensified HIPAA requirements, and Congress recently allocated more HIPAA security compliance enforcement dollars to the Center for Medicare and Medicaid Services (CMS) and the Office of the Inspector General (OIG), points out **Wayne J. Miller,** a healthcare 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, 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." Recent preliminarily guidance suggests that this notice targets breaches of unencrypted data, says Miller. 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 Health and Human Services Secretary.

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 hospitals, explains Miller. Attention: 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 third-party protected health information (PHI) disclosures to a "limited data set" or the "minimum necessary," including those disclosures you make to health plans, said **Steven J. Fox, Esq.,** partner 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 healthcare operations.

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