HELPFUL TIPS: MOBILE DEVICE SECURITY

Privacy tips for Public Bodies/Trustees using mobile devices

This document is intended to provide general advice to organizations on how to protect personal information and personal health information when using mobile devices.

January 2018

Office of the
Saskatchewan Information
and Privacy Commissioner

Helpful Tips: 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. These devices have become indispensable because they are fast, easy to use, compact and portable. However, the convenience comes with some associated risks.

When it comes to the theft of a mobile device, it is tempting to think that thieves are most interested in the physical device. However, the reality is the information on the device is far more valuable. When one considers the confidential nature of the information that could be breached it is easy to understand its value, for example:

- Personal Health Information (PHI)
- Personal Information (PI)
    - Financial information – both personal (i.e. bank account information) & corporate (i.e. customer credit card information)
    - Social Insurance Numbers
    - Work History (i.e. performance reviews)
    - Personal contact information (i.e. phone numbers, e-mail lists)
- Meeting minutes
- Unpublished research drafts
- Decryption keys and passwords

Privacy breaches can have far reaching implications because of the nature of the information compromised and the number of individuals affected by it. There have been a number of high profile privacy breaches in Canada involving public bodies in the last few years. In some cases, these breaches have impacted millions of people.

As such, public bodies/trustees should ensure they have met the duty to protect the PI or PHI on the mobile devices.

What is the Duty to Protect?

The Freedom of Information and Protection of Privacy Act (FOIP), *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP), *The Health Information Protection Act* (HIPA) and their Regulations provide the rules regarding when public body/trustee should collect, use and disclose PI/PHI. Any collections, uses or disclosures unauthorized by FOIP or LA FOIP would be a

privacy breach. Also, these statutes have an explicit duty on public bodies/trustees to protect PI/PHI (see section 24.1 of FOIP/23.1 of LA FOIP/16 of HIPA).

Section 24.1 of FOIP/23.1 of LA FOIP/16 of HIPA requires that a public body have administrative, technical and physical safeguards to protect PI/PHI.

Administrative safeguards are controls that focus on internal organization, policies, procedures and maintenance of security measures that protect PI/PHI. Examples include written policies and procedures, annual training for employees, confidentiality agreements, agreements with information management service providers (IMSPs), auditing programs, records retention and destruction schedules and access restrictions.

Technical Safeguards are the technology and the policy and procedures for its use that protect PI/PHI and control access to it. Examples include separate user identifications, passwords, firewalls, identification and authentication controls, virus scanners and audit capabilities in digital systems.

Physical Safeguards are physical measures, policies, and procedures to protect PI/PHI and related buildings and equipment, from unauthorized intrusion and natural and environmental hazards. Examples include locked filing cabinets, offices and storage rooms, alarm systems and clean desk approaches.

Subsection 24.1(a) of FOIP/23.1(a) of LA FOIP/16(a) of HIPA indicates that a public body must protect the integrity, accuracy and confidentiality of the PI/PHI in its possession or under its control;

Integrity refers to the condition of information being whole or complete; not modified, deleted or corrupted.

Confidentiality implies a trust relationship between the person supplying information and the individual or organization collecting or using it.

Subsection 24.1(b) of FOIP/23.1(b) of LA FOIP/16(b) of HIPA indicates that public bodies must protect against any reasonably anticipated:

- threat or hazard to the security or integrity of the PI/PHI in its possession or under its control;
- loss of the PI/PHI in its possession or under its control; or
- unauthorized access to or use, disclosure or modification of the PI/PHI in its possession or under its control;

Threat means a sign or cause of possible harm.

Hazard means a risk, peril or danger.

Security means a condition of safety or freedom from fear or danger.

Unauthorized access occurs when individuals have access to PI/PHI that they do not need-to-know, either by accident or on purpose. This would also qualify as either an unauthorized use or unauthorized disclosure.

A need-to-know is the principle that public bodies and their staff should only collect, use or disclose PI/PHI needed for the purposes of the mandated service. PI/PHI should only be available to those employees in an organization that have a legitimate need-to-know that information for the purpose of delivering their mandated services.

An unauthorized collection occurs when PI/PHI is collected, acquired, received or obtained by any means for purposes that are not allowed under sections 25, 26, 27, 28 or 29(2) of FOIP/24, 25, 26, 27 or 28(2) of LA FOIP/23, 24 or 25 of HIPA.

Unauthorized use refers to the use of PI/PHI for a purpose that is not authorized under sections 27, 28 or 29(2) of FOIP/26, 27 or 28(2) of LA FOIP/26, 27, 28, 29 or 30 of HIPA.

Unauthorized disclosure refers to the act of revealing, showing, providing copies, selling, giving, or relaying the content of PI/PHI in ways that are not permitted under sections, 29 or 30 of FOIP/28 or 29 of LA FOIP/27, 28, 29, 30 of HIPA.

Subsection 24.1(c) of FOIP/23.1(c) of LA FOIP/16(c) of HIPA indicates that public bodies should have education programs in place for their employees which addresses the public body's duties under FOIP/LA FOIP, safeguards the public body has established, the need-to-know and consequences for violating HIPA. The IPC has indicated that annual training is best practice. Annual training should include reminders about mobile security.

The remainder of this document will describe best practices for mobile security.

ADMINISTRATIVE SAFEGUARDS

Policies and Procedures

Organizations should have clear, written, comprehensive and enforceable policies and procedures to manage the use of mobile devices by employees. Random audits can assist with ensuring compliance with policies and procedures. Organizations should ensure that its policies and procedures are regularly reviewed and updated as necessary.

Administrative Safeguards

Develop strong, written and enforceable policies and procedures specifically for the use of mobile devices. Make sure they address the following (not a comprehensive list):

- ☐ Ensuring password-enabled screen locks are engaged
- ☐ Developing strong passwords and a schedule for changing them
- ☐ Rules around the sharing of passwords
- ☐ Step-by-step procedures for what to do if a device is lost or stolen
- ☐ A scheduled inventory of all mobile devices should be occurring
- ☐ Enable the ability to remotely wipe a device
- ☐ When using the device, de-identify PI/PHI whenever possible
- ☐ Avoid saving PI/PHI on the mobile device
- ☐ Use encryption
- ☐ How to identify and avoid unsecured networks
- ☐ Address BYOD (Bring Your Own Device) requirements
- ☐ Unauthorized users should not be allowed to use the device
- ☐ Employees should not download free applications or software
- ☐ How to properly dispose of a device when the organization no longer uses it

Educate employees about the policies and procedures:

- ☐ Ensure the policies and procedures are easy for employees to understand
- ☐ Provide regular training sessions
- ☐ Ensure the policies and procedures are accessible

Bring Your Own Device (BYOD) Programs

BYOD is an arrangement whereby an organization authorizes its employees to use personal mobile devices for both personal and business purposes. A BYOD specific policy should be developed which includes:

- User responsibilities;
- How an organization may conduct reasonable and acceptable monitoring on a BYOD device;
- Whether geo-tracking information generated by the mobile device will be tracked by an organization;
- Acceptable and unacceptable uses of BYOD devices;
- Sharing of devices with family members or friends;
- Application (app) management;
- Data/voice plan responsibility;
- Device and information security requirements; and
- Access requests.

TECHNICAL SAFEGUARDS

Strong Passwords

The use of passwords is a basic security measure that should be taken. Strong passwords are comprised of at least eight characters, with 14 or more being the ideal. They can include a combination of upper and lower case letters, numbers and symbols, rather than dictionary words. Avoid using predictable passwords like birthdates, favorite sports teams or easy-to-guess dictionary words like “password” or “Letmein”. However, password phrases can be very good for example, “IwenttoballetinReginaon7thAve.”

Passwords should be changed frequently. As a result of the need for complex and frequently changed passwords, employees will often write down the passwords near or on their devices. Avoid writing passwords down and putting them in places that can be easily found. Passwords should not be shared amongst employees.

In summary, here are some good practices for the use of passwords:

- Keep passwords confidential;
- Avoid writing down passwords;
- Use different passwords for unlocking the device and unlocking encrypted files;
- Use different passwords for different purposes (avoid using the same password for everything);
- Change passwords frequently;
- Consider using password phrases;
- Change assigned temporary passwords; and
- Do not reuse passwords.

Authentication

Authentication is the process of determining whether someone is who they declare to be. Multiple layer authentications are best with the user being required to provide at least two of the following:

- something they know (password matched with a username);
- something they have (such as a security token (e.g. a fob or swipe card). This is a physical device that an authorized user is given to ease authentication.);
- something they are (biometrics (fingerprints, iris scans).

Encryption

Encryption is a mathematical process that helps to disguise stored or transmitted data. It codifies ordinary data into what appears to be an unintelligible stream of random symbols. A "key" is required to decipher the data.

The effectiveness of the encryption depends on both the encryption software and the strength of the "key" used. Encryption standards are always evolving. Contact your IT Department for your organization's encryption practices.

System Integrity

It is important to maintain system integrity and to avoid things that compromise it. Here are some things to consider:

- Make sure your device has anti-virus, malware and spyware software installed and enabled;
- Periodically run full system scans;
- Keep software up-to-date;
- Turn automatic updates 'on';
- Never download free software or applications from the internet without a high level of assurances that the product is safe;
- Consider using a firewall.

Wireless Security

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. Here are some things to consider:

- Use encryption;
- Sufficiently de-identify the information;

- When using a laptop in a public place take steps to prevent others from seeing what you are working on;
- Set your device so any wireless connection is off by default. Turn it on when needed;
- For confidential work, only use secure connections;

Data Wiping

Consider configuring your device to it can be 'wiped' remotely. Wiping occurs when the data on the device is deleted. This can be useful if the device is lost or stolen.

Technical Safeguards
☐ **Use strong passwords**
☐ **Use multi-layer authentication**
☐ **Use encryption**
☐ **Protect the system's integrity**
☐ **Only connect to secure wireless networks**

PHYSICAL SAFEGUARDS

The following safeguards offer relatively inexpensive ways to ensure physical security of mobile devices:

- Do not leave mobile devices in vehicles. If it is necessary, lock the device in the trunk.
- Never leave the device unattended in a public place.
- Lock mobile devices away when not in use.

Mobile Device Loss

If your device is lost or stolen, report it immediately to your supervisor, your organization's Privacy Officer and the police, if appropriate. Your organization will need to evaluate the incident and take any necessary steps to mitigate risks that may arise.

You may wish to consult our resources, *Privacy Breach Guidelines for Government Institutions and Local Authorities* or Privacy Breach Guidelines for Trustees.

Proper Disposal

Thousands of surplus devices that once housed sensitive data are being stored, recycled or donated. Proper management of surplus devices is important to protect the PI/PHI that may still be on the device.

Here are some things to consider:

- Mobile devices should be properly secured until they are wiped clean of all data; and
- Prior to recycling, refurbishing or donation, wipe all data from the device including the hard drive.

Physical Safeguards
☐ **Do not leave your mobile device unattended**
☐ **Securely store mobile devices when not in use**
☐ **Report lost or stolen devices to your Privacy Officer and if appropriate, the police**
☐ **Safely dispose of mobile devices when no longer needed**

CONTACT INFORMATION

If you have any questions or concerns regarding mobile device security, please contact us:

306-787-8350 | toll free 1-877-748-2298

503 – 1801 Hamilton Street | Regina SK S4P 4B4

webmaster@oipc.sk.ca | www.oipc.sk.ca | @SaskIPC