Guidelines for Use of Mobile Devices

This section will:

- summarize the risks and benefits of using mobile devices to provide health care services
- identify key requirements and best practices for using mobile devices

Mobile devices such as smartphones and tablets allow a physician convenient and timely access to patients and other health care providers remotely. However, the use of mobile devices in a practice can create privacy and security risks to personal information. Those risks include loss or theft of the device, malicious programs that track or spy on the device and having personal information be intercepted or monitored by unauthorized third parties. Any wireless device, including a mobile device, that is connected to a network (e.g., Wi-Fi, Bluetooth, 3G and near-field communication) can serve as an illicit entry point to the entire network if it is not properly set up with appropriate security controls.

Best Practices

Physicians have an obligation to ensure adequate administrative, physical and technical safeguards are in place before using mobile devices in their practice. This obligation extends to staff and third parties who have access to personal information under the practice's custody or control. Physicians must also take reasonable steps to ensure any devices, apps or programs used by their practice comply with PIPA.

- Ensure:
    - devices have strong, up-to-date, industry-standard encryption for transmitting personal information to minimize the risk of unauthorized interception
    - devices are protected with a secure password that is at least six characters long with a combination of numbers, upper and lower case letters
    - anti-malware software is installed and up to date to protect against attacks
    - any systems to which the device is connected provides adequate end-to-end security
    - any cloud services used to transmit or store data are secure and use encryption (do not use public services that can be easily accessed by unauthorized third parties)
    - voice command features are disabled if they are not needed, as this feature allows the device to always be listening
    - the screen is set to lock automatically after a short period of inactivity
- Never:
    - use public Wi-Fi connections as they are vulnerable to unauthorized interception

- "jailbreak" or root the device as this weakens its security

- Limit:
  - the number of incorrect password attempts before the data is deleted
  - access permissions for apps, unless the permissions are related to the service
  - location information used by programs to avoid creating a log of your movements, which may include visits to patients' homes
- Always:
  - use apps that come from official app stores and that use strong, up-to-date, industry-standard encryption
  - keep software up to date
- Promptly report a lost or stolen device, and consider using programs that help you locate your phone.
- When returning or disposing of a device, ensure it is completely wiped and safely disposed of.
- Delete personal information from the device once it's been added to the patient's medical record.

It is recommended that policies regarding the use of mobile devices in a practice be included in the practice's privacy management program.

For more information on mobile devices and privacy, see

- Top 15 Tips: Mobile Devices: Tips for Security and Privacy
- Contemplating a Bring Your Own Device (BYOD) Program? Consider These Tips