Health Information Compliance Alert

Privacy Compliance: Use These Quick Tips To Keep 'Removable Media' In Check

Don't let lost diskettes cause deep regrets.

You have your protected health information, but can you take it with you? Yes, you can, but unfortunately, so can many others who shouldn't. HIPAA requires you to have controls on so-called "removable media."

Here are some simple tips you can use to keep diskettes, floppy disks, CD-ROMs and other media properly accounted for.

HIPAA's security rule requires you to take certain precautions when it comes to media devices that contain PHI [164.310(d)(1)]. That means you have to implement policies and procedures that address the receipt and removal of hardware and electronic media that contain electronic PHI into and out of your facility, as well as the movement of such media within your facility.

1. Identify your problem areas. How many diskettes contain PHI in your facility? Do you know where they are at all times? There are at least two basic types of problems you need to address with removable media.

On the one hand, you may have lack of proper controls and, on the other hand, you could encounter malicious copying of media. While experts admit there's not much you can do to entirely prevent the latter, you can at least make it more difficult for unauthorized personnel to gain access to media devices.

2. Limit placing PHI on removable media. This is probably the best solution for media control. "There's little reason to place PHI on floppies, memory sticks and the like. PHI on removable media should be limited to backup media, if possible," advises **Fred Langston,** senior principal consultant with **Guardent** in Seattle.

3. Store media in a safe zone. It sounds simple enough, but in many cases PHI-containing media devices can get out in the open due to the lack of proper storage, or simply through carelessness. Media should be "in secured areas or in locked cabinets with an audit trail of who took possession of or accessed the media," Langston warns.

4. Track media containing PHI. Langston knows that placing PHI onto removable media may be mandatory for some organizations, and advises CEs to label and classify all PHI-containing media and to track such media until its destruction or deletion is secure. "Think of removable media as something that needs to be tracked from cradle to grave."

5. Help lost media find its way home. If diskettes or CD-ROMs containing PHI have been lost, you can easily create an incentive for their eventual return. **Albert Oriol**, CHE, CISSP with **The Children's Hospital** in Denver, says he's designing a labeling system that would offer a small reward for the return of lost media. Disks would be labeled with a note that asks the finder to call a toll-free number "and we'll give you ten bucks for it, or something to that effect, which would get that media back to us."

Oriol admits that this system doesn't necessarily preclude someone from reading whatever PHI is contained on your media device, but it at least creates an incentive for its eventual return.

6. Portable computers present high risks of disclosure. Oriol says he's developed a "Data Classification Matrix" for his organization that addresses the proper security precautions for personal laptop computers and Personal Digital Assistants (PDAs). Computers containing confidential medical information cannot be left unattended at any time unless the confidential information is encrypted. He also requires portable computers to use locks when deployed in unattended

public areas or any offsite locations.