MDS Alert

Clip and Save: Bolster Mobile Device Security

Keep these strategies in mind for a comprehensive plan to minimize cyber vulnerabilities.

Use these tips to secure protected health information (PHI) on mobile devices, also courtesy of the Department of Health and Human Services Office of the National Coordinator for Health Information Technology.

- **Set strong passwords:** Always use a password or other user authentication on mobile devices. Multi-factor authentication passwords are recommended.
- **Encrypt:** Install and enable encryption to protect health information stored, utilized, 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:** Don't share your mobile device with anyone, lock the device when not in use, and implement at-rest protocols.
- **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.