Safeguarding Privacy on Mobile Devices

www.ipc.on.ca

Table of Contents

Introduction	1
Tips for Safeguarding Mobile Devices	3
Checklist	4
Further Resources	8

Introduction

The ability to seamlessly and continuously move and use information has become an important part our daily lives. Just a few years ago, the most practical ways to transport large amounts of electronic information were through storage and access on laptops or USB keys. Today, the market is literally inundated with devices and services (such as cloud storage) that are capable of storing and transmitting large amounts of personally identifiable information (PII). The technological innovations continue to rapidly evolve and breaches of PII are becoming more common. It has never been more important for organizations and their employees to be *proactive, not reactive,* in protecting PII that is stored and accessed on mobile devices.

PII refers to any information which may be used to identify an individual. In Ontario, we continue to hear stories of breaches of PII on lost or stolen mobile devices due to inadequate protection. Mobile devices include laptops, mobile phones, smartphones, tablets, USB flash drives, memory cards, and even wearable devices that can take photos or record and transmit biological information (such as blood glucose level or heart rate).

DID YOU KNOW?

Login passwords are not enough to secure PII on your mobile device, no matter how strong they are. When a mobile device containing PII is lost or stolen, access to PII must have been both password-protected and **encrypted** to not be considered a breach of PII.

The very nature of mobile devices that makes them so attractive to access and store PII, *their portability*, makes them especially vulnerable to loss and theft. But breaches of PII are not inevitable. They can be avoided by proactively implementing safeguards.

A breach costs everyone. It costs the organization time, money, and reputation and it costs the individuals (often thousands of individuals per

breach) possible identity theft, fraud, discrimination, and loss of trust in the organization and its employees to whom they depended upon to protect their privacy.

When PII is stored or accessed on a mobile device while away from an organization's secure network, both the organization and employee are responsible for protecting the information. Organizations are responsible for the privacy and security of the PII they are entrusted with throughout the lifecycle of that information (starting from collection, through to the use, sharing, and finally the removal or destruction of PII) and should have strong information privacy and security policies and practices in place that are shared with and understood by their employees.

There is a rapidly growing trend toward "Bring-Your-Own-Device" (BYOD) whereby personally owned mobile devices (especially smartphones and tablets) are used for work purposes. Whether or not the device is corporately or personally owned, both the organization and its employees are responsible for protecting the PII stored and accessed on the device.

DID YOU KNOW?

It does not matter whether a device is corporately owned or personally owned. Organizations and their employees are both responsible for protecting the PII they are entrusted with in the course of their work.

Employees are responsible for complying with their organization's information privacy and security policies and should avoid the use of "workarounds." Workarounds enable access, sharing, and storing of PII outside an organization's IT network, which exposes PII to vulnerability. An example includes sending PII while at work to a personal email address and later accessing the PII outside the organization's secure network. While using a workaround may seem efficient, it compromises the privacy and security of PII. Organizations and employees should work together to improve information flow to avoid workarounds.

It is important to preserve the highest level of security possible on mobile devices used to access PII. "Jailbreaking" and "Rooting" (terms used to describe the process of bypassing restrictions on certain smartphones) may be attractive to those who seek to personalize their device or use otherwise prohibited apps and functions, but they expose your device to a much greater risk of malware and data leakage. Those

who choose to jailbreak or root a device should not use it to access or store PII for work purposes.

Tips for Safeguarding Mobile Devices

Before using your mobile device to store PII, consider alternatives. Is it possible to access the PII you need on a server via a protected remote connection (e.g. a virtual private network)?

Before you remove PII from the workplace, ensure you have authorization to do so and that you are complying with your organization's information security and privacy policies. Only take records of PII with you that you need to do the work and use de-identified data instead of PII whenever possible.

Make sure that access to PII on your mobile device is protected by strong login passwords and encryption. Many of the breaches that have occurred in Ontario involved mobile devices that were only safeguarded with a login password. Passwords alone do not protect organizations or employees from the legal responsibilities related to a breach, such as notification of individuals when their PII has been lost, stolen, or accessed by unauthorized individuals.

Strong passwords are unique. They should not be shared with other devices, programs, or services (e.g. email, social media, or other

DID YOU KNOW?

USB keys and other portable storage media can be protected in the following ways:

- Consider alternatives. Only store the PII you need for the job. Use de-identified data instead of PII whenever possible.
- Ensure PII is strongly encrypted whenever stored on portable storage devices and use strong passwords to access encrypted PII.
- Keep the device safe from theft and loss and always know what PII is on the device.
- Report lost or stolen devices containing PII to your employer as soon as possible.
- Securely remove PII from your device as soon as you are done with it.

SAFEGUARDING PRIVACY ON MOBILE DEVICES

You can protect the personally identifiable information (PII) you store or access on mobile devices for work purposes in the following ways:

- ☐ **Consider Secure Alternatives**

  Is there a secure alternative available that would allow you to complete the work without storing PII on your mobile device (e.g. remote access)?

- ☐ **Confirm Authorization to Store or Access PII Using a Mobile Device**

  Are you authorized to store or access PII on your mobile device?

- ☐ **Minimize or De-identify PII Whenever Possible**

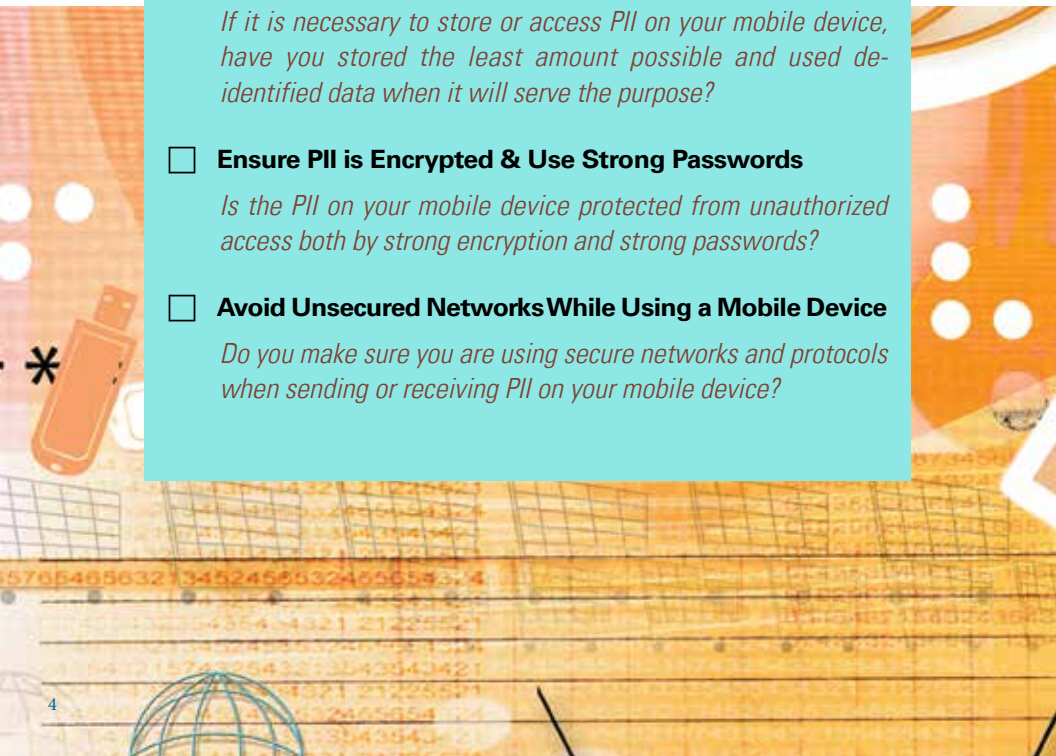
  If it is necessary to store or access PII on your mobile device, have you stored the least amount possible and used de-identified data when it will serve the purpose?

- ☐ **Ensure PII is Encrypted & Use Strong Passwords**

  Is the PII on your mobile device protected from unauthorized access both by strong encryption and strong passwords?

- ☐ **Avoid Unsecured Networks While Using a Mobile Device**

  Do you make sure you are using secure networks and protocols when sending or receiving PII on your mobile device?



☐ **For Mobile Computing Devices: Use Protective Software & Configure Your Device Settings**

For laptops, smartphones, tablets, and other mobile computing devices, have you installed and are you using up-to-date firewalls, anti-virus, and anti-theft software? Have the settings on your device been configured to protect PII from unauthorized access?

☐ **Be Aware of the Physical Security of the Mobile Device**

Do you make sure your mobile device is transported and used in a secure manner to prevent loss, theft and "shoulder-surfing" or eavesdropping?

☐ **Know the PII on your Mobile Device**

If your mobile device were to be lost or stolen, could you identify all the PII stored on it?

☐ **Report Immediately the Lost or Stolen Mobile Device**

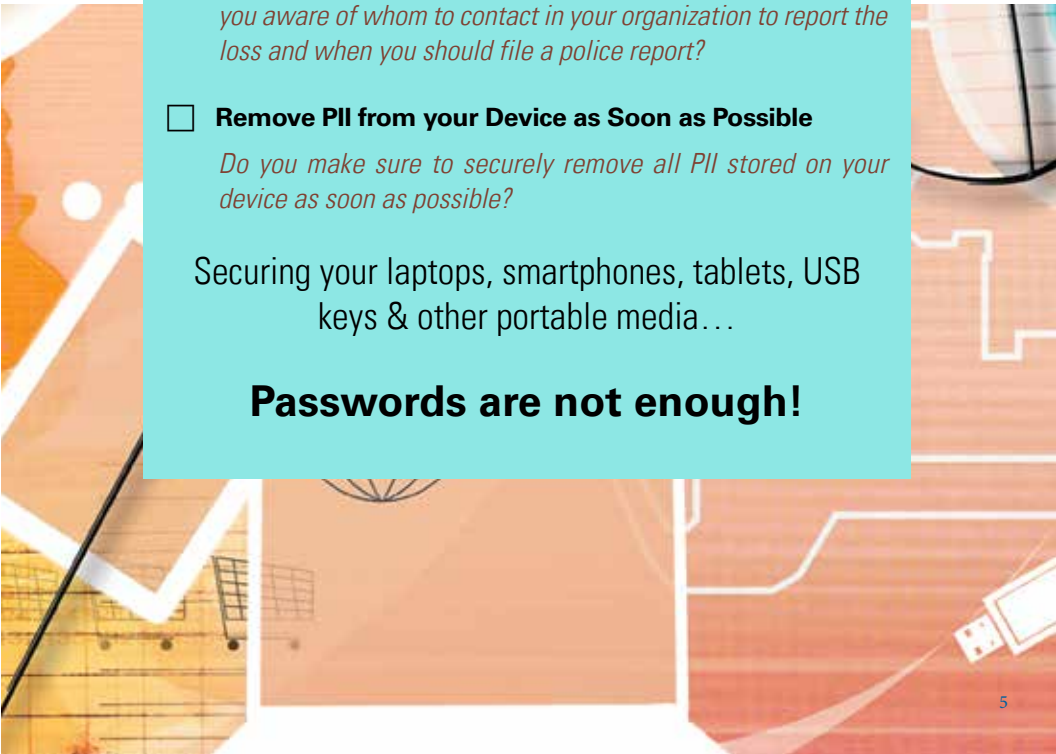
If you were to experience loss or theft of your mobile device, are you aware of whom to contact in your organization to report the loss and when you should file a police report?

☐ **Remove PII from your Device as Soon as Possible**

Do you make sure to securely remove all PII stored on your device as soon as possible?

Securing your laptops, smartphones, tablets, USB keys & other portable media…

Passwords are not enough!



accounts). A password used to protect a device should not be the same password used to access files of PII within the device. A strong password consists of at least eight characters (fourteen or more is ideal) and should be a combination of upper and lower case letters, numbers, and symbols (such as $, #, or !). Avoid any single words that can be found in the dictionary of any language (whether spelled backwards or forwards).

Ensure mobile computing devices are installed with protective software. Laptops, smartphones, and tablets should use a personal firewall, anti-virus, anti-spyware, and anti-theft programs that are up-to-date with the latest security patches. If you lose your mobile device, there are often programs and services available for locating and remote-wiping the device, which means you or your organization's IT department would be able to remove the PII on your mobile device before anyone else is able to access it.

DID YOU KNOW?

Laptops, smartphones, tablets and other mobile computing devices should include additional safeguards for the protection of PII:

- These types of mobile devices should have up-to-date firewalls, anti-virus, and anti-theft software installed.
- You should configure the settings on these types of devices to provide the highest level of security (e.g. automatic lock).
- Avoid unsecure networks when connecting to the Internet.

Mobile computing devices can also be configured to improve the privacy and security of the information they contain. For example, enabling the automatic lock feature will require a password to access the device at a pre-determined time interval. You may also be able to configure the settings of the device so that a certain number of failed attempts to access the device will result in automatic deletion of the information it contains. These configurations may already be part of your organization's information privacy and security policies.

Do not leave mobile devices containing PII unattended in public places (such as conferences or coffee shops) and avoid accessing PII in the open, where people looking over your shoulder could easily view it. Consider using a protective case with a physical lock to transport your mobile device and leave your contact information attached to the device so that if it is lost, it may be possible for someone to return it to you.

Be mindful of the networks you use to connect your mobile computing device to the Internet when outside your organization's secure network. Avoid connecting to unsecured Wi-Fi networks (also known as "hotspots"). Doing so may result in the information you send and receive being transmitted in plain text, which makes it susceptible to eavesdropping. If you must use an unsecured Wi-Fi network, be sure to limit your activity involving PII to websites that offer encrypted connections for the duration of your session (look for ***https*** instead of *http* at the start of the URL in the address bar of your browser).

Bluetooth technology allows two devices to share information wirelessly over short distances (similar to Wi-Fi, but only on paired devices). Connect via Bluetooth to devices that support data encryption (as of Bluetooth v2.1, encryption is enabled by default) whenever possible. Putting a mobile device in "discover" mode to pair with another device may compromise PII so you should turn the device back to "non-discoverable" when you're finished setting up the Bluetooth connection.

You should always be prepared in the case of a breach by knowing the PII that you have on your mobile device. If and when a breach happens, contact your organization right away. Knowing the PII and who it pertains to will help you when notifying affected individuals. If the device is unencrypted and you are unable to remotely wipe the PII, consider filing a police report.

Any PII that is kept on a mobile device should be stored there only as long as necessary to serve its intended purpose. When you are finished with the PII, make sure you securely remove it with a digital wipe utility program, or check with your IT department for their assistance.

Lastly, knowing your responsibilities to protect PII can go a long way toward protecting everyone's privacy. Be aware of when you might be handling PII and be proactive in protecting it.

Further Resources:

The IPC has the following additional materials available in print or for download on our website at www.ipc.on.ca:

Encrypting Personal Health Information on Mobile Devices (Fact Sheet), May 2007

Health-Care Requirement for Strong Encryption (Fact Sheet), July 2010

Privacy Breach Protocol: Guidelines for Government Organizations (paper), March 2012

Safeguarding Personal Health Information When Using Mobile Devices for Research Purposes, Sep 2011

What to do When Faced with a Privacy Breach: Guidelines for the Health Sector (paper), June 2006

Order HO-004 (Health Order addressing stolen laptop containing personal health information), Mar 2007

Order HO-007 (Health Order addressing need for encryption on mobile devices), Jan 2010

Order HO-008 (Health Order addressing unencrypted stolen laptop containing personal health information), Jun 2010

Secure Destruction of Personal Information (fact sheet), Dec 2005

Elections Ontario's Unprecedented Privacy Breach: A Special Investigation Report, Jul 2012

About the IPC

The role of the Information and Privacy Commissioner is set out in three statutes: the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act*. The Commissioner is appointed by the Legislative Assembly of Ontario and is independent of the government of the day.

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

For more information:
Information and Privacy Commissioner
Ontario, Canada
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8 CANADA

Tel: 416-326-3333 or 1-800-387-0073
Fax: 416-325-9195 TTY: 416-325-7539
info@ipc.on.ca www.ipc.on.ca

MIX
Paper from responsible sources
FSC® C017307
www.fsc.org

Cette publication est également disponible en français

Revised May 2014