How to be HIPAA Compliant With Your Mobile Device

written by CPH Insurance | June 15, 2016

Mobile devices have become the all-in-one technology lifesaver. With the development of all-in-one devices, phones, internet, cameras and computers are shrunk down for personal use. Although this may seem ideal for work, how safe is your mobile device? Today if you lose your phone, you don't just lose a way to communicate when you aren't home or at the office, but you lose files and data that can be crucial for everyday life. It can also be a loss of security.

One of the largest down falls for individuals who own mobile devices is that they don't invest in a privacy screen. A privacy screen isn't just beneficial to ensure that a phone screen won't get cracked. With a privacy screen, it makes it impossible for 'peeping Tom's' to view what is being done on a personal mobile device. This may sound extreme, but with new HIPAA laws, reading a patient's file on your commute to work could leave you and your practice at danger for breached information. Technology is so advanced that most of the time we don't even think about the security problems of having information accessible on mobile devices.

Once a mobile device is visibly protected, it's important to go to the extreme. What happens if you leave your phone at the airport or at a Starbucks? The files on the phone can now be hacked and accessed. Every phone should have a downloadable application that will wipe it clear if the phone is lost or breached by an outside source. Applications like Find My iPhone, an app that Apple products use, allow users to track where their phone is through GPS. If the product is on, the owner of the phone can remotely erase all content on the phone for security purposes if needed.

All mobile devices have the ability to auto-lock the device with a password or code to unlock the phone. We suggest that phones put their auto-lock setting to two minutes or less to ensure that all information or files that can be accessed on the phone are safe. Also, some settings will allow users to not have a password to unlock their phones, we suggest always having a password and changing it frequently. Like a computer or email account, having a password is just one more wall of protection for users.

Data encryption is a huge topic with the new HIPAA laws, more information is being stored in online cloud storage and is being encrypted so an information breach is less likely. We suggest doing the same with the high-risk information kept on your phone. By encrypting information, even the most skilled hackers won't be able to scale the last barrier of protection. While not all information on your phone is important, text messages to your significant other or your high score on Candy Crush, encrypting client information and data from work is a must.

The information in this blog is provided by our practice management partner, Simple Practice.