Eli's Hospice Insider

MEDICAL PRIVACY: Get Hip to Tougher HIPAA Requirements and Enforcement

Hint: Encrypting PHI on laptops may prevent your hospice from ending up on the nightly news.

New rules in the economic stimulus bill provide a major stimulus for your hospice to examine its HIPAA compliance and get a step ahead of tougher requirements coming down the pike. Indeed, ignorance will be no defense in case of a wrongful disclosure that could land your hospice in more hot water than it might imagine.

Ramped up HIPAA enforcement has already started, warns Chicago attorney **Michael Roach,** who predicts hospices and other providers will in the future see the Department of Health & Human Services performing"not for cause audits," which are required by the American Recovery and Reinvestment Act.

Not only that: The attorney general in each state can now enforce HIPAA effective immediately, says **Jim Sheldon-Dean,** a HIPAA compliance consultant in Charlotte, Vt. And that can mean big trouble for providers in states like New York that have aggressive attorneys general, he points out.

Beware Notification Requirements

A part of ARRA known as the HITECH Act (Health Information Technology for Economic and Clinical Health) ups the antes for your hospice to encrypt patients' protected health information (PHI) this year. If you don't -- and have a breach of what the law calls unsecured PHI -- the hospice has to follow notification requirements that in some cases require it to report the breach to the media. The notification requirements go into effect 30 days after HHS publishes interim final regulations, which the agency is required to do by Aug. 17, 2009 at the latest, Roach tells **Eli.**

Unsecured PHI basically refers to any PHI that's not properly encrypted based on standards spelled out in HHS guidance issued on April 27, Roach adds.

The notification requirements vary based on the number of patients involved. If the breach involves 10 or more individuals without current contact information for themselves or their responsible parties, then the covered entity is required to post notice of the breach for a period of time specified by the HHS Secretary, says Roach. "The posting must occur either on the covered entity's Web site or via the media -- HHS apparently decides. HHS may in regulatory guidance clarify this, or perhaps not."

It gets worse: If the breach involved more than 500 people, the entity has to notify prominent media outlets to report it, Roach notes. A breach that large could occur if someone hacked into a database where the provider keeps all patients' EMRs, for example, he notes. Yet once the rules go into effect, accidentally sending an e-mail with unencrypted PHI to the wrong e-mail address would count as a breach of unsecured PHI requiring you to notify the patient, says Roach.

3 Strategies Put You on the Road to Compliance

To get a grip on the new requirements and to avoid HIPAA trouble, experts suggest a three-prong approach, as follows:

1.Weigh the Benefits and Costs of Encryption. Start by reviewing the April 27 HHS guidance, which talks about the standards for encrypting PHI, suggests Roach (www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf). Then talk to your computer tech people about the feasibility of encryption, if you don't already have it in place. And don't view encryption as an all-or-none undertaking. Sheldon-Dean recommends encrypting any portable devices or media (laptops, portable hard drives, USB memory sticks, etc.) that hospice staff members take off the premises. "That's pretty much required

according to good standards these days," he says. Even if such devices stay put in the office, you need to secure them when unattended. And encryption is a good idea. "Laptops go missing from within offices all the time."

Another good place to start encryption is in safeguarding more sensitive information or example, patients with an HIV diagnosis, Sheldon-Dean suggests.

2. Develop Plan B (for Breach).

If you aren't going to encrypt all PHI, decide how the hospice will follow the notification procedures in case of a breach, Roach advises. For example, develop policies and procedures for what the hospice will do first and then second, he adds. You wouldn't want someone who caused or was aware of the breach to sit on that information.

Tip: If your hospice had a breach involving secured PHI (properly encrypted), it would still have to maintain a list of accountings of disclosures, says attorney **Heather Berchem** with Murtha Cullina LLP in New Haven, Conn. If a consumer wanted that information, Berchem doesn't see any way around a covered entity having to provide it.

Also keep in mind that around 44 states have some form of notification requirements related to medical privacy breaches, Roach cautions.

3. Shore Up Privacy Protection.

Retrain staff on existing HIPAA policies and procedures that can help prevent disastrous breaches. For example, Roach heard recently at a conference about one case involving a home health nurse working at home ho violated her agency's policy by getting into a hospital database to do her work.

While the nurse was replicating the patient database on her computer, she left the computer unattended to run some errands. Meantime, someone broke into her home and stole the computer, which by then included 40,000 patient files, including patients' Social Security numbers, Roach recounts.

Compliance tip: HHS issued guidance on remote access to data some years ago, which is what providers should be following, advises **Peter Arbuthnot,** a regulatory analyst with a healthcare software developer in Jackson, Miss. Review the guidance at: www.cms.hhs.gov/SecurityStandard/Downloads/SecurityGuidanceforRemoteUseFinal122806.pdf.

Editor's note: Effective on Feb. 17, 2010, ARRA also imposes new requirements for business associates that could affect your hospice agreements with BAs. For details, see the next **Eli's Hospice Insider.**