Health Information Compliance Alert

Mobile Device Safeguards: Quick Tips For Tighter Security

Beware of file-sharing apps and public Wi-Fi connections.

Mobile devices are certainly handy in the healthcare industry, especially when treating patients. But you don't have to compromise the privacy and security of your patients' protected health information (PHI) when using mobile devices.

Here are some tips to secure PHI on mobile devices, courtesy of the **HHS Office of the National Coordinator** for **Health Information Technology** (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 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 you security software up-to-date.

Use proper disposal methods: Delete all stored health information on your mobile device before discarding it.