# Psychiatry Coding & Reimbursement Alert

## Office Security: Ensure PHI Safety Across All Providers' Data Devices

**There's more to it than just passwords.**

In this modern world, it is very likely that your providers use devices like smartphones, tablets, and laptops in their daily work. But if you don't stay on top of the security of those devices, your practice could end up breaching information about your patients.

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.

**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.

**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. "Strong passwords typically include a combination of capital and lowercase letters, numbers, and special symbols (e.g. "#") found on a keyboard," notes Kent Moore, senior strategist for physician payment at the American Academy of Family Physicians. "Strong passwords are also typically only used on one device (i.e. don't use the same password more than once) and changed often."
- **Encrypt:** Install and enable encryption to protect health information stored or sent by 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.
- **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