

CORPORATE ACCESS & PRIVACY OFFICE PROTOCOL PROTECTION OF PERSONAL HEALTH INFORMATION ON MOBILE COMPUTING DEVICES

Introduction

Health information custodians are required under the *Personal Health Information Protection Act, 2004 (PHIPA)* to take steps that are reasonable in the circumstances to ensure that personal health information is protected against theft, loss and unauthorized use or disclosure.

The Information and Privacy Commissioner has ordered (Order HO-004, March 2007) that it is not reasonable to store personal health information on mobile computing devices, unless steps are taken to ensure that any personal health information stored on such devices is protected against unauthorized access, in the event that the device is lost or stolen.

There is no excuse for unauthorized access to personal health information due to the theft or loss of a mobile computing device – any personal health information contained on such a device must be encrypted.

Definitions

"personal health information" means identifying information about an individual in oral or recorded form, if the information,

- (a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,
- (b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,
- (c) is a plan of service within the meaning of the *Long-Term Care Act, 1994* for the individual,
- (d) relates to payments or eligibility for health care in respect of the individual,
- (e) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance,
- (f) is the individual's health number, or
- (g) identifies an individual's substitute decision-maker.

"identifying information" means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual.

"mobile computing devices" means portable computing devices that allow you to store, organize, access and transmit information. Mobile computing devices include, but are not limited to: notebooks, laptops, PDAs, tablet computers, USB drives, and handheld computers.

Health information custodians at the City are:

- Toronto Public Health
- Emergency Medical Services
- Homes for the Aged
- Seaton House, Robertson House, Women's Residence
- Employee Health

Acceptable Measures to Protect Personal Health Information

Limiting Storage of Personal Health Information on Mobile Computing Devices

- Avoid storing identifiable personal health information on mobile computing devices.
- USB drives must never be used to store personal health information.
- Where personal health information must be stored on a mobile device, such as a laptop, only the minimal amount of information necessary should be stored, and for the minimal amount of time necessary to complete the work.
- Personal health information should be de-identified or coded, in a manner such that the identities of the individuals whose personal health information is stored on the device could not be readily ascertained if the information were accessed by unauthorized persons.
- If the information is coded, the code that is needed to unlock the identities of individuals should be stored separately on a more secure computing device, such as a central server.

Password Protection

- Because passwords may be guessed, written down, stolen, shared, hacked or cracked with software that is readily available, they are often the weakest link in the security chain.
- Password protection alone is not considered to provide adequate protection against unauthorized access to personal health information stored on mobile computing devices.

Encryption

- Where identifiable personal health information is stored on vulnerable devices, such as laptop computers or flash drives, the information must be encrypted.
- Use up-to-date encryption techniques to ensure that personal information is appropriately secured.
- If the chosen encryption technology or software requires a password as a key, then strong passwords should be used. Strong passwords consist of at least eight characters and combine letters, numbers and symbols in what appear to be random strings.
- The encryption of files and folders should not rely on a user's login password due to vulnerabilities associated with such passwords. Do not use login passwords as passwords to decrypt files and folders.

- Encryption software packages should have built-in mechanisms to enforce the use of strong encryption keys.
- In addition to the encryption of individual files or folders using strong encryption keys, another option is to encrypt an entire hard disk within a laptop computer. Full disk encryption is a type of software or hardware that can be used to protect all the data on a hard disk, including the operating system, resident data, temporary files, and deleted files. Other disk encryption software can be used to protect everything on a hard disk, except the operating system.

Breaches

To the extent that personal health information on a mobile computing device has been encrypted to protect it from unauthorized access, the Information and Privacy Commissioner has ruled that it will not consider the theft or loss of that device to be a loss or theft of personal health information.

If the case can be made that the personal health information was not stolen, lost or accessed by unauthorized persons as a result of the loss or theft of a mobile computing device because the data were encrypted (and encrypted data does not relate to identifiable individuals), the custodian would not be required to notify individuals under PHIPA.

In the event that a breach occurs from the theft or loss of a device containing personal health information, it must be reported immediately to the Corporate Access and Privacy Office, in accordance with the [Managing a Privacy Breach Policy](#). In the case of Toronto Public Health, the breach must be reported to the Manager, Information Management, Toronto Public Health.