Table of Contents

Introduction

The following principles represent some current best practices of mobile device security.[1] These principles provide a set of guidelines, which are by no means exhaustive or comprehensive, that incorporate physical, technological, and administrative safeguards that may be used to supplement existing University policies and procedures regarding a mobile device. These guidelines summarize and synthesize some suggested best practices.

1 Data Limitation

Consider the following crucial question:

> **Do I really need to save personal and confidential information on my mobile device; is it really necessary that I transport this sensitive information?**

If the answer is no, then do not copy or transport the information. If the answer is yes, consider the following points to ensure that the security of the information is maintained with the highest integrity.

- Ensure all personally identifying information (PI)/personally identifying health information (PHI) is de-identified[2] as much as possible for the intended application.

[1] Helpful Tips – Best Practices: Mobile Device Security, available online: http://www.oipc.sk.ca/Resources/Helpful%20Tips%20-%20Best%20Practices%20-%20Mobile%20Device%20Security%20-%20March%202011.pdf [hereafter "OIPC SK"]

[2] De-identification is the process whereby portions of PI/PHI are removed, so that the PI/PHI cannot be linked to an identifiable individual while, at the same time, retaining the core elements necessary for the purpose(s) of the user.

- Consider alternatives to storing PI/PHI on your mobile device. Remotely accessing needed information via a protected remote connection (*i.e*., secure websites, Virtual Private Networks) is a more secure alternative to storing PI/PHI on the device.[3]
- Copy as few records containing PI/PHI as possible. Instead of accessing the entire database, take only the subset of records/data that you need.
- When no longer required, remove PI/PHI from your mobile device as soon as practicable. Deleting data files from the screen of a mobile device will not necessarily delete the data completely, so it may be necessary to use wiping software to permanently erase the data.

2 Password Protection

As a bare minimum, mobile devices must be password protected. Public bodies would be found to be negligent if password protection was not used to safeguard PI/PHI on their mobile devices.

Mobile computing devices should utilize passwords at power-on and when returning from a screensaver time-out. Do not share or disclose your password(s) to others.[4]

Passwords only are effective if not stolen or accidentally revealed, guessed, shared, or forgotten. In order to avoid these problems, best practices suggest some rules regarding passwords. The International Standards Organization (ISO) suggests that passwords be of sufficient lengths yet be easy to remember, not based on anything someone else could easily guess or obtain using person-related information (*i.e.,* birthdates, phone numbers), not vulnerable to dictionary attacks (*i.e.,* do not solely consist of words found in dictionaries), and are free of consecutive all numeric or all-alphabetic characters.[5]

The AICT CCID management team provides the following password creation guidelines:[6]

Ensure that your CCID password is set/changed to something you will find easy to remember. You should never have to write down your password. You should never tell anyone your password. This includes anyone from your family, or even anyone from AICT.

AICT or other University staff will never need to ask you for your password.

Beware of impostors who claim to be someone from an official position asking you what your password is - such requests are **always fraudulent** and may often come in an email message. If you are ever concerned that someone might have seen your password, or if a computer you use was broken into, you should change your password immediately. It is recommended that

[3] Whether the use of these alternatives present a practical solution, and whether the remote connection(s) is/are sufficiently secure, are factors for the government institution or University to consider.

[4] International Standards Organization, International Standard – Code of Practice for Information Security Management ISO/IEC 17799 at pg. 64. [Hereinafter ISO/IE – 17799]

[5] International Standards Organization, International Standard – Code of Practice for Information Security Management ISO/IEC 17799 at pg. 64. [Hereinafter ISO/IE – 17799]

[6] https://password.srv.ualberta.ca/passwords.html

you change your password periodically, as long as doing so doesn't mean you end up writing it down. To change your password, go to
https://password.srv.ualberta.ca/

After reading the instructions carefully, type your new password. Your requested new password will be run through a program that checks for easy to guess passwords (the same type of program that hackers use to guess passwords), so there are a few rules that you need to keep in mind:

- your password must be AT LEAST 8 characters
- it must contain at least a mixture of both upper and lower case letters, and should contain at least one numerical digit or other non-alphabetic character
- it must not be based on a single word found in *any* dictionary (any language, including odd ones like Klingon and Elvish)

Tips on choosing a new, secure password:

- pick a phrase that you can easily remember and use the first letter of each word (*i.e.*, " My dog Fido loves playing fetch in the park" might be helpful to create and remember the password "MdFlpfitp3")
- join together multiple mispelled words with mixed capitalization, numbers or miscellaneous characters (*i.e.*, CheeZ4DewDles)

Realize, however, that if your first attempt doesn't work, you must try something different. Even if something does not look like it's based on a single word to you, it may be a word in another language (the system looks at many, from French to Chinese to Klingon, because these are actually what hackers use to crack passwords). Also realize that the examples above are explicitly checked for by the program so please don't use the examples we have shown or derivatives of them. Since they are here on this page, they would be a very poor choice if we didn't prevent you from using them.

3 Encryption

Password protection on mobile devices represents a first-level method of safeguarding PI/PHI contained on those devices; in and of itself, password protection is not a complete solution.

Encryption is the current standard of minimum safeguarding. Privacy oversight offices from several Canadian jurisdictions have found that encryption is now the standard of practice for data protection on mobile devices. Several Commissioners have found organizations and individuals to be in contravention of the relevant legislation if they have not incorporated encryption protection on their mobile devices.[7]

Encryption is another security layer preventing unauthorized people from viewing sensitive information. Encryption is a mathematical process that helps to disguise stored or transmitted electronic information. Encryption codifies ordinary data into what appears to be an unintelligible stream of random symbols. A decryption key is required to decipher the encrypted data.

In Order HO-004, Ontario Information and Privacy Commissioner, Ann Cavoukian, addressed the theft of a laptop that belonged to the Hospital for Sick Children (theft occurred on January 4, 2007). It contained PHI of current and former patients. After the investigation under Ontario's Personal Health Information Protection Act,[8] the Commissioner ordered the hospital to revise policies and procedures to ensure that PHI be encrypted, particularly on mobile devices. She concludes her report with the following comment:

> "There is no excuse for unauthorized access to personal health information due to the theft or loss of a mobile computing device – any PHI contained therein must be encrypted."[9]

Alberta Information and Privacy Commissioner, Frank Work, has ruled on several instances in which mobile devices have been stolen or lost without reasonable security measures in place to protect the PI/PHI they contained. Alberta's Health Information Act[10](HIA) requires in section 60 that reasonable security measures be taken to protect health information. That section of HIA is reproduced below:

> 60(1) A custodian must take reasonable steps in accordance with the regulations to maintain administrative, technical and physical safeguards that will
> (a) protect the confidentiality of health information that is in its custody or under its control and the privacy of the individuals who are the subjects of that information,
> (b) protect the confidentiality of health information that is to be stored or used in a jurisdiction outside Alberta or that is to be disclosed by the custodian to a person in a jurisdiction outside Alberta and the privacy of the individuals who are the subjects of that information,
> (c) protect against any reasonably anticipated
> (i) threat or hazard to the security or integrity of the health information or of loss of the health information, or
> (ii) unauthorized use, disclosure or modification of the health information or unauthorized access to the health information,
> and
> (d) otherwise ensure compliance with this Act by the custodian and its affiliates.
> (2) The safeguards to be maintained under subsection (1) must include appropriate measures
> (a) for the security and confidentiality of records, which measures must address the risks associated with electronic health records, and
> (b) for the proper disposal of records to prevent any reasonably anticipated unauthorized use or disclosure of the health information or unauthorized access to the health information following its disposal.

[7] Saskatchewan OIPC, FOIP Folio March 2007, at pg. 3, available online: http://www.oipc.sk.ca/FOIPFOLIO/March2007.pdf [hereinafter; Folio March 2007]

[8] The Personal Health Information Protection Act, 2004, S.O. 2004, c. 3 Sched. A., available online: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm

[9] Ontario OIPC, Order HO-004 at pg. 2, available online: http://www.ipc.on.ca/images/Findings/up-3ho_004.pdf [hereinafter: HO-004].

[10] *The Health Information Act, 2001*, c.H-5 [hereafter "HIA"], available online: http://www.qp.gov.ab.ca/documents/Acts/H05.cfm?frm_isbn=0779719352&type=htm

> (3) In subsection (2)(a), ―electronic health records‖ means records of health information in electronic form.[11]

Commissioner Work has found that organizations are in contravention of the law if they fail to encrypt PI/PHI stored on mobile devices. He insists that a layered defence strategy, including properly implemented encryption, is required.

> "We have said time and again. It doesn't matter if the mobile device is password protected, or even double password protected, there must be another layer of protection and that layer is encryption."[12]

The following statements of David Loukidelis, British Columbia's Information and Privacy Commissioner, suggest encryption is the preferred form of securing data on mobile devices.

> "If electronic records containing sensitive personal information, such as a patient's diagnostic information, are being stored on desktop computers, laptops or a server, or your computers are connected to the internet, a reasonable security precaution would be to use both password protection and encryption to protect the information. …
>
> If a laptop containing sensitive personal information is taken off site, the data should be password protected and encrypted. The laptop should be in your control at all times. Consider locking laptops in a secure place after working on them at home.
>
> The use of a password to protect sensitive personal information will not, by itself, meet the test of reasonable security measures."[13]

This sentiment was reinforced in a joint press release issued by Commissioner Loukidelis and the New Brunswick Ombudsman. Their statements echo the conviction that encryption is the new standard in data protection on mobile devices. New Brunswick Ombudsman, Bernard Richard, stated:

> "New Brunswick's Health Department failed to ensure that personal health information was protected through encryption and that's not good enough. … personal health information is especially sensitive and deserves the best protection of all, particularly in an electronic environment."[14]

Whole disk encryption[15]

Whole disk encryption is, quite simply, when an entire hard drive is encrypted (as such it is more relevant to mobile devices such as laptops). It is easily implemented on new systems, and

[11] HIA, supra, 60(1)

[12] Alberta OIPC News Release H2007-IR-002. Available online: http://www.oipc.ab.ca/ims/client/upload/NR_CapitalEncrypt3.pdf

[13] British Columbia OIPC Investigation Report F06-02 at pg. 27, available online: http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF06-02.pdf

[14] British Columbia OIPC News Release IR F08-02, available online: http://www.oipc.bc.ca/news/rlsgen/NR_IR_F08-02.pdf [Herein after NR IR F08-02].

[15] OIPC SK, supra note 1

should be considered as a requirement for any new mobile device. Whole disk encryption software is available from multiple companies for those installations on older systems.

Whole disk encryption is potentially the most secure option available to organizations or individuals who feel they must store PI/PHI on mobile devices. A system with an encrypted disk requires a decryption password upon start-up. Without that password, there is an extremely low probability that the PI/PHI it contains could ever be viewed by an unauthorized person.

Device encryption[16]

Similar to whole disk encryption, entire devices may be encrypted. Portable storage devices, such as a flash drive or USB key, present an alternative to storing PI/PHI on a laptop. Encryption in these devices is a must as they are frequently lost or misplaced.

4 Physical Security

Ensuring the physical security of a mobile device may appear to be common sense, however, the importance of taking basic steps to maintain physical security cannot be understated.[17] If the device is not stolen in the first place then a breach, though not impossible, is highly unlikely. As the Government of Canada's Public Safety website points out:

> "If an unauthorized user has physical access to a laptop computer system, then gaining administrative access (*i.e.*, the ability to run any program) to the laptop, and its sensitive data, is a simple process."[18]

The following safeguards offer relatively inexpensive ways of ensuring the physical security of mobile devices.[19]

- Do not leave mobile devices unattended in your vehicle. If it absolutely cannot be avoided, lock them in the trunk of the vehicle. If the vehicle has no trunk, leaving the device in the vehicle is not a secure option.
- It is never advisable, when using your mobile device in a public place, to leave it unattended. If it is absolutely necessary to leave a mobile device unattended, it should be secured to a large heavy object. For example, a cable lock could be utilized to secure a laptop to the object in such an instance.
- Equip your mobile device with an audible alarm. There are free applications which will sound an alarm whenever anyone unplugs the power cable, the mouse is moved or unplugged, or the laptop is shut down.

[16] *Ibid.*
[17] *Ibid.*
[18] Government of Canada, Public Service Canada. General Best Practices for Laptop Security, available online: http://www.publicsafety.gc.ca/prg/em/goc/in04-001-en.asp
[19] OIPC SK, supra note 1

- Lock mobile devices away when not in use.
- Use a non-descript lockable briefcase or laptop case that does not bear any visible logos of your organization or of the device manufacturer.
- Consider using asset tags. Asset tags are semi-permanent tags which will leave a type of tattoo if removed. This simple security measure may deter those thieves who realize an identifying mark will be left on the laptop.

5 System Integrity[20]

It is very important to maintain the integrity and security of the software on your mobile device by updating software. The process of updating software for known vulnerabilities is referred to as patching. Patching software regularly prevents unauthorized users from exploiting known vulnerabilities. Most vendors provide simple notification and update procedures and services. Most software manufacturers will offer some form of updating service for their products.

Update services offer simple and reliable ways to make sure the software on your mobile device stays updated with security and reliability updates, device drivers, service packs, and other updates. Some software can be enabled to continuously check for, download, and install updates automatically.

- Make sure your mobile device (in particular computers) has anti-virus, malware, and spyware software installed and enabled. Periodically run full system scans to check for viruses and other malicious codes. Extend the full scan to the contents of your mobile devices as well (*i.e.*, run a full scan on everything on your USB, or all drives of your laptop or desktop computer).

- If the mobile device is a computer, keep the software up to date. Turn automatic updates on.

- Mobile device users should never download free software or applications from the Internet without a high level of assurance that the product is safe and contains no adware, spyware, or viruses. This includes downloading applications for iPad®, BlackBerry® and iPhone®. Applications that are not properly screened could infect the mobile device with vulnerabilities such as clickjacking/tapjacking, smudge attacks or keystroke caching.[21] Organizations may wish to set permissions on network devices so that users are not allowed to install software. They can do this through the use of configuration profiles.

- Consider using a personal firewall. It will effectively defend a computer from many of the most pervasive and dangerous internet attacks.

- Those organizations that have the ability to do so can implement and deploy sophisticated frameworks that offer very good protection for mobile devices and their networks. These run

[20] *Ibid.*

[21] Clickjacking/tapjacking: Superimposing a transparent page over top of a legitimate one. You think you are navigating through a certain web page but you are not. Through this, the false page can navigate you through steps that open up access to your device. Smudge attacks: Touch screens are touched, so oil residues, or smudges, remain on the screen as a side effect. Latent smudges may be usable to infer recently and frequently touched areas of the screen—a form of information leakage. Keystroke caching: allows a hacker to log every keystroke the device user types.

the gamut from quarantining mobile devices when they connect to the network in order to verify patch levels and virus scans, to preventing laptops remotely connecting to networks while connected to the Internet.

6 Wireless Security Considerations

Public wireless networks are by their nature open therefore not secure. Data transmitted by one device across the open airwaves can be picked up and read by another device. As such, it is important to incorporate some basic safety practices when accessing wireless connections with mobile devices.[22]

- Ensure the PI/PHI you are working with is encrypted, and when possible, sufficiently de-identified.

- Watch out for shoulder surfing. Working on a laptop in a public place may allow others to see what you are working on. Try to work away from crowds in a secluded area. You may also want to consider using a privacy filter. Privacy filters are screens that are temporarily affixed to a laptop monitor. With a privacy filter in place, only someone looking directly at the screen can see it, but to others it looks dark.

- Avoid connecting to two separate networks (such as Wi-Fi and Bluetooth) simultaneously, which may turn your device into an access point.

- Set your device so any wireless connection is off by default (i.e. Wi-Fi and Bluetooth). Turn on wireless connections only when it is required. If you have a laptop, but are not using the wireless card, turn it off.

- When carrying out confidential work over the Internet, ensure you use a secure connection. Secure communication environments are often created using Hypertext Transfer Protocol over Secure Socket Layer (HTTPS). HTTPS is how most of us carry out our on-line banking, file our taxes, and, hopefully, when using a credit card for on-line shopping. This is a reliable, secure and easy method of ensuring Internet security.

7 Data Wiping[23]

A worthwhile security consideration for individuals and organizations is configuring their mobile devices (specific to this case, cell phones and PDA‘s) so that they can be “wiped” remotely. Wiping occurs when the data on a device is deleted and there is no data back-up performed. Setting devices so that they can be wiped is useful if the device is ever lost or stolen.

Remote wiping is a feature which allows a device administrator to force a device to delete its contents remotely. Wiping provides good risk mitigation in the event that a mobile device is lost or stolen, and there is a chance that someone could access PI/PHI. Wiping is intended to

[22] OIPC SK, supra note 1

[23] *Ibid.*

provide an additional layer of security on top of the previous suggestions. It is suggested that your IT administrators provide confirmation of the remote wipe success or failure.

8 Mobile Device Loss

If, despite all your precautions, a mobile device is stolen or lost, report it immediately to your organization. The following stakeholders need to be immediately notified:

- Your supervisor/manager
- Your IT administrator responsible for connecting the stolen or lost device onto the faculty, department, or unit's network
- The University's Privacy Officer and/or IT Security Officer

9 Proper Disposal[24]

Mobile devices do not last forever. Technology is quickly outdated and old models are traded in for newer versions. Thousands of surplus devices that once housed sensitive data are being stored, recycled or donated. This data could include the personal information or personal health information of individuals. Therefore, proper management of surplus devices is critical to avoid this sensitive information falling into the wrong hands.

Proper disposal should include the following:

- Mobile devices should be stored securely until they are sent for recycling, refurbishing or donation. This can include a locked file cabinet or room.

- Prior to recycling, refurbishing or donation the mobile device should be thoroughly wiped clean of all data. This includes hard drives on laptops. Your IT administrators should conduct the data wiping.

- If the recycling, refurbishing or donating process is contracted to an outside organization, proper contracts need to be in place that include confidentiality, security clearance for staff and disposal deadlines. To ensure clear accountability, monitor contracts by scheduling regular inspections.

- Internal random audits will ensure compliance with policies, procedures and processes. It is one thing to have them in place, but it is another to ensure they are being followed.

[24] *Ibid.*