

# Helpful Tips

## Best Practices: Mobile Device Security



### Background

Mobile computing and communication devices (mobile devices), such as the laptop computer, iPad, flash drive, PDA, BlackBerry®, cell phone, iPhone, etc. are common fixtures in the office environment of government institutions, local authorities, and trustees (both individuals and organizations). These devices have become indispensable tools because they offer increasingly large capacity in fast, easy to use, compact, portable formats; in short, they are convenient. However, that convenience bears with it some associated risks.

Mobile devices are easy to steal and easy to misplace. As a result of either of these misfortunes, privacy breaches of confidential information occur whether the information contained in them is accessed or not. Beyond the theft or loss of a device, privacy breaches can occur as a result of utilizing unsecured wireless networks.

Privacy breaches of this sort can have far reaching implications due both to the nature of the information being compromised, and the number of individuals affected by it. As such, it is the view of the Office of the Information and Privacy Commissioner (OIPC) of Saskatchewan that government institutions, local authorities, and trustees must address three different kinds of safeguards:

- (1) administrative,
- (2) technical, and
- (3) physical

in order to discharge their obligations to protect personal information and personal health information in their custody/possession or control as provided by in Saskatchewan access and privacy legislation.<sup>1</sup>

<sup>1</sup> Saskatchewan OIPC Investigation Reports [H-2005-002](#), [F-2007-001](#), [H-2007-001](#), available online: [www.oipc.sk.ca/reviews.htm](http://www.oipc.sk.ca/reviews.htm)





## How many people could be affected?



Now multiply the intrinsic value of the information on the device by the storage capacity of the device. Considering the ever increasing storage capacity of mobile devices, it is easy to gain a sense of how significant numbers of individuals could be affected by security breaches involving these devices.

The OIPC of British Columbia investigated a privacy breach following the theft of a laptop from a lawyer's office.<sup>5</sup> The laptop contained client files and information relating to legal work; including contracts, notarized documents, leases and wills of both current and former clients. The OIPC asked the lawyer to notify his current and former clients of the loss of their personal information.

The Ontario OIPC investigated the theft of a single laptop computer from a physician's personal vehicle.<sup>6</sup> In this case, the computer contained the PHI of approximately 2,900 current and former patients of a children's hospital involved in five prospective research studies and five retrospective research studies.

The Alberta OIPC investigated two high profile cases involving laptop theft as well. In the first, a single laptop computer was stolen from the vehicle of an employee of a private sector management company.<sup>7</sup> This computer contained the PI of 8,000 Alberta physicians. The other involved the theft of four laptop computers from a regional health authority office. In this case, the PHI of 20,000 private citizens was breached.

Regardless of the size of the breach, the sensitivity of the information and the relative ease with which it could be breached requires that the stewards of the information take as many measures as reasonably possible to safeguard the information.

<sup>5</sup> British Columbia Mediation Case Summary [P07-04-MS](http://www.oipcbc.org/Mediation_Cases/pdfs/2007/P07-04-MS.pdf), available online: [http://www.oipcbc.org/Mediation\\_Cases/pdfs/2007/P07-04-MS.pdf](http://www.oipcbc.org/Mediation_Cases/pdfs/2007/P07-04-MS.pdf)

<sup>6</sup> HO-004. *supra*, note 2.

<sup>7</sup> Alberta OIPC Investigation Report [P2006-IR-005](http://www.oipc.ab.ca/ims/client/upload/ACFAB50.pdf), available online: <http://www.oipc.ab.ca/ims/client/upload/ACFAB50.pdf>

<sup>8</sup> Alberta OIPC Investigation Report [H2007-IR-002](http://www.oipc.ab.ca/ims/client/upload/H1652%20Oct%2019-07%20Final%20CH%20Laptop%20IR.pdf), available online: <http://www.oipc.ab.ca/ims/client/upload/H1652%20Oct%2019-07%20Final%20CH%20Laptop%20IR.pdf>



## What can be done?

The following principles represent some current best practices of mobile device security. These principles provide a set of guidelines, which are by no means exhaustive, that incorporate physical, technological, and administrative safeguards that may be used to supplement existing organizational policies and procedures regarding a mobile device. These guidelines summarize and synthesize some suggested best practices for private and public sector organizations.



## BEST PRACTICES: Mobile Device Security

### 1 Data Limitation

Almost every source cited in the research for this document suggested, in one form or another, that users of mobile devices ask themselves the following crucial question:

**Do I really need to save PI/PHI 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 PI/PHI is de-identified<sup>9</sup> as much as possible for the intended application.
- 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.<sup>10</sup>
- Remove 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 practical. Deleting data files from the screen of a mobile device won't necessarily delete the data completely, so it may be necessary to use wiping software to permanently erase the data.

<sup>9</sup> 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.

<sup>10</sup> 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, local authority or trustee to consider.



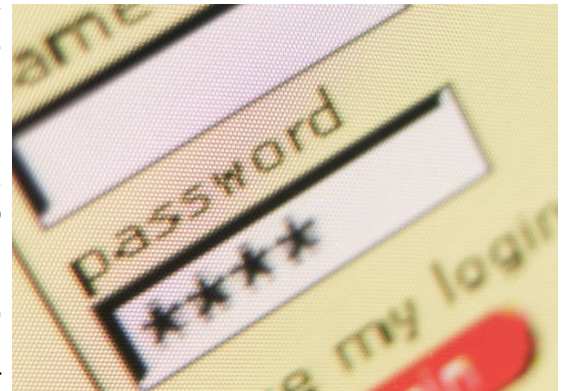
## 2 Password Protection

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

It is a relatively standard practice that initially each user registers or is registered by someone else, using an assigned or self-declared password. On subsequent uses, the user must know and use the previously declared password. For example, all accounts should utilize passwords at power-on and when returning from a screensaver time-out.

Passwords only are effective if not stolen or accidentally revealed, guessed, 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.<sup>11</sup>



The Ontario OIPC provides further advice on the creation of strong passwords:

“Strong login passwords are comprised of at least eight characters, with 14 or more being ideal. These should include a combination of upper and lower case letters, numbers and symbols (such as %, &, or #), rather than dictionary words. Do not use passwords that are predictable, such as birthdays, your spouse’s name or your favourite sports team, or easy-to-guess combinations of dictionary words, such as the frequently used LetMeIn. Instead, try basing a mixed, multi-character password on a phrase or favourite song, book title or TV program. For example, My favourite show 24 is on Tuesdays at 9 can become the password: Mfs24ioT@9.”<sup>12</sup>

<sup>11</sup> International Standards Organization, *International Standard - Code of Practice for Information Security Management ISO/IEC 17799* at pg. 64. [Hereinafter ISO/IE - 17799]

<sup>12</sup> Ontario OIPC, *Safeguarding Privacy in a Mobile Workplace* (Pamphlet), available online: <http://www.ipc.on.ca/images/Resources/up-mobileworkplace.pdf>



### 3 Authentication



Authentication is the process of determining whether someone is who they declare to be.<sup>13</sup> While password identification represents the minimum security level for authentication, best practice literature suggests multiple layer authentications.

Authentication is most commonly achieved through the use of logon passwords. Knowledge of the password is assumed to guarantee user authenticity.

Best practice regarding multiple layer authentications suggests a user should be required to present at least two of the following:

- (a) something they know (password matched with a username)
- (b) something they have (such as a security token. This is a physical device that an authorized user of computer services is given to ease authentication. Security tokens are used to prove one's identity electronically by acting like an electronic key to access something)
- (c) something they are (biometrics).

Biometric encryption is the process of using a characteristic of the body (a biometric) as a method to code or scramble/descramble data. Physical characteristics such as fingerprints, hands, retinas, and voices are either currently in use, or are being researched as, methods of biometric encryption today.<sup>14</sup> In this encryption process, a biometric and a Personal Identification Number (PIN), or other cryptographic key<sup>15</sup>, are securely bound so that neither the PIN nor the biometric can be retrieved from the stored template. The PIN is re-created only if the correct biometric is presented on verification.<sup>16</sup>

Since physical characteristics are unique to each individual, biometric encryption is seen as an answer to combat computer related theft and fraud. One reason this new technology is believed to be superior to the use of passwords or PINs is that a biometric trait cannot be lost, stolen, or recreated, at least not easily.

<sup>13</sup> Laudon, Kenneth C. and Laudon, Jane. *Management Information Systems: Managing the Digital Firm 3<sup>rd</sup> Canadian Edition*, Pearson Prentice Hall, 2007 at pg. 323.

<sup>14</sup> Ontario OIPC, *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security and Privacy* at pg. 4, available online: [http://www.ipc.on.ca/images/Resources/up-1bio\\_encryp.pdf](http://www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf) [Hereinafter: ONT Biometric Encryption]

<sup>15</sup> A cryptographic key is a small piece of information that when utilized with an encryption algorithm transforms plaintext to indecipherable text or vice versa.

<sup>16</sup> ONT Biometric Encryption, supra note 14 at pg. 16.



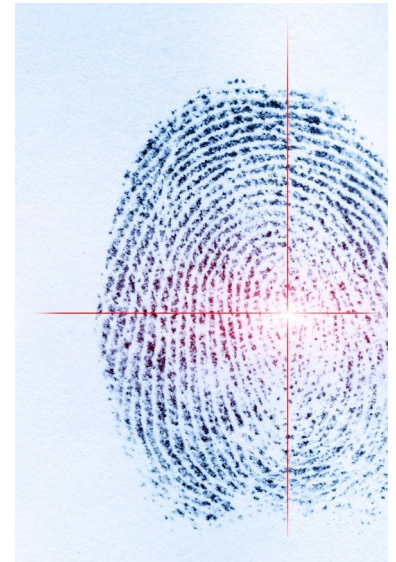
## 3 Authentication

Biometric encryption has the potential for virtually unlimited application in terms of mobile devices. Currently the cost of such applications may prove prohibitive for organizations and individuals who do not have the financial resources to utilize this technology.

It is important that users of mobile devices recognize that while password protection and multiple layer authentications do provide some security for those devices, there are some general guidelines that should be observed in their regard. It has been said that “good fences make good neighbours.” While it may not actually be true that good fences make good neighbours, a good fence at least helps to keep out the bad neighbours. Strong passwords and multiple layer authentications are equivalent to those good fences, and following some basic rules about passwords is a proactive means to ensure that those fences stay in place before a security problem occurs.<sup>17</sup>

As noted in the *Handbook of Applied Cryptography*.

“It is sound cryptographic [the practice and study of hiding information] practice to change the key (encryption/decryption transformation) frequently. As a physical analogue, consider an ordinary resettable combination lock. The structure of the lock is available to anyone who wishes to purchase one but the combination is chosen and set by the owner. If the owner suspects that the combination has been revealed he can easily reset it without replacing the physical mechanism.”<sup>18</sup> [added by writer]



<sup>17</sup> For more discussion on proactive password practices see: Bishop, Matt and Klein, Daniel. *Improving System Security via Proactive Password Checking*, 1992, available online: <http://www.klein.com/dvk/publications/passwd-matt-final.pdf>

<sup>18</sup> Menezes, Alfred, van Oorschot, Paul and Vanstone, Scott. *The Handbook of Applied Cryptography*, CRC Press, 1996 at pg. 12.



## 3 Authentication

Passwords and encryption keys can be further protected by following the good security practices forwarded by the ISO:

- keep passwords confidential;
- avoid keeping a record of the password, unless the recording method has been approved, and the record can be securely stored;
- do not use the same password to log into your computer and to unlock your encrypted files;
- do not use the same password for everything that requires a password (i.e. do not use your work password for your personal banking password);
- change passwords and keys frequently, especially when there is any indication of possible system or password compromise;
- change temporary passwords at first log-on;
- do not reuse passwords; and
- do not share passwords.<sup>19</sup>

## 4 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 in their mobile devices.<sup>20</sup>

Encryption is the only guaranteed way to prevent people from viewing confidential data. Encryption is a mathematical process that helps to disguise stored or transmitted computer data. Encryption codifies ordinary data into what appears to be an unintelligible stream of random symbols. A 'key' is required to decipher the encrypted data.



<sup>19</sup> ISO/IEC 17799, supra note 11 on page 5

<sup>20</sup> Saskatchewan OIPC, *FOIP Folio March 2007*, at pg. 3, available online: <http://www.oipc.sk.ca/FOIPFOLIO/March2007.pdf> [hereinafter, Folio March 2007]



### 4 Encryption

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. It contained PHI of current and former patients. After the investigation under Ontario's *Personal Health Information Protection Act*,<sup>21</sup> 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."<sup>22</sup>

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*<sup>23</sup> (HIA) requires at 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.
- (3) In subsection (2)(a), "electronic health records" means records of health information in electronic form.<sup>23</sup>

<sup>21</sup> *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](http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm)

<sup>22</sup> HO-004 supra note 2, at pg. 2.

<sup>23</sup> *The Health Information Act, 2001*, c.H-5, available online: [http://www.qp.gov.ab.ca/documents/Acts/H05.cfm?frm\\_isbn=0779719352&type=htm](http://www.qp.gov.ab.ca/documents/Acts/H05.cfm?frm_isbn=0779719352&type=htm)



### 4 Encryption

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.”<sup>24</sup>

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.”<sup>25</sup>

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.”<sup>26</sup>



<sup>24</sup> Alberta OIPC News Release [H2007-IR-002](#). Available online: [http://www.oipc.ab.ca/ims/client/upload/NR\\_CapitalEncrypt3.pdf](http://www.oipc.ab.ca/ims/client/upload/NR_CapitalEncrypt3.pdf)

<sup>25</sup> British Columbia OIPC Investigation Report [F06-02](#) at pg. 27, available online: [http://www.oipc.bc.ca/orders/investigation\\_reports/InvestigationReportF06-02.pdf](http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF06-02.pdf)

<sup>26</sup> British Columbia OIPC News Release [IR F08-02](#), available online: [http://www.oipc.bc.ca/news/rlsgen/NR\\_IR\\_F08-02.pdf](http://www.oipc.bc.ca/news/rlsgen/NR_IR_F08-02.pdf) [Herein after NR IR F08-02].



## 4 Encryption

Commissioner Loukidelis agreed:

“BC’s health ministry should not have been couriering around unprotected tapes of personal health information like this. It doesn’t matter that the tapes can only be read using technology that’s not commonly available. **Proper encryption is the basic standard for portable data storage like this.**”<sup>27</sup> (Emphasis added)

In Saskatchewan *The Health Information Protection Act*<sup>28</sup> (HIPA) also stipulates, at section 16, that trustees ensure that technical, administrative and physical safeguards are in place to protect PHI. That section is reproduced below:

16 Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:

- (a) protect the integrity, accuracy and confidentiality of the information;
- (b) protect against any reasonably anticipated:
  - (i) threat or hazard to the security or integrity of the information;
  - (ii) loss of the information; or
  - (iii) unauthorized access to or use, disclosure or modification of the information; and
- (c) otherwise ensure compliance with this Act by its employees.<sup>29</sup>

The Information and Privacy Commissioner of Saskatchewan recommends that all Saskatchewan public sector organizations make a point of reading the above referenced decisions. The Commissioner believes that encryption is the standard for data protection on mobile devices, and recommends that public sector organizations carefully consider whether their organizations currently meet this standard.<sup>29</sup>

Since the effectiveness of encryption depends on both the encryption standard and the strength of the key used, the same rules outlined above for passwords should be applied to encryption keys.



<sup>27</sup>

Ibid.

<sup>28</sup>

HIPA, supra note 3 on pg. 2.

<sup>29</sup>

*FOIP Folio March 2007*, supra note 19 at pg. 8.



### 4 Encryption

Encryption standards are always evolving as are the methods used for breaking them. Government institutions, local authorities, and trustees are ultimately responsible for ensuring that the encryption installation they use is up to date, and meet the generally accepted standards in effect at the time. To be effective, encryption installations need to be regularly reviewed and updated.

Encryption is complex. There is an endless array of choices in terms of encryption installations. The risk of unencrypted data loss is enormous to any organization, so government institutions, local authorities, and trustees should always seek input from their Information Technology (IT) departments or from other qualified professionals to ensure they chose the encryption solutions appropriate for them.

How encryption is implemented is largely determined by the amount of data to be encrypted and the size of the organization (thus the number of mobile devices requiring access to the data).<sup>30</sup> Outlined below are the most common methods of data encryption.



#### Whole disk encryption

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 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.

#### Folder encryption

Current operating systems provide some built-in encryption options. They provide only limited protection and are insufficient, in and of themselves, because they rely on the user's login password. If a person gains access to the user's password, they will then have access to the data.

<sup>30</sup> Ontario OIPC, *Encrypting Personal Health Information on Mobile Devices. Fact Sheet 12, May 2007*, available online: [http://www.ipc.on.ca/images/Resources/up-fact\\_12e.pdf](http://www.ipc.on.ca/images/Resources/up-fact_12e.pdf) [Hereinafter "Fact Sheet 12"]



### 4 Encryption

#### Device encryption

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. Like hard drives, there are options to encrypt the entire device or just the parts of the device. Encryption in these devices is a must as they are frequently lost or misplaced.

It is important to remember that encryption is a significant piece of the puzzle in terms of securing PI/PHI on mobile devices; it is however, not the entire solution.

It is important for mobile device users to bear in mind the following note of caution regarding encryption. If a mobile device user should lose or forget their encryption password, there is an extremely low probability that the PI/PHI it contains could ever be viewed. This means that data could be lost or at least inaccessible even to legitimate users. This should also be a consideration for organizations in context of important corporate information. Backup copies of such data should be maintained in a separate, secure environment. As well, encryption passwords for mobile devices should be recorded and secured appropriately.

### 5 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. 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."<sup>31</sup>



<sup>31</sup> 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>



### 5 Physical Security

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

- 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.
- 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.



### 6 System Integrity

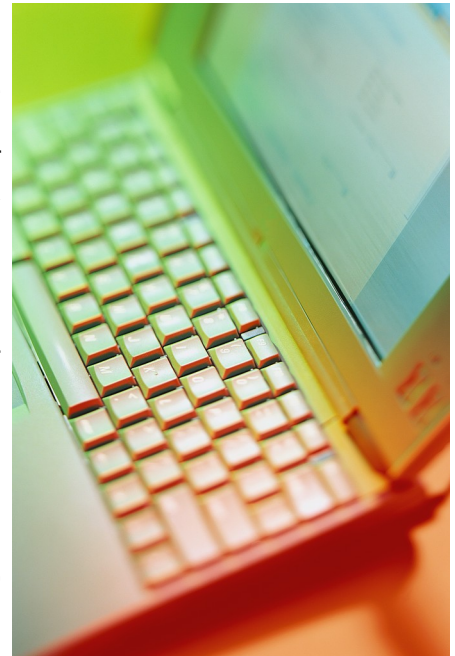
It is very important to maintain the integrity and security of the software on your mobile device by updating software. The process of updating software for known vulnerabilities is referred to as patching. Patching software regularly prevents unauthorized users from exploiting known vulnerabilities.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



### 6 System Integrity

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<sup>32</sup>, smudge attacks or keystroke caching<sup>1</sup>. 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 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.



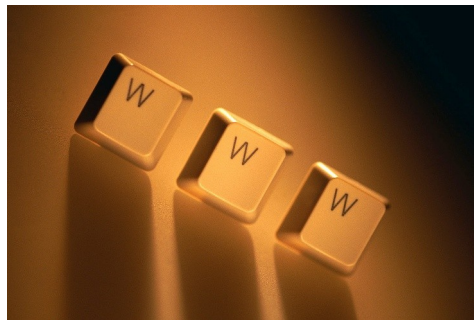
<sup>32</sup> **Clickjacking/tapjacking:** Superimposing a transparent page over top of a legitimate one. You think you are navigating through a certain web page but you are not. Through this, the false page can navigate you through steps that open up access to your device. **Smudge attacks:** Touch 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.



### 7 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.

- 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.



### 8 Data Wiping

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". 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 provide an additional layer of security on top of the previous suggestions. It is suggested that the exchange environment provide confirmation of the remote wipe success or failure.

### 9 Mobile Device Loss



If, despite all your precautions, a mobile device is stolen or lost, report it immediately to your organization (i.e. Privacy Officer, etc.) and the police, if appropriate in the circumstances. If the PI/PHI contained on the mobile device was inadequately protected, consider notifying affected individuals of the potential privacy breach. You will need to evaluate the incident and take the necessary steps to mitigate risks that may arise.

#### Responding to a Privacy Breach

There are several resources available to organizations that encounter a privacy breach. These resources can assist organizations with how to assess the impact of a breach, and how to respond to a breach.

The Saskatchewan OIPC offers the *Privacy Breach Guidelines* which provide guidance for government institutions, local authorities and health care trustees faced with a privacy breach.<sup>33</sup> The Access and Privacy branch of the Ministry of Justice and Attorney General offers the *Information Management Handbook*<sup>34</sup> for all government and local authorities. Another resource for carrying out a breach of privacy assessment is the *Breach Notification Assessment Tool*. It was jointly produced by the Ontario and British Columbia OIPCs.<sup>35</sup> The Alberta OIPC also offers a resource for reporting privacy breaches with their Key Steps in Responding to Privacy Breaches. The Alberta OIPC also offers a resource for reporting privacy breaches with their *Key Steps in Responding to Privacy Breaches*.<sup>36</sup>

<sup>33</sup> Saskatchewan OIPC *Privacy Breach Guidelines*, available online: [http://www.oipc.sk.ca/Resources/Privacy%20Breach%20Guidelines1%20\(3\).pdf](http://www.oipc.sk.ca/Resources/Privacy%20Breach%20Guidelines1%20(3).pdf); Saskatchewan OIPC *Reviews and Investigations* at pg. 52, available online: <http://www.oipc.sk.ca/Presentations/OIPC%20%20Reviews%20and%20Investigations.%20December%2010.%202007%20for%20web.pdf>

<sup>34</sup> Ministry of Justice, Access and Privacy branch *Information Management Handbook*, available online: <http://www.justice.gov.sk.ca/InformationManagementHandbook>

<sup>35</sup> British Columbia and Ontario OIPCs *Breach Notification Assessment Tool*, available online: [http://www.oipcbc.org/pdfs/Policy/ipc\\_bc\\_ont\\_breach.pdf](http://www.oipcbc.org/pdfs/Policy/ipc_bc_ont_breach.pdf) and at: [http://www.ipc.on.ca/images/Resources/up-ipc\\_bc\\_breach.pdf](http://www.ipc.on.ca/images/Resources/up-ipc_bc_breach.pdf)

<sup>36</sup> Alberta OIPC *Key Steps in Responding to Privacy Breaches*, available online: <http://www.oipc.ab.ca/ims/client/upload/Key%20Steps%20in%20Responding%20to%20a%20Privacy%20Breach%202007.pdf>



### 10 Proper Disposal



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.

It is vital that proper policies, procedures and processes are developed and in place to ensure that sensitive data on surplus devices is protected from unauthorized release.

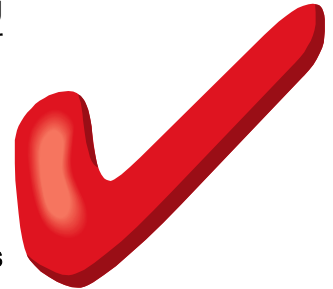
Proper disposal should include the following:

- 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. Refer to page 17– Best Practice #8– Data Wiping for more information .
- 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.



### MOBILE DEVICE CHECKLIST

The following checklist is included for readers to use to assist them in making sure they are taking as many steps as possible to protect PI/PHI on their mobile devices.



- I have minimized the amount of PI/PHI that I have on mobile devices (preferably none in identifiable form).
- I deleted PI/PHI from all mobile devices as soon as I have finished working with it.
- I know what PI/PHI is stored on each of my mobile devices.
- I have enabled my operating system encryption.
- I have purchased a system with whole disk encryption.

OR

- I have purchased software to implement whole disk or virtual disk encryption on my mobile device.
- If I use portable storage devices such as USB keys, I encrypt them before I use them.
- If I use a password to access encrypted data, it is a strong password AND it is different than the password that I use to login to my computer.
- I never write my password down.
- I do not share my password with anyone.
- If I don't use whole disk encryption, I can identify where ALL of the PI/PHI on my system is stored.
- I only store PI/PHI on the encrypted disk.
- I regularly verify or audit that my encryption policies are, in fact, being implemented and followed.<sup>37</sup>

---

<sup>37</sup> Fact Sheet 12, supra note 30 at pg. 4



## RESOURCES

The most accessible resources available to you may likely be your organization's Privacy Officer and your Information Technology (IT) department. Please consult with your organization's Privacy Officer and/or IT department or a recognized IT professional for advice on mobile device security considerations.

A list of resources utilized in the creation of this article, as well as other useful resources on the topics covered within are found below.

- A special note of thanks to the staff of the Saskatchewan Legislative Assembly Service, Communication and Technology Services for their input into this article.

---

Office of the Information & Privacy Commissioner of Saskatchewan  
Website: <http://www.oipc.sk.ca>

---

### Legislation

*The Health Information Protection Act.*

Available online: <http://www.qp.gov.sk.ca/documents/english/Statutes/Statutes/H0-021.pdf>

*The Freedom of Information and Protection of Privacy Act*

Available online: <http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/F22-01.pdf>

*The Local Authority Freedom of Information and Protection of Privacy Act.*

Available online: and <http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/L27-1.pdf>

### Reports

Investigation Report H-2005-002: Prevention Program for Cervical Cancer. April 27, 2005.

Available online: <http://www.oipc.sk.ca/Reports/H-2005-002.pdf>

Investigation Report F-2007-001

Available online: <http://www.oipc.sk.ca/Reports/InvReportF-2007-001.pdf>

Investigation Report H-2007-001

Available online: <http://www.oipc.sk.ca/Reports/IR%20H-2007-001.pdf>



## RESOURCES

---

Office of the Information & Privacy Commissioner of Saskatchewan  
Website: <http://www.oipc.sk.ca/default.htm>

---

### Newsletters:

February/March 2011 FOIP Folio - iPad Mobile Devices – It's All About Access!  
March 2007 FOIP Folio - Laptop Encryption.  
March 2006 FOIP Folio - Is your computer being hijacked?  
December 2005 FOIP Folio - Watch your BlackBerry®.  
Available online: <http://www.oipc.sk.ca/newsletters.htm>

### Publications

Privacy Breach Guidelines  
Available online:  
[http://www.oipc.sk.ca/Resources/Privacy%20Breach%20Guidelines1%20\(3\).pdf](http://www.oipc.sk.ca/Resources/Privacy%20Breach%20Guidelines1%20(3).pdf)

---

Government of Saskatchewan  
Website: <http://www.gov.sk.ca>

---

Information and Technology Office  
Website: <http://www.ito.gov.sk.ca/>

Ministry of Justice & Attorney General  
Access & Privacy Branch  
Website: <http://www.justice.gov.sk.ca/accessandprivacy>  
Information Management Handbook  
Available online: <http://www.justice.gov.sk.ca/InformationManagementHandbook>

Public Service Commission of Saskatchewan  
Human Resources Information Technology Manuals  
[www.psc.gov.sk.ca/Default.aspx?DN=f40bcab3-91c0-4253-8b39-8f52f2ff734c](http://www.psc.gov.sk.ca/Default.aspx?DN=f40bcab3-91c0-4253-8b39-8f52f2ff734c)



### RESOURCES

---

Office of the Information & Privacy Commissioner of British Columbia  
Website: <http://www.oipc.bc.ca>

---

Protecting Personal Information Outside the Office, February 2005.

Available online: [http://www.oipc.bc.ca/pdfs/public/PersonalInfoOutsideOffice\\_\(Feb2005\).pdf](http://www.oipc.bc.ca/pdfs/public/PersonalInfoOutsideOffice_(Feb2005).pdf)

Investigation Report F06-01: Investigation into the Sale of Provincial Government Computer Tapes Containing Personal Information. March 31, 2006.

Available online:

[http://www.oipc.bc.ca/orders/investigation\\_reports/InvestigationReportF06-01.pdf](http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF06-01.pdf)

Physicians & Security of Personal Information, June 2006.

Available online: <http://www.oipc.bc.ca/pdfs/private/PhysicianSecurityofpersonalinformation.pdf>

Mediation Summary P07-04 MS: Laptop Stolen from Lawyer's Office. February 13, 2007.

Available online: [http://www.oipc.bc.ca/Mediation\\_Cases/pdfs/2007/P07-04-MS.pdf](http://www.oipc.bc.ca/Mediation_Cases/pdfs/2007/P07-04-MS.pdf)

Investigation Report F08-02: Investigation Into the Sale of Unencrypted Computer Tapes. May 07, 2008.

Available online:

[http://www.oipc.bc.ca/orders/investigation\\_reports/InvestigationReportF08-02.pdf](http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF08-02.pdf)



### RESOURCES

---

#### Information & Privacy Commissioner of Alberta

Website: <http://www.oipc.ab.ca/home/>

---

Investigation Report P2006-IR-005: Report of an Investigation into the Security of Personal Information. September 26, 2006.

Available online: <http://www.oipc.ab.ca/ims/client/upload/ACFAB50.pdf>

Investigation Report H2006-IR-002: Report of an Investigation Concerning a Stolen Laptop Computer. December 5, 2006.

Available online: [http://www.oipc.ab.ca/ims/client/upload/H2006-IR-002%20\\_2\\_1.pdf](http://www.oipc.ab.ca/ims/client/upload/H2006-IR-002%20_2_1.pdf)

Investigation Report H2007-IR-002: Investigation Report Concerning Stolen Laptops Containing Health Information. November 5, 2007.

Available online:

<http://www.oipc.ab.ca/ims/client/upload/H1652%20Oct%2019-07%20Final%20CH%20Laptop%20IR.pdf>

Key Steps in Responding to Privacy Breaches

Available online:

<http://www.oipc.ab.ca/ims/client/upload/Key%20Steps%20in%20Responding%20to%20a%20Privacy%20Breach%202007.pdf>

---

#### Manitoba Ombudsman

Website: <http://www.ombudsman.mb.ca/>

---

Protecting Personal & Personal Health Information When Working Outside the Office. April 2007.

Available online:

<http://www.ombudsman.mb.ca/pdf/PN-BBT12%20Protecting%20Personal%20and%20Personal%20Health%20Information%20when%20Working%20Outside%20the%20Office.pdf>



### RESOURCES

---

Information & Privacy Commissioner of Ontario  
Website: <http://www.ipc.on.ca>

---

Fact Sheet 10, Key Steps in Responding to Privacy Breaches: Secure Destruction of Personal Information. December 2005.

Available online: [http://www.ipc.on.ca/images/Resources/up-fact\\_10\\_e.pdf](http://www.ipc.on.ca/images/Resources/up-fact_10_e.pdf)

Breach Notification Assessment Tool. December 2006.

Available online:

[http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-S\\_Summary/?id=581](http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-S_Summary/?id=581)

Fact Sheet 12, Encrypting Personal Health Information on Mobile Devices, March 2007.

Available online: [http://www.ipc.on.ca/images/Resources/up-4fact\\_12\\_e.pdf](http://www.ipc.on.ca/images/Resources/up-4fact_12_e.pdf)

Order HO-004: Order regarding a stolen laptop computer belonging to the Hospital for Sick Children. March, 2007.

Available online: [http://www.ipc.on.ca/images/Findings/up-ho\\_004.pdf](http://www.ipc.on.ca/images/Findings/up-ho_004.pdf)

Safeguarding Privacy in a Mobile Workplace (Pamphlet)

Available online: <http://www.ipc.on.ca/images/Resources/up-mobilewkplace.pdf>

BlackBerry® Cleaning: Tips on How to Wipe Your Device Clean of Personal Data

Available online: <http://www.ipc.on.ca/images/Resources/blackberry-cleaning.pdf>



### RESOURCES

---

#### The SANS Institute

---

Grant, Chris. Defense-In-Depth Applied to Laptop Security: Ensuring Your Data Remains Your Data. October 14, 2003.

[http://www.sans.org/reading\\_room/whitepapers/bestprac/1263.php](http://www.sans.org/reading_room/whitepapers/bestprac/1263.php)

---

Government of Canada  
Communications Security Establishment Canada  
Website: <http://www.cse-cst.gc.ca/index-e.html>

---

Public Safety Canada  
General Best Practices for Laptop Security  
<http://www.publicsafety.gc.ca/prg/em/ccirc/2004/in04-001-eng.aspx>

---

#### British Columbia Medical Association

---

British Columbia Medical Association Privacy Toolkit:  
<http://www.bcma.org/publications-media/privacy-toolkit>

---

#### Canadian Institute of Health Research

---

Best Practices for Protecting Privacy in Health Research September 2005, Public Works and Government Services Canada, 2005

[http://www.cihr-irsc.gc.ca/e/documents/et\\_pbp\\_nov05\\_sept2005\\_e.pdf](http://www.cihr-irsc.gc.ca/e/documents/et_pbp_nov05_sept2005_e.pdf)

---

#### International Standards Organization

---

Technical Report ISO/IEC 17799: Information Technology- Security techniques - Code of Practice for Information Security Management, Second Edition. June 15, 2005.



### RESOURCES

---

National Institute of Standards and Technology  
Computer Security Division  
Computer Security Resource Center  
Website: <http://csrc.nist.gov>

---

Federal Information Processing Standards Publication 140-2 (FIPS PUB 140-2), May 25, 2001.  
<http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

Federal Information Processing Standards Publication 200 (FIPS PUB 200), Minimum Security Requirements for Federal Information and Information Systems. March 2006.  
<http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf>

---

#### Purdue University

Mobile Device Best Practices  
<http://www.purdue.edu/securepurdue/bestPractices/mobileDevice.cfm>

---

RCMP Technical Security Branch  
Website at: <http://www.rcmp-grc.gc.ca/ts-st/pubs/index-eng.htm>

---



## RESOURCES

---

### Stanford University

---

Best Practices for Securing Mobile Computing Devices

[http://www.stanford.edu/group/security/securecomputing/mobile\\_devices.html](http://www.stanford.edu/group/security/securecomputing/mobile_devices.html)

---

### University of Western Ontario

---

Portable Data Device Security Best Practices

<http://security.uwo.ca/portable-data/Portable%20Data%20Best%20Practices.html>

---

### Individual Authors

---

Bishop, Matt, and Klein, Daniel. Improving System Security via Proactive Password Checking, 1992.

Available online: <http://www.klein.com/dvk/publications/passwd-matt-final.pdf>

Laudon, Kenneth C. and Laudon, Jane. *Management Information Systems: Managing the Digital Firm 3<sup>rd</sup> Canadian Edition*, Pearson Prentice Hall, 2007.

Menezes, A., Van Oorschot, P. and Vanstone, S.. *The Handbook of Applied Cryptography*, CRC Press, 1996.

