Are You Exposed? 5 Major Threats to Your Mobile Device

written by CPH Insurance | June 15, 2016

With the ever-changing HIPAA laws, your mobile device may seem more like that imaginary albatross than the simple, social tool the telephone was originally meant to be.

In the mental and allied health fields, nearly all social communications on the phone represent major threats.

1. Email threats – Since your business email connects directly to your phone, sensitive patient information is openly available. It's simple that if you're checking your phone in public, outsiders may be able to view the files you're looking at on your mobile device. This can be solved with a simple **privacy screen**. Not only will it prevent your phone from cracking, but it will limit any strangers from viewing information that may compromise your practice.

2. Network security – Constantly switching between 3G, 4G, and WIFI represents a major threat to the invisible viewer. Unsecured WIFI networks allow all the data being streamed to be visible to those who know how to access the open information moving across the network. Avoid connecting with networks that are unsecured or secured with many "guest users."

3. Physically losing your phone – When you lose your phone, the files become exposed. Hacking and accessing the information is easy when your device is physically available. Every mental or allied health professional should install a **downloadable application that will wipe it's contents** if the phone is lost or breached, and even track the phone through GPS so that it can be erased remotely if the phone's content becomes threatened. Also, an auto-lock with a password is a good way to keep the phone safe in case anyone is looking through it. Also, remember to follow Breach Notification protocol when you lose your phone just in case your application did not erase the device in time.

4. Online Cloud Access – A phone that directly syncs with an online cloud can compromise the security of information for those who find the phone – but protect it for those accessing via mobile. **HIPAA compliant cloud storage systems encrypt your data**, so if you are on an unsecured network, your data is still somewhat impenetrable.

5. Applications with extensive privileges – Be careful with what programs you download. Free apps and fun games are top sources of malware on a phone. As with your computer, **invest in a security program** to keep an eye on what gets sent back to the maker of the app.

We do not recommend keeping personal patient information on your phone – but in the ever mobile world, it's important to take extra precautions. **You never know when you could suffer an attack.**