BYOD: 5 Things Every Practice Needs to Consider
By Michael J. Sacopulos, JD, Founder and President of Medical Risk Institute

Protecting patient information on personal devices should be a major concern for your practice. There are frequent reports of personal devices (laptops, smartphones, ipads) with sensitive data being lost or stolen. These reports end with a practice spending significant amounts and often having to publish notice of the breach in local media. If you decide to let employees bring their own devices, how do you avoid risk of data being loss or a violation of HIPAA? Here are 5 things every practice needs to consider:

BYOD Policy: A bring-your-own-device (BYOD) policy is necessary because your employees will expect to have information at their fingertips at all times. Protected health information is finding its way onto these devices, many of which are unprotected. If your practice does not have one, Medical Risk Institute offers all ADAM members a discount on their policies.

Encryption: Safeguard mobile devices from potential loss of data by encrypting. Standard email and text messages are easily tracked or intercepted. Consider using encrypted conversation apps. The challenge is that it would take you and your co-worker/patient to have the software for it to work. It is not totally impossible; it would just take a little bit more coordination.

Remote Wipe: Install software on your device to wipe all data in the case it is lost or stolen. With a remote wipe, a signal can be sent to the lost device to automatically delete the data.

Turn on Your VPN: If your mobile device is getting Internet access from an unusual or unsecure location, spies could be lurking. The most important thing you need to know about a Virtual Private Network is it secures your mobile device's internet connection to guarantee that all of the data you're sending and receiving is encrypted and secured from prying eyes.

Password Protection: It sounds simple, but many passwords are too simple. Put a strong password on your phone. A strong password can prevent someone from reading stored data on your phone, or at least slow them down until you have the opportunity to wipe the phone.
By examining and implementing the 5 steps above, you will have significantly decreased your chances of having a breach and all the nastiness that comes with it.

Originally Posted July 2014
Tag: Other