Long-Term Care Survey Alert

MEDICAL PRIVACY :Get Hip to Tougher HIPAA Requirements and Enforcement

Hint: Encrypting PHI on laptops may prevent your nursing home from being on the nightly news.

If medical privacy compliance seems old hat, give your team a heads up that HIPAA enforcement now packs a much bigger punch.

And ignorance of new rules coming down the pike will be no defense in case of a wrongful disclosure.

In fact, ramped up HIPAA enforcement has already started, warns Chicago attorney **Michael Roach,** who predicts nursing facilities and other providers will see the Department of Health & Human Services performing "not for cause audits," which are required by the American Recovery and Reinvestment Act (ARRA).

Not only that: Based on changes in ARRA (a.k.a. the economic stimulus bill), the attorney general in each state can now enforce HIPAA, which is already in effect, says **Jim Sheldon-Dean,** a HIPAA compliance consultant in Charlotte, Vt. And that can mean trouble for providers in states like New York that have aggressive attorneys general, he points out.

Also: The survey agency could report a HIPAA violation to the state attorney general, observes attorney **Heather O. Berchem,** with the law firm of Murtha Cullina LLP in New Haven, Conn.

Beware New Requirements

ARRA ups the ante for your facility 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 facility has to notify the individuals whose PHI was breached, HHS, and in some cases, the media, according to Roach. "If the breach involved more than 500 people, the entity has to notify prominent media outlets to report the breach," he says.

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 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**.

Get on the Road to Compliance

To avoid HIPAA trouble, consider these approaches:

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. Then talk to the organization's computer tech people about what it would take to encrypt PHI, he adds.

Key point: You don't have to view encryption as an all-or-none undertaking. Sheldon-Dean recommends encrypting PHI on any portable devices or media (laptops, portable hard drives, USB memory sticks, etc.) that facility 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. Another good place to start using encryption is in safeguarding more sensitive information, such as patients with an HIV diagnosis, Sheldon-Dean suggests.

CPT® 2023 American Medical Association. All rights reserved.

2. Develop a plan to address a breach. If you aren't going to encrypt all PHI, decide how the facility will follow the notification procedures in case of a breach, Roach advises. For example, develop policies and procedures for what the facility 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 nursing facility had a breach involving secured PHI (properly encrypted), it would still have to maintain a list of accountings of disclosures, says Berchem. If a consumer wanted that information, Berchem doesn't see any way around a covered entity having to provide it.

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 who violated her agency's policy by getting into a hospital database to do her work at home. While the nurse was replicating the hospital 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 relays.

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.

CPT® 2023 American Medical Association. All rights reserved.