Codify
BY AAPC

Health Information Compliance Alert

Mobile Device Management: Beef Up Mobile Device Security With 5 Quick Tips

Tip: Manage your logins and passwords accordingly.

Smartphones, tablets, and laptops are versatile, and most practice workflows depend heavily on their mobility. They encourage coordination among providers, make data sharing between facilities easier, and promote better engagement with patients, too. However, it's this mobility that also makes them vulnerable to loss, theft, and infiltration.

Though keeping devices close limits the chance of unauthorized access, accidents do happen. Basics like privacy controls, screen shields, and secure WiFi connections are a must, but there are HIPAA-friendly policies you can implement to decrease violations, improve interoperability, and safeguard data.

Consider these five tips to secure electronic protected health information (ePHI) on mobile devices:

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 (i.e. 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.

BYOD Tip: If staff use their own devices for work, office management need to set Bring Your Own Device (BYOD) parameters from the get-go. This may include "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

It's always a good idea to use a password or other user authentication on mobile devices. "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

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 [MDM] 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.