MDS Alert

MEDICARE PRIVACY: Don't Let HIPAA Breaches Trip Up Your Facility

HHS security guidance targets electronic PHI.

HIPAA is back on CMS' radar screen, so watch out for privacy lapses resulting from electronic protected health information.

The **U.S. Department of Health & Human Services** recently issued security guidance warning providers of "security incidents" involving portable devices that store electronic protected health information (EPHI). In fact, nurses taking laptops to the hospital to collect preadmission MDS data could result in the types of problems that the guidance warns providers against.

HHS says it prepared the guidance document "with the main objective of reinforcing" some ways a "covered entity" can protect EPHI when staff accesses or uses it outside the organization's "physical purview."

Beware: The **Centers for Medicare & Medicaid Services** has authority to enforce the HIPAA Security Standards, says HHS in the document. And it "may rely on the guidance" to determine if the facility's actions are "reasonable and appropriate" for safeguarding residents' EPHI.

Here's What to Do

Facilities can implement simple strategies to prevent laptops and other portable devices from saddling the facility with a HIPAA disaster:

Implement policies prohibiting people from taking home laptops or other portable devices, such as PDAs, or CDs with PHI on them in any form, advises **Peter Arbuthnot,** regulatory analyst with **American HealthTech** in Jackson, MS.

Prohibit staff from putting PHI on laptops or hard drives, suggests HIPAA expert **Michael Roach, MHSA, JD,** partner, **Meade Roach Consulting** in Chicago. "You can purchase a flash drive that requires a password" to store the information, he says. "Those are on the market now" and hold much more data than a disk. "They are tiny -- you plug them into the USB port of the laptop," adds Roach.

Beware: "If a nurse or other facility staff person were using a non-protected flash drive and it got into the wrong hands, the government could reasonably ask why didn't you spend a couple dollars more to buy password-protected flash drives," Roach says.

Another option: Perhaps the nurse collecting preadmission information at the hospital could transmit the resident-specific information to the facility using a secure portal with encryption, so the data does not remain on the laptop, says Arbuthnot.

More Suggestions From HHS

In addition to password protecting portable or remote devices storing EPHI, facilities can use a number of strategies to protect EPHI, according to the recent HHS security guidance:

• Require use of lock-down or other locking mechanisms for unattended laptops;

• Password protect files;

• Require that all portable or remote devices that store EPHI employ encryption technologies of the appropriate strength.

Use Secure Connections When Offsite

Facilities should have strict IT guidelines about how staff use portable devices or offsite computers to connect to the facility's system, says Arbuthnot. "This secured connection is sometimes a WEP (Wired Equivalent Privacy) connection."

Beware: The "types of connections that travelers are accustomed to seeing in hotels is exactly the non-secured type of connection" that HHS is warning users about in the security guidance, adds Arbuthnot.

The HHS HIPAA security guidance suggests prohibiting "transmission of EPHI via open networks, such as the Internet, where appropriate" and the use of "offsite devices or wireless access points (e.g., hotel workstations) for nonsecure access to e-mail." "If the MDS nurse or physician has to communicate with the facility in a way that involves PHI, he or she could do so by telephone," suggests **Joy Morrow, RN, PhD,** senior clinical consultant with **Hansen, Hunter and Company PC** in Beaverton, OR.

Take a Practical Approach

Keep in mind that PHI is identifiable health information or a patient's health information that can be tied to him through his name, birth date, Social Security number, etc., says Morrow.

Thus, "a nursing facility could develop a way to identify residents through a numbering or other system when e-mailing and faxing PHI with physicians," she says.