Codify
BY AAPC

Dermatology Coding Alert

Compliance: Avoid PHI Breaches With Mobile Technology

Secure passwords are just the beginning.

Chances are good that at least one provider in your practice uses a smartphone, tablet, or laptop in his daily routine. If he isn't carefully monitoring the security of that device, your practice might have HIPAA issues.

Fortunately, there are strategies that you can employ to help protect your mobile devices and your patients' protected health information (PHI). Follow these five steps to keep your practice compliant.

Take Advice from ONC

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. During this decision-making process, you should also have a lengthy discussion on encryption, company security regarding email, and communication with patients.

2. Evaluate the risks: Consider the risks of using mobile devices to transmit PHI. Conduct a risk analysis to identify threats and vulnerabilities. A risk analysis is vital not only to vet this process, but also to keep on file to help create further policies around this very important requirement.

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. You should create many policies to comply with HIPAA. You can find lots of helpful information on the US Department of Health and Human Services Office of Civil Rights website (www.hhs.gov/ocr).

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. Remember to not only have policies around this, but also outline your breach notification policy and disciplinary actions as well.

5. Conduct training: Provide mobile device privacy and security awareness and ongoing training for your staff. Along with this training, make certain you keep track of the training and update it regularly for all employees as well as new employees.

Tighten Mobile Device Security

Here are some tips to secure PHI on mobile devices, also courtesy of the ONC:

- **Set strong passwords:** Always use a password or other user authentication on mobile devices.
- **Encrypt:** Install and enable encryption to protect health information stored or sent on any mobile devices.
- **Use automatic log off:** Also, make sure your mobile device requires a unique user ID for access.
- **Enable remote wipe:** Install and activate wiping and/or remote disabling to erase the data on your mobile

device if it is lost or stolen

- **Keep the device with you:** Maintain physical control of your mobile device. Know where it is at all times to limit the risk of unauthorized use. Always keep things in your sight. Items in car trunks or on counters tend to get lost or stolen.
- **Use a screen shield:** Also, don't share your mobile device with anyone, and lock the device when not in use.
- **Install a firewall:** Install and enable a firewall to block unauthorized access.
- **Use a secure Wi-Fi connection:** Use adequate security to send or receive health information over public Wi-Fi networks.
- **Research mobile applications before downloading:** Disable and do not install or use file-sharing applications.
- **Employ security software:** Install and enable security software to protect against malicious applications, viruses, spyware, and malware-based attacks. Keep your security software up to date.
- **Use proper disposal methods:** Delete all stored health information on your mobile device before discarding it.

Correction:

An article in Dermatology Coding Alert Vol. 11 No. 5, "Don't Let Faulty Coding Cut In to Your Laceration Repair Reimbursement," marked the incorrect answer to this question:

Question 1: Your dermatologist performs laceration repair for an 18-year-old male patient for a cut that he received from broken glass. The laceration was 4.5 cm long and present on the right thigh area. Since there were glass shards interspersed in the wound, your dermatologist had to spend a lot of time in removing all the pieces of embedded glass. After the debridement, the dermatologist closed the wound with a single layer of sutures. What CPT® code should you report?

A. 12001

B. 12002

C. 12031

D. 12032

The correct answer is "D. 12032." We apologize for the error.