Health Information Compliance Alert

ePHI: Are Your ePHI Practices Faulty?

Stop electronic protected health information leaks before they happen with this cautionary advice.

If your facility's doctors and staff use Smartphones and similar devices to transmit patient care advice, your door could be wide open for PHI leaks -- and massive penalties.

Patient health information is protected by the law and if it needs to be shared over a Smartphone or email then the potential breach points are many, stresses **Ester Horowitz, CMC, CITRMS, CIISA**. Read on for practical tips on how to keep your device ePHI from getting you into hot water.

Track How PHI is Stored and Who Has Access

Take a close look at where your ePHI is kept and how it's transmitted within the facility. When someone in the facility is entering PHI into a computer it should be done in such a manner that an unauthorized person cannot catch the drift by watching what is being typed in.

Ensure that staff remove ePHI stored in media such as a hard drive or a laptop before they hand the device to someone who is not authorized to view it, recommended **Layna S. Cook** in her audio presentation titled "'Email that to me.' -- Electronics, Health Information, and HIPAA" sponsored by The Coding Institute's AudioEducator.

There might be many devices like pen drives, tablets, netbooks and laptops being used within your facility which can be carried into and taken out of the facility. Take steps to ensure that these are listed and individually identifiable Horowitz tells **Eli**. Keep a log of their usage and track what data is moving where.

Tighten Up Password Protection/Encryption

If employees and health providers carry work home, how they do so would determine vulnerabilities, Horowitz observes. Suppose devices are left in a car and the car is broken into or the devices are lost in transit? Are they programmed to render data indecipherable or unreadable if an unauthorized person or software accesses it?

Encryption is necessary for internal, authorized users, as well. When a doctor orders a lab test, he might ask for the results to be emailed to him before he takes further treatment decisions. This is where you need to ensure that the exchange is encrypted so as to become indecipherable if it is intercepted. "ePHI should be encrypted and

decrypted to prevent access by persons or software programs that have not been granted access rights," counsels Cook. Health information is "secure" if it is rendered unusable, unreadable, or indecipherable through the use of a technology or methodology approved by HHS.

Terminate Former Employees' Access

One of the biggest dangers of unauthorized access is unauthorized modification to ePHI, experts warn. Email accounts of former employees need to be terminated immediately after the employee leaves to prevent unauthorized access.

If users within the facility have been assigned a unique name and/or number for identifying and tracking user identity, then you also need to have measures in place which tell you what information was accessed and when. Those systems should also tell you if any PHI has been modified. All dedicated computers within the facility should have an automatic logoff after a specified period of inactivity, says Cook.

Codify
BY AAPC