JMTM
WWW.JOURNALMTM.COM

EDITORIAL

PRINCIPLES OF SECURITY FOR THE USE OF MOBILE TECHNOLOGY IN MEDICINE

Dr Chandrashan Perera MBBS[1,2]
[1]Editor-In-Chief, Journal of Mobile Technology in Medicine, [2]Austin Hospital, Melbourne, Australia
Corresponding Author: editor@journalmtm.com
Journal MTM 1:2:5-7, 2012
doi:10.7309/jmtm.10

The rapid uptake of mobile technologies has allowed a number of innovations in the medical field[1,2]. However, as with any new technology, there are a number of security concerns that need to be acknowledged and addressed in order for these technologies to be implemented safely[3]. This is of particular significance in the medical realm where confidentiality of patient data needs to be preserved. Whilst data security is considered a more sensitive topic with evolving technologies, it is important to also consider the security benefits provided by mobile technologies.

Portability is one of the hallmark features to mobile technologies, allowing rapid access to information at convenience to the clinician. Unfortunately this too represents one of the greatest security risks, as each mobile device can carry large amounts of patient data, and have access to further sensitive information. In the past, should a clinician lose a briefcase with paper files, whilst disastrous, only the information stored within the briefcase would be lost. With the loss of a mobile device, this could represent potential access to large amounts of patient data. An interesting study conducted by Symantec® in 2012[4] called "Project Honey Stick", showed some fascinating insights into data accessed on an unsecured lost smartphone. They characterised this by placing 47 unsecured smartphones in the public, and ran special software on the smartphones which would track the use of these devices. Key findings from there study included:

- 89% of devices were accessed for personal related apps and information
- 83% of devices were accessed for business related apps and information

- 70% of devices were accessed for both business and personal related apps and information
- 45% attempted to access corporate email

The first and most important safeguard to this situation is to have a passcode enabled. Depending on the operating system of your mobile device, this can be in the form of a 4 digit pin, a pattern or an alphanumeric password. To maximise the protection offered by this passcode, it is recommended that a regular alphanumeric passcode be enabled, rather than a simple 4 digit PIN, (which can also be enabled on iOS devices http://goo.gl/Zdsxk). Furthermore, features such as "Erase data after 10 failed passcode attempts" are strongly recommended to further protect data. With regular backups in place, the inconvenience of having one's device wiped is far outweighed by the inconvenience of all data on one's mobile device being revealed.

The second step is to enable data encryption, which is enabled by default on all recent iOS devices with a passcode[5], Blackberry® devices, and most newer Android devices are also being capable of this, though the details would need to be confirmed with your particular device. Data encryption helps protect against instances when devices fall into the hands of those with technical expertise. Rather than guessing the passcode, one who wishes to access your data can manually offload the contents of the device onto a computer, and then can try to access this data directly, bypassing the mobile device itself. If the device is encrypted, then this data needs to be first manually decrypted before it can be accessed. If the device's data is only secured with a simple 4 digit passcode,

this process takes minutes using a "bruteforce" attack, whereas a secure alphanumeric passcode could take days, months or years to bypass[6]. Presently, this type of attack has been confirmed to work on iOS devices before the iPhone 4S and iPad 2, however it is only a matter of time before newer devices also become susceptible.

Another strategy to limit data loss in the event of device loss is to simply not have any data on the device itself. Applications can be constructed for mobile devices such that the device only acts as a portal of interaction to a central cloud based server which stores the data itself. The application itself would need to be secured with a secure password to prevent unauthorised access, however this eliminates a number of security concerns, as no patient data is stored on the device itself. An example of such use is the Citrix Receiver®, which is discussed in greater detail in a separate article in this issue of the Journal of Mobile Technology in Medicine[7].

Direct attacks on mobile devices from "viruses" and "malware" are far less common than previously experienced on traditional desktop computers due to a number of reasons. For example, on the iOS platform, applications can only be downloaded and installed through a curated "App store", and this certainly helps reduce the chances of installing programs with unsavoury intentions. Other devices where applications can be installed without going through this vetting process are more vulnerable. For example, the first malicious program for smartphones was reported by Kapersky Labs® in 2010, named "Trojan-SMS.AndroidOS.FakePlayer.a"[8]. This was a virus that sent SMS's to premium rate numbers without the owners consent. Maintaining the latest version of the operating system of your device ensures that you are up to date with the latest security patches and is an essential part of mobile security. It is important to note that this is an area of concern for some mobile operating systems where there is much fragmentation of devices, and as such some devices may not receive updates as frequently as other devices.

There are also key advantages to mobile devices. The ability to remotely locate and wipe devices is invaluable in mobile technologies, and it is strongly recommended that all mobile devices used for medical purposes need this capability. This is increasingly becoming a standard feature in many mobile platforms. Remote location functionality of devices allows tracking using the data and GPS functionality to show the real-time location of a mobile device, potentially allowing for recovery. Remote wiping works on a similar principle, but rather sends out a command to the device to destroy all data on the device, thus preventing unauthorised access to the data residing on the device. The disadvantage of these features is the requirement for the mobile device to have internet connectivity. Whilst portability is a key security concern, this also confers advantages. Desktop computers are typically left on in hospitals and anyone walking past can utilise an unsecured terminal and peruse confidential patient data. Whilst password protections are in place, in practice, I have personally seen many unattended computers with pathology and radiology viewers running unsecured. With portable mobile device, there is a tendency to carry these on your person, thus reducing the chances for access by third parties.

As with all evolving technologies, data security is an area that must be addressed in order for safe implementation of mobile technology. Currently there are no formal guidelines from regulatory bodies governing security in mobile devices, and as such one needs to be aware of these issues. Whilst mobile devices present a number of potential vulnerabilities, the greatest arising from their portability, there are a number of methods of overcoming such concerns. Previously, the loss of a paper file was irreversible, however with newer technologies, the loss of a mobile device need not represent a catastrophic event if adequate measures are in place.

References

1. Luanrattana R, Win KT, Fulcher J, Iverson D. Mobile technology use in medical education. J Med Syst. 2012 Feb.;36(1):113–22.

2. Zurovac D, Talisuna AO, Snow RW. Mobile phone text messaging: tool for malaria control in Africa. PLoS Med. 2012 Feb.;9(2):e1001176.

3. Fernando JIE. Clinical software on personal mobile devices needs regulation. Med J Aust. 2012 Apr. 17;196(7):437.

4. Wright S. The Symantec Smartphone Honey Stick Project. Symantec; 2012 Mar. p. 1–17.

5. Apple. iOS:Understanding Data Protection [Internet]. Apple. 2011. [accessed 2012 May 12]. Available from: http://support.apple.com/kb/HT4175

6. Greenberg A. Here's how Law Enforcement Cracks your iPhone [Internet]. Forbes. 2012 [accessed

2012 May 12]. Available from: http://www.forbes.com/sites/andygreenberg/2012/03/27/heres-how-law-enforcement-cracks-your-iphones-security-code-video/

7. Boekel P, Scandrett K. An Experience of the Virtual Desktop: a Surgical Perspective. JournalMTM. 2012 Jun. 1:2:8-10.

8. KaperskyLab. First SMS Trojan detected for smartphones running Android [Internet]. Kapersky Lab. 2010 [accessed 2012 May 12]. Available from: http://www.kaspersky.com/about/news/virus/2010/First_SMS_Trojan_detected_for_smartphones_running_Android