TECH BRIEF

Prepare your patients as mHealth moves into the security spotlight

ENJOY SAFER TECHNOLOGY™

PREPARE YOUR PATIENTS AS mHEALTH MOVES INTO THE SECURITY SPOTLIGHT

By Lysa Myers, ESET Security Researcher

Mobile health, or "mHealth" for short, is an increasingly popular topic of discussion among healthcare professionals. The concept is simple: patients can track, transmit and store health information on mobile devices such as tablets, phones, watches or body monitors and share it with physicians or other practitioners.

Both healthcare providers and mobile device vendors are keen on encouraging people to use mobile technology to track health information, as it can really improve patient participation and outcomes. But with all that information floating around on small devices that are easily lost or stolen, it can also increase patients' privacy concerns.

Educating your patients about privacy and security best practices should be a priority if you use or plan to implement mobile health programs. Here's how.

How can patients use mobile devices to improve their health?

Here are some of the most common ways patients can participate in improving health by using mobile devices:

- **Searching for healthcare practitioners**
- **Booking/tracking/coordinating healthcare appointments**
- **Communicating with healthcare practitioners**
- **Tracking health and fitness activities**
- **Tracking symptoms of chronic conditions**
- **Tracking markers like heart rates, sleep quality, weight or body fat percentage**
- **Recording a log of prescribed medications, supplements or diet changes**

What are the security concerns for patients?

With all those potential benefits, it can be difficult to see any potential pitfalls. How could this health data possibly be used in a way that is worrisome to patients?

Right now, one of the biggest concerns is that security can be an afterthought for mobile devices and apps—if it is included at all.

Apps may collect a lot of unnecessary data, especially about a patient's device or its location. If this data isn't secured, and someone is able to break into the app account or steal the device itself, ample information about the patient's movements could be accessed. Many people wouldn't feel comfortable with untrusted individuals knowing when they sleep, where they go on daily runs, or when they're away from home. In addition, the sort of data collected by mobile devices is not currently covered by HIPAA regulation.

While many patients are well-versed in the use of mobile devices and privacy settings, some may not be aware of how tracking devices might expose sensitive information. Share these tips with patients to help them mitigate potential privacy problems and enjoy using their tracking devices:

- **Carefully consider new purchases**

  Before they buy, patients should be aware that not all of these devices include security features, or the security may be difficult to implement. Tell your patients that unless they are certain that their device is 100% secure, they should treat it as though any information on it could be accessible to unauthorized users. Smartphones or tablets may have better options available for protecting data, though their popularity and the sensitive information they hold make them a tempting target for would-be thieves.

- **Protect sensitive data**

  Patients should have an anti-malware scanner on smartphones to check for malicious applications or links, which may seek to steal data. Any important information should be encrypted both on the device itself and any time it gets sent via the network, e.g., email, IM or text messages. Installing or enabling device-finder apps such as "Find My iPhone" will allow the owner to remotely wipe data from a lost or stolen device.

- **Protect the device**

  Any mobile device used for mHealth tracking should require a passcode, password or biometric authentication (such as a fingerprint scan) to view the contents of the device, as well as a short time-out period. That way, if it falls into the wrong hands, the data on it will not be easily accessible.

> ***"The principle of least privelge simply means that no individuals, machines or systems should have access to things they do not strictly need."***

- **Be aware of the principle of least privilege**

  The principle of least privilege simply means that no individuals, machines or systems should have access to things they do not strictly need. For example, a nurse or physician's assistant in a medical office likely has a legitimate need to access patient health data, while a receptionist or the accounting staff might not. You can follow the principle of least privilege at your office or facility and let your patients know that you have implemented these safeguards on behalf of their privacy.

- **Update early and often**

  Reminding patients to perform regular updates of apps and operating systems on devices, especially smartphones, tablets and smart watches, is a good way to minimize potential hacking or virus intrusions. Updates should only be obtained directly from a trusted app store or the vendor's website.

Watch out for Wi-Fi®

Wi-Fi is a fact of life—there are free hotspots available wherever you go these days. But that public Wi-Fi can be an easy way for attackers to eavesdrop and snag data in transit—including the types of data transmitted via health tracking devices. Patients should be cautioned to avoid accessing or transmitting their health data via public Wi-Fi as much as possible. If they need to do so, perhaps during travel or a hospital stay, ask them to make sure the connection is encrypted. Internet connections should have the lock icon, and URLs should start with HTTPS rather than HTTP to help ensure a more secure connection.

Having your patients take advantage of the mHealth trend to share their tracking data offers potential benefits for both you and your patients. Managing their data throughout the day encourages patients to take an active role in wellness, helps keep you up to date, and can even lead to better outcomes. By making sure your patients are treating their data and devices with care, you can all feel good about mHealth security.

For more information on protecting your mobile devices for both business and home, visit eset.com/us