

SAFEGUARDING PRIVACY IN A MOBILE WORKPLACE

Checklist for taking personally identifiable information (PII) out of the workplace:

- Does your organization's policy permit the removal of PII from the office?
- Is it necessary for you to remove PII from the office?
- Has your supervisor specifically authorized you to remove the PII in question for the office?
- Have you considered less risky alternatives, such as remote access to PII stored on a central server?
- If you must remove PII from the office, have you kept the number of records, and the number of fields within those records, to the minimum necessary?
- If possible, have you de-identified the PII to render it anonymous?
- If it is not possible to de-identify the PII, have you encrypted it?
- Have you protected your mobile storage device and/or any files containing PII, with strong passwords?
- If your mobile device is lost or stolen, will you be able to identify all the PII stored on it?

**Protect the information
you keep on your laptops,
cellphones and PDAs**

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner of Ontario





Being able to do work offsite

offers many benefits – to both employees and employers. But there is a downside. The personally identifiable information contained on your laptop, USB, PDA or cellphone can disappear just as easily as the device on which it is stored.

Personally identifiable information (PII) consists of any information which may be used to identify an individual. When you walk out the door with PII on your electronic devices, you leave the protective shelter of any IT security infrastructure provided by your employer that may have been established and designed to operate without any effort or awareness on your part. When you take information out of that context, you enter into a different world where what you don't know CAN hurt you – your reputation, your finances – and possibly that of thousands of others.

Thousands of mobile devices go missing every year in North America alone. Laptops and PDAs get left behind, USB keys get misplaced, and cellphones fall out of pockets. Identity thieves are abounding and they're looking for opportunities to grab PII or business data that you may be carrying. They might be operating remote cameras or skimming devices or standing right next to you in an airport line-up or a hotel lobby. Even if they 'only' want to steal your hardware and not the PII, unless you take appropriate precautions, you will need to respond as if that information has been compromised. **YOU** need to reduce the risk of becoming a target by taking steps to protect personal information, whether it's your own



information, that of your employer, or, most importantly, that of your customers or clients.

This brochure is intended to help people taking their work “on the road,” whether it be in the private sector, public sector, or most important, the health care sector. It provides best practices for securing mobile devices and protecting the even more valuable information that you or other employees may carry out the door on such devices. It will be up to you to determine what measures to put into place, based on the sensitivity of the information involved. The first principle of privacy is accountability, and when you take PII with you, or collect new information, you are personally responsible for ensuring that privacy is protected.

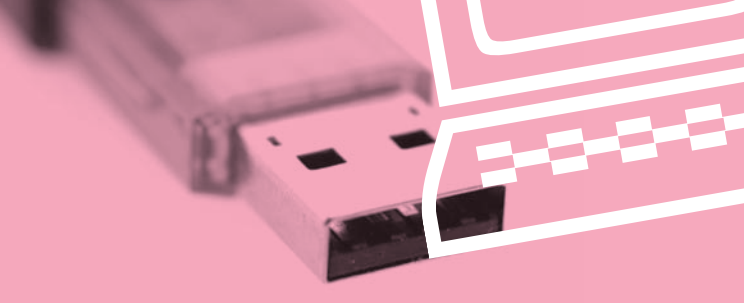
BEFORE YOU WALK OUT OF THE WORKPLACE

- 1** Consider alternatives to storing PII on your mobile device. Is it possible to access the PII you need on a server via a protected remote connection, such as a secure website or a Virtual Private Network (VPN)?
- 2** Remove as few records containing PII as possible. Instead of accessing the entire database, take only the subset of records that you need to work with, for example records for clients you will be visiting.
- 3** Consider multiple ways to protect the PII. If you are moving data to a portable device, such as a USB key or laptop, can sensitive fields (such as health card numbers, social insurance numbers or bank account numbers) be removed altogether? Can the data be made anonymous?

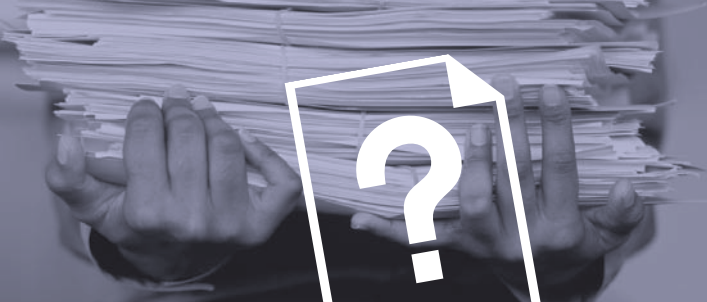


- 4** If you must have PII on your mobile device, then encrypt the data and password-protect the device. On its own, password protection is not sufficient. Strong encryption and layered security measures are a must. (Refer to the IPC's fact sheet, *Encrypting Personal Health Information on Mobile Devices*.) Follow your organization's encryption policies or, if you are a sole practitioner, use an up-to-date encryption technique. There are a number of security services and products available, including laptops with pre-installed full disk-encryption software. In order to prevent data falling into the wrong hands, this technology forces users to authenticate themselves to the software before the operating system boots up.
- 5** Protect all your devices with passwords: power-on passwords, screensaver passwords, account 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**.



- 6** Protect your passwords and encryption keys by:
 - not writing them down or storing them on the device;
 - reviewing other options, such as the innovative programs for some PDAs (signature-based, or tapping a certain point on a picture), as alternatives to having to retype your password;
 - not using the same password to log into your computer and to unlock your encrypted files.
- 7** Enable the automatic lock feature of your device after five minutes or less of idle time.
- 8** When using mobile devices featuring Bluetooth technology, you will be more secure if you:
 - set your device so Bluetooth is “off” by default. Turn it on only as necessary;
 - keep devices set to “non-discoverable;”
 - use as many characters as possible for your Bluetooth PIN;
 - configure these settings in a private location.
- 9** If you handle PII or other confidential information online or perform financial transactions, then your laptop and your PDA should, at a *minimum*, have personal firewall, anti-virus and anti-spyware programs that are up-to-date with the latest security patches.
- 10** Use a lockable briefcase or laptop case that does not bear any visible logos of your organization. Place an “if found, return by calling [phone number]” card inside your briefcase, with no other identifying information.



WHILE YOU ARE OUT

- 1** Only conduct confidential work on mobile devices over which you have control. Do not use public computers or networks – or work on confidential material in public places. And do not perform this type of work on computers that are shared with family members.
- 2** Even when doing non-confidential work on public wireless networks, Wi-Fi or “Hot Spots” in airports, hotels, coffee shops, public libraries, etc., consider the following points:
 - These networks are inherently open and unsafe. Data transmitted by your device across the open airwaves can easily be picked up and read by another device;
 - Watch out for shoulder surfing;
 - Never connect to two separate networks (such as Wi-Fi and Bluetooth) simultaneously, which turns your computer into a bridge or access point.
- 3** Do not carry out confidential work unless you use an encrypted link (such as a Virtual Private Network – VPN) to the host network. Otherwise, any information sent or received travels in plain view, accessible to anyone. This premise applies to web browsing, e-mail and Instant Messaging.
 - Set your device so the Wi-Fi access is “off” by default. Turn it on only as necessary.
 - If in doubt, DON'T turn on the Wi-Fi access.
- 4** Do not leave devices containing PII or other confidential information in your vehicle. (If it absolutely cannot be avoided, lock them in the trunk **before** you start the



trip, not in the parking lot of your destination or a stopover. If the vehicle has no trunk, leaving the device in the vehicle is **not** a secure option.)

- 5 When carrying portable devices, make it a point to go through a quick checklist of your belongings when you leave: a cab, hotel room, meeting place, airplane, or restaurant.
- 6 Secure your mobile devices at all times. Use a cable lock with an audible alarm when not working on them, or lock them away when not in use.
- 7 If – despite all your precautions – you lose your device or it is stolen, report the loss immediately to the police and your organization. If you are not sure that the PII was adequately protected, you may be required to notify individuals potentially put at risk. You will need to evaluate the incident and take the necessary steps to mitigate risks that may arise. Among the resources you can turn to is the IPC’s *Breach Notification Assessment Tool*, listed at the end of this publication. (Note: Some types of handheld devices are more secure than others. For example, if a BlackBerry were set up correctly, the contents could be erased by a network administrator in the event that it is lost or stolen. Some devices can be set to erase themselves after several failed password entries.)

WHEN YOU HAVE COMPLETED YOUR WORK

If possible, remove PII from your mobile device(s) as soon as practical, but understand that deleting data files from the screen of a mobile device won’t necessarily delete the data completely.

FURTHER RESOURCES

The IPC has additional materials available in print or for download from our website, www.ipc.on.ca:

- *Identity Theft: How to Protect Yourself* (brochure);
- *Identity Theft: Business Take Note: Steps to Protect Customer Information* (brochure);
- *Breach Notification Assessment Tool* (paper);
- *What to do if a privacy breach occurs: Guidelines for government organizations* (paper);
- *What to do When Faced With a Privacy Breach: Guidelines for the Health Sector* (paper);
- *Order HO-004* (Health Order addressing stolen laptop containing personal health information);
- *Order HO-005* (Health Order addressing wireless video of a patient);
- *Encrypting Personal Health Information on Mobile Devices* (fact sheet);
- *Secure Destruction of Personal Information* (fact sheet).
- *Wireless Communication Technologies: Video Surveillance Systems* (fact sheet).

INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, CONTACT INFORMATION

General inquiries should be directed to:

Tel: (416) 326-3333

1-800-387-0073

Fax: (416) 325-9195

TTY (Teletypewriter): (416) 325-7539

e-mail: info@ipc.on.ca

Website: www.ipc.on.ca

2 Bloor Street East

Suite 1400

Toronto, Ontario

M4W 1A8

