Protecting Personal Health Information on Mobile and Portable Devices

STOP. THINK. PROTECT.

Patient privacy is in your hands. www.ipc.on.ca

Guidance from the Information and Privacy Commissioner of Ontario

Why is the Protection of Personal Health Information (PHI) So Critical?

- Extreme sensitivity of personal health information;

- Greater number of persons involved in the delivery of health care to an individual;

- Increased portability of personal health information;

- Emphasis on information technology and electronic exchanges of personal health information;

- Need to use or disclose health information for secondary purposes seen to be in the public interest (i.e. research).

Personal Health Information Protection Act

- The *Personal Health Information Protection Act* ("the *Act*") came into effect on November 1, 2004;

- The *Act* governs the collection, use and disclosure of "personal health information" by "health information custodians" and their "agents."

Definition of Personal Health Information

PHI is defined as ***identifying*** information that:

- Relates to an individual's physical or mental health;

- Relates to the provision of health care to the individual;

- Identifies an individual's health care provider;

- Identifies an individual's substitute decision-maker;

- Relates to payments or eligibility for health care;

- Is the individual's health number;

- Relates to the donation of body parts or bodily substances;

- Is a plan of service under *Long-Term Care Act, 1994.*

Health Information Custodians

Health Information Custodians *include*:

- Health care practitioners who provide health care and persons that operate group practices of such health care practitioners;
- Community care access corporations;
- Hospitals, psychiatric facilities, independent health facilities;
- Long-term care homes, care homes, homes for special care;
- Pharmacies, laboratories, specimen collection centres;
- Centres, programs or services for community health or mental health whose primary purpose is the provision of health care;
- Ambulance services;
- Medical officers of health;
- Ontario Agency for Health Protection and Promotion;
- Minister/Ministry of Health and Long-Term Care;
- Minister/Ministry of Health Promotion.

Agents

- An agent is a person that acts for, or on behalf of and with authorization of, the health information custodian in respect of personal health information;

- It is irrelevant whether or not the agent:

  - is employed by the health information custodian;

  - is remunerated by the health information custodian;

  - has the authority to bind the health information custodian;

- A health information custodian remains responsible for personal health information collected, used, disclosed, retained or disposed of by an agent.

Provisions Related to the Security of Personal Health Information

- The *Act* requires health information custodians to maintain the security of personal health information;

- This includes the requirement to:
  - Take steps that are reasonable in the circumstances to protect personal health information from theft, loss and unauthorized use or disclosure and records of personal health information from unauthorized copying, modification or disposal (section 12(1));
  - Ensure records of personal health information are retained, transferred and disposed of in a secure manner (section 13);
  - Notify individuals at the first reasonable opportunity if personal health information is stolen, lost or accessed by unauthorized persons (section 12(2)).

Provisions Related to Data Minimization

- The *Act* also provides that a health information custodian must ***not*** collect, use or disclose:

  - Personal health information if other information will serve the purpose of the collection, use or disclosure (section 30(1));

  - More personal health information than is reasonably necessary to meet the purpose of the collection, use or disclosure, as the case may be (section 30(2)).

Application of the Provisions to PHI on Mobile and Portable Devices

- The IPC has issued three orders interpreting these provisions in the context of mobile devices:

  - **Order HO-004 –** Theft of a laptop containing the unencrypted personal health information of 2,900 individuals;

  - **Order HO-007 –** Loss of a USB memory stick containing the unencrypted personal health information of 83,524 individuals;

  - **Order HO-008 –** Theft of a laptop containing the unencrypted personal health information of 20,000 individuals.

Application of the Provisions to PHI on Mobile and Portable Devices

- The IPC has also issued numerous guidelines and best practices in this regard, such as:

  - *Encrypting Personal Health Information on Mobile Devices;*

  - *Health-Care Requirement for Strong Encryption;*

  - *Wireless Communication Technologies: Safeguarding Privacy and Security;*

  - *Safeguarding Privacy In a Mobile Workplace;*

  - *Innovative Wireless Home Care Services: Protecting Privacy and Personal Health Information.*

Available at **www.ipc.on.ca**

How to Protect
Personal Health Information
on Mobile or Portable Devices

STOP.

Ask yourself:

Do I really need to store any personal health information on this device?

THINK.

- Consider the alternatives;

- Would de-identified or encoded information serve the same purpose?

- Could you access the information remotely through a secure connection or virtual private network (VPN) instead?

PROTECT.

*If you must store personal health information
on mobile or portable devices:*

- Make sure it is strongly encrypted and
protected with strong passwords;

- Store the least amount of information
for the shortest amount of time;

- Develop policy and procedures for secure
retention on mobile or portable devices;

- Provide training for agents and audit compliance on the policies
and procedures
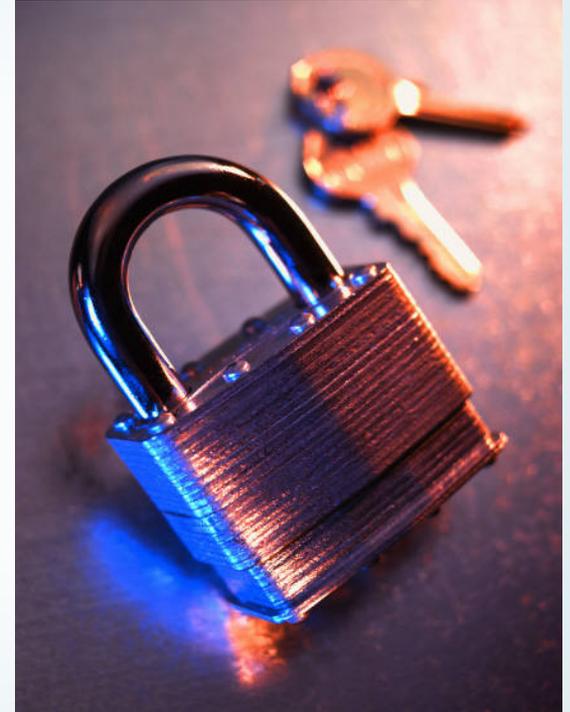
What is Encryption?

- It means to encode information to render it meaningless through an array of letters, numbers and symbols;

- It is accomplished through the use of a computer algorithm and encryption keys.

ENCRYPTION

?b64L+7N6IX2$bhSq*
&*Sg$%*#@)':{Q

What is Strong Encryption?

- Does not refer to a particular technical or design specification or a specific encryption feature;

- Refers to the high degree of confidence that plaintext personal health information will not be disclosed to unauthorized persons;

- Strong encryption includes ensuring that:
  - An up-to-date encryption algorithm that is consistent with industry standards and practices is used;
  - Encryption is thoroughly integrated into operations and is supported by security policies, procedures and practices;
  - Encryption is operational by default.

What is Strong Encryption?

- Strong encryption also includes ensuring that:
    - The encryption solution has been successfully deployed;
    - The encryption solution continues to function appropriately;
    - Error messages indicating a malfunction of the encryption solution are monitored and responded to immediately;
    - Encryption keys of a sufficient length are used;
    - Safeguards are implemented to protect encryption keys from theft, loss and access by unauthorized persons;
    - The encryption solution is subject to ongoing security reviews and updates.

What Are Strong Passwords?

- Strong passwords consist of at least eight characters;

- Strong passwords combine letters, numbers and symbols in what appear to be a random string;

- Strong password protection includes the development and implementation of policies and procedures:
  - Identifying the minimum and maximum password length;
  - Outlining the standard for password composition;
  - Providing for automatic expiry after a defined period;
  - Requiring that the device be locked after a defined number of failed log-in attempts;
  - Imposing a mandatory system-wide password-protected screen saver after a pre-defined period of inactivity;
  - Requiring agents to keep passwords private (i.e. not writing down or sharing passwords).

Fact Sheet #12

Encrypting Personal Health Information on Mobile Devices

- Why are login passwords not enough?

- What is encryption?

- What are the options?

  - Whole disk (drive) encryption;

  - Virtual disk encryption;

  - Folder or Directory encryption;

  - Device encryption;

  - Enterprise encryption.

www.ipc.on.ca/images/Resources/up-fact_12e.pdf

Fact Sheet # 16
Health-Care Requirement for Strong Encryption

- Secure Implementation;

- Secure Encryption Keys;

- Secure Authentication of Users;

- No Unintended Creation of Unencrypted Data;

- Identified, Authorized and Trained Users;

- Encryption by Default;

- Availability and Life Cycle Protection;

- Threat and Risk Assessment.

Ann Cavoukian, Ph.D., Information & Privacy Commissioner of Ontario, Canada
Ross Fraser, CISSP, ISSAP, Information Security Consultant

Fact Sheet

Number 16
July 2010

Health-Care Requirement for Strong Encryption

The Office of the Information and Privacy Commissioner (IPC), in Order HO-004, and most recently in Order HO-007, required that health information be safeguarded at all times, specifically by ensuring that any personal health information stored on any mobile devices (e.g., laptops, memory sticks, PDAs) be strongly encrypted.[1] The Order did not otherwise define what constitutes "strong encryption" in the context of protecting the confidentiality, integrity, and availability of personal health information.

Accordingly, this paper provides a working definition of strong encryption and discusses the minimum functional and technical requirements of what may be considered to be strong encryption in a health-care environment. These, in turn, will provide procurement criteria that, if met, will ensure that personal health information stored on encrypted mobile devices or storage media will remain accessible to authorized users, but no one else.

Special thanks go to Dr. Robert Kyle, Durham Region Commissioner and Medical Officer of Health, for supporting the production of this paper.
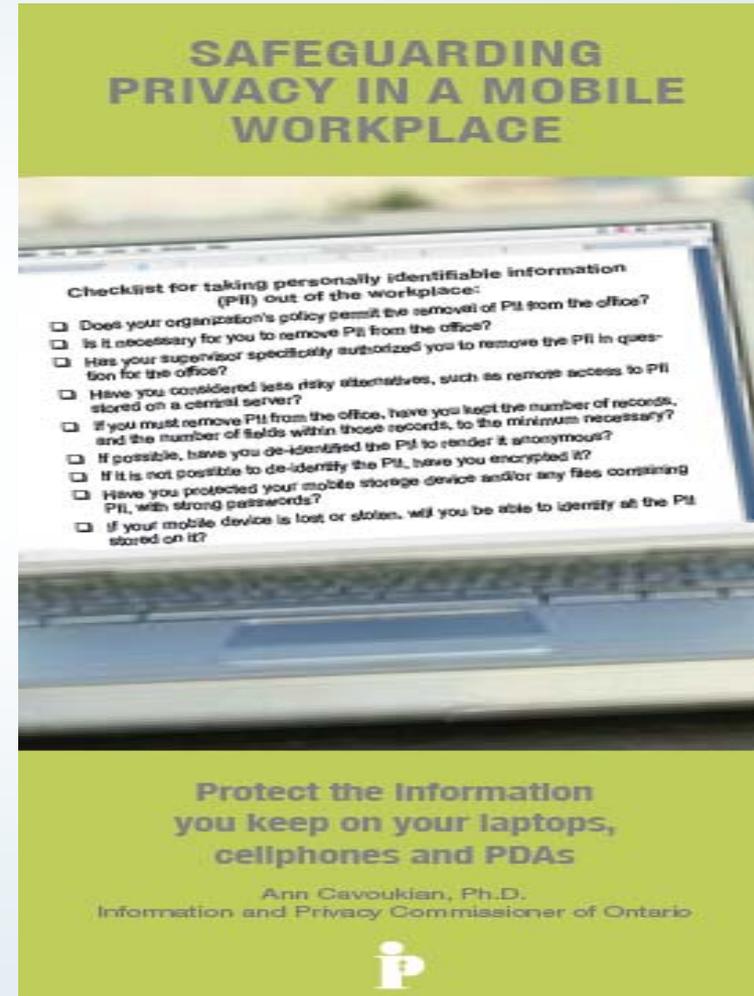
Strong Encryption

Introduction

The term 'strong encryption' does not refer to a particular technical or design specification, or even to a specific encryption feature that could be inserted into a procurement or audit specification. No particular encryption technology — no matter how 'strong' it may be — can ever, by itself, ensure that information remains secure. Instead, a variety of circumstances and factors need to be taken into account to ensure that personal information is protected against access by unauthorized parties.

To begin with, a good encryption algorithm must be used — one that has been subjected to rigorous peer review. Next, the algorithm must be properly implemented. This may only be confirmed if the encryption system is tested by an independent security testing lab. Once the encryption system is deployed, the encryption keys must be protected and managed effectively. Users who are authorized to decrypt data must be securely authenticated by means of passwords, biometrics, or security tokens. Systems must not leave unencrypted copies of data in web browser caches or on laptop

www.ipc.on.ca/images/Resources/fact-16-e.pdf

Brochure on Mobile Devices
Safeguarding Privacy In A Mobile Workplace

- Does your organization's policy permit the removal of personally-identifiable information (PII) from the office?
- Is it necessary 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 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?
- If your mobile device is lost or stolen, will you be able to identify the PII stored on it?

SAFEGUARDING PRIVACY IN A MOBILE WORKPLACE

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

Protect the Information you keep on your laptops, cellphones and PDAs

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

www.ipc.on.ca/images/Resources/up-mobilewkplace.pdf

How to Contact Us

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner, Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario, Canada
M4W 1A8

Phone: (416) 326-3948 / 1-800-387-0073
Web: www.ipc.on.ca
E-mail: info@ipc.on.ca