Health Information Compliance Alert

Fact Finder: Don't Let These ARRA Items Slip Under Your Radar

ARRAAAAAGH! New law gives HIPAA sharper teeth.

You've got some new things on your to-do list, HIT pros. The byzantine stimulus package passed earlier this year has some new HIPAA requirements tucked away here and there. Here's what our technology & attorney experts are saying about the American Recovery and Reinvestment Act (ARRA).

Wake-Up Call: You bear the IT compliance burden even if a third party installs and maintains your system. Even smaller health care organizations are responsible for ensuring the same privacy protections as larger places that have their own IT departments, says **Jim Sheldon-Dean,** founder and director of compliance services at Lewis Creek Systems in Vermont.

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 **Wayne J. Miller,** a healthcare attorney with the Compliance Law Group in Los Angeles. If the data breach affects more than 500 people, you must also notify prominent media outlets in your state and report the incident immediately to the Health and Human Services Secretary.

Time to Rewrite All Those Business Associate

Agreements: 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. You will likely need to modify your business associate agreements as a result. 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.

Keep Your Eye on Disclosures: In addition, you are required to keep private health information (PHI) disclosures to a "limited data set" or the minimum amount 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. 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.

Add-On: Congress has also just allocated more HIPAA security compliance enforcement dollars to the **Center for Medicare and Medicaid Services** (CMS) and the **Office of the Inspector General** (OIG), Miller points out.