Part B Insider (Multispecialty) Coding Alert

Clip And Save: Boost Mobile Device Management in 5 Easy Steps

Keep BYOD rules straightforward - but realistic.

Now, more than ever, providers depend on the convenience mobility affords. In fact, as the pandemic rages on, the merits of virtual care continue to stack up with many practices using mobile devices to connect with patients under the Medicare telehealth expansion.

Consequently, it's this ease-of-use that also makes these tools vulnerable to loss, theft, and infiltration. Keeping devices close limits the chance of unauthorized access, but accidents do happen. Basics like privacy controls, screen shields, and secure WiFi connections are a must; however, there are HIPAA-friendly policies you can implement to decrease breaches and safeguard data.

Consider these five tips to secure your mobile devices and protect your patients' electronic protected health information (ePHI):

1. Determine Device Usage and Users

Your first step should be to outline what mobile devices will be used in your practice - and who will have control of them. Plus, if more than one person will be using a device (such as an office tablet to check in patients), ensure that all users have their own logins and passwords. This lets IT management review logs for outlier activity.

Tip: If staff use their own devices for work, office management needs to set bring your own device (BYOD) parameters from the get-go. This may encompass "centralized security management," including "configuration requirements" and user classes specific to the devices, suggests HHS Office of the National Coordinator for Health Information Technology (ONC).

2. Protect Data with Strong Passwords

Using a password or other user authentication on mobile devices is always a good idea. "In my experience, the best passwords come from a password manager. They can be long, complex, and unique without taxing your ability to remember all the passwords to all your accounts," says **Jen Stone, MSCIS, CISSP, QSA,** a security analyst with Security Metrics in Orem, Utah.

3. Utilize Multi-Factor Authentication

When you add multi-factor authentication to your password protocols, you add another layer of protection. That's because the "other authenticator is the private information or proof that only you can provide that serves the purpose of proving you are who you say you are," explains **Adam Kehler, CISSP,** principal consultant and healthcare practice lead with Online Business Systems.

4. Use Encryption for Devices

When you encrypt ePHI, you're not only protecting patients' data, but all the information stored and transmitted on the mobile devices. "Encryption is not expensive, but it can require some expertise to properly apply it," Stone maintains. "Implement access control so that only authorized individuals can get to ePHI."

5. Invest in Security Software and Safe Apps

CPT® 2023 American Medical Association. All rights reserved.

The type of IT products your organization needs will depend on its size, complexity, and infrastructure. Software you may want to consider includes:

- Firewalls to block unauthorized access;
- Remote wipe or disabling to erase data if the device is lost or stolen; and
- Security software to circumvent malware, spyware, and other malicious programs. And it's essential you hire and work closely with IT experts to ensure you install, enable, and update your products.

"While a small office can get by with just a policy that says what a user should do, a larger organization will need to establish a mobile device management solution that allows the devices to be managed by IT, not the user," cautions HIPAA expert **Jim Sheldon-Dean,** founder and director of compliance services at Lewis Creek Systems LLC in Charlotte, Vermont.

CPT® 2023 American Medical Association. All rights reserved.