Health Information Compliance Alert

Security Rule: Take 5 Steps To Manage Mobile Device Use In Your Organization

Weigh the risks versus the benefits before using mobile devices.

As more and more healthcare providers are using smartphones, tablets and laptops in their everyday practice, mobile device security has become more important than ever. Fortunately, there are strategies that you can employ to help protect your mobile devices and your patients' protected health information (PHI).

The **HHS Office of the National Coordinator for Health Information Technology** (ONC) offers the following steps you should take to manage mobile device use:

1. Decide on usage: First, decide whether you'll use mobile devices to access, receive, transmit, or store patients' PHI. Also, decide whether you'll use mobile devices as part of your organization's internal network or systems, such as your electronic health record (EHR) system.

2. Evaluate the risks: Consider the risks of using mobile devices to transmit PHI. Conduct a risk analysis to identify threats and vulnerabilities.

3. Create a risk management strategy: Identify a mobile device risk management strategy, including privacy and security safeguards. This strategy will help your organization to develop and implement mobile device safeguards and reduce risks identified in your risk analysis. Your strategy should include an evaluation and regular maintenance of the mobile device safeguards you put in place.

4. Implement policies and procedures: Develop, document, and implement mobile device policies and procedures. Address in your policies and procedures topics like mobile device management, using your own device, restrictions on mobile device use, and security or configuration settings for mobile devices.

5. Conduct training: Provide mobile device privacy and security awareness and ongoing training for your staff.