A Mobile Healthcare Check-up

mobilesecurity.com [San Francisco, CA] The last time you watched “General Hospital” (or “Casualty” for BBC fans), the doctors were probably writing notes using pens and reading patients' information off their charts. The last time you actually went to the doctor, it’s far more likely she pulled up your medical records on a tablet or smartphone.

A recent study by the Ponemon Institute found that 81% of healthcare providers use mobile devices to amass and store patient information. It also revealed that nearly half of these organizations do not take adequate security precautions to protect their devices. Essentially, there’s nothing wrong with the increasing use of mobile devices in all sorts of situations – your waiter uses a handheld device to take the hassle out of paying your bill; when you take your car to the shop, the mechanic is using a handheld to test emissions and store data about your car; but when emerging technologies are being used to store the most personal of private information, data security has to be the top priority. The market for medical apps is a fast-growing and clearly very lucrative one, but should patients be concerned about security risks?

If applied well, medical apps have a ton of potential to cut costs and improve healthcare. Indeed there are some great reasons why they're quickly becoming a cornerstone of modern healthcare. Most physicians already keep a digital record of their patients' charts, so entering data from examinations via an Electronic Health Record app (EHR) can provide a faster turn-around for test results or even speed up the detection of a fatal drug interaction. Members of Seattle's Group Health Cooperative have access to a comprehensive app that allows patients to access their own records and test results, receive care reminders and contact their doctors outside regular hours. There are even diagnostic apps like NETRA (Near-Eye Tool for Refractive Assessment), which can provide an eye exam that, because it's available on a mobile device, could be accessed cheaply and remotely. Walgreens Pharmacy will text customers when their prescriptions are ready to collect; while Kaiser Permanente is developing a text message reminder service for patients.

In fact, so long as providers stick to some pretty vague rules with regard to information about patients, they're on fairly safe soil. Check out the wording of this particular party piece: providers are required to offer their "services while minimizing the risks of violating the Health Insurance Portability and Accountability Act, or HIPAA". Passed in 1996, the HIPAA requires that physicians take "special care" to regulate and protect the disclosure of patient health information (PHI). Of course, no one had a smartphone in 1996, so HIPAA doesn't specify what's illegal and what isn't when it comes to mobile security. HIPAA's Security Rule permits healthcare professionals to communicate electronically with their patients, and the law requires them to employ "reasonable" precautions whenever doing so.

Make your own judgment call on what "reasonable" precautions are, but it's clear that when healthcare professionals are accessing or transmitting private data on their mobile devices, it leaves patient information vulnerable. An app unrelated to healthcare that requires text message permissions, for instance, could hypothetically be privy to SMS reminders or notifications sent from your healthcare provider. If a physician or staff member loses their smartphone, and it isn't sufficiently encrypted, patient information could be made public. Even something as innocuous as using public wi-fi runs the risk of exposing records.

Until more specific legislation comes into force, healthcare providers, doctors and patients all have a responsibility to reduce the risk succumbing to security issues – by using the same precautions that would be expected of a bank or government agency.

References:

- HIPAA Law and Related information

- Preventing a HIPAA violation

- Healthcare Quality Improvement

Mobilesecurity