



Fact Sheet

Safeguarding Personal Health Information

The *Personal Health Information Protection Act, 2004* (the *Act*) requires health information custodians (custodians) to protect personal health information in their custody or control and to ensure that records are retained, transferred and disposed of in a secure manner.

The purpose of this fact sheet is to highlight some important safeguards for protecting personal health information. Custodians should also consult additional resources such as the *Physician Privacy Toolkit* and the *Hospital Privacy Toolkit* (the *Toolkits*)¹, which set out these requirements in detail, and may be adapted to all custodians.

Storage of Personal Health Information

Custodians must take reasonable steps to keep personal health information securely stored. What is reasonable varies depending on the sensitivity of the information and the risks to which it is exposed. The size of an organization is also a factor to consider. For instance, large organizations dealing with significant amounts of sensitive personal health information will need different security than small offices. Custodians must therefore scale security measures to fit their own circumstances.

Steps to ensure safe storage of personal health information should address physical security,

technological security and administrative controls.

Physical security includes:

- Locked filing cabinets; and
- Restricted office access and alarm systems.

Technological security includes the use of:

- Passwords, user IDs;
- Encryption²; and
- Firewalls and virus scanners.

Administrative controls include:

- A concise written set of security rules;
- Appointment of a staff member with overall responsibility for security;
- Staff training;
- Security clearances;
- Access restrictions;
- Regular audits of actual practices for compliance with security policies; and
- Confidentiality agreements.

¹ The Toolkits were developed by the Ontario Medical Association, the Ontario Hospital Association, the Ontario Hospital eHealth Council and the Information and Privacy Commissioner/Ontario. Web links are provided under the heading Resources and Links at the end of this fact sheet.

² See IPC Fact Sheet No. 12, Encrypting Personal Health Information on Mobile Devices http://www.ipc.on.ca/images/Resources/up-4fact_12_e.pdf.



Where electronic health records are kept, custodians should ensure that they:

- Use features such as passwords to prevent unauthorized access;
- Install automatic back-up for file recovery to protect records from loss or damage; and
- Keep an audit trail that, at a minimum:
 - Records the date and time of each entry for each patient;
 - Shows any changes in the record; and
 - Preserves the original content when a record is changed, updated or corrected.

Note: Where a record is corrected under the *Act*, particular items may be struck out in a way that does not obliterate the record, or the content may be severed and stored separately with a link that enables a person to trace the incorrect information.³

A person who provides services to enable a custodian to collect, use and disclose information electronically must comply with the privacy protections set out in the regulations under the *Act*.⁴

Privacy breaches

Custodians must notify individuals whose personal health information has been stolen, lost or accessed by an unauthorized person.

Retention of personal health information

The *Act* requires personal health records be kept for as long as needed to allow an individual to exhaust any legal recourse regarding a request for access.

As a best practice, personal health records should be retained for their minimum retention periods.

The *Act* does not establish specific retention periods for personal health information. However, custodians should refer to their governing legislation and regulatory procedures to determine what record retention requirements apply in their circumstances.

The *Toolkits* include a summary of retention periods set by other authorities for health records, OHIP records, and research records.⁵

Transfer of personal health information

Records may be transferred to facilities, other custodians or successors.

Custodians must securely transfer records, and refer to their governing legislation and regulatory procedures to determine appropriate transfer requirements.

The *Act* requires custodians to make reasonable efforts to notify patients before transferring records to a successor, or if that is not reasonably possible, as soon as possible after the transfer.

³ Section 55(10) of the Act addresses duties upon granting a request for correction.

⁴ See section 10(4) of the Act and section 6 of O.Reg 329/04. The latter provision also sets out the requirements applicable to health information network providers.

⁵ See the Physician Privacy Toolkit, pages 45-48, and the Hospital Privacy Toolkit, pages 114-119.



Disposal of personal health information

Custodians must have procedures to securely dispose of personal health records so that the personal health information cannot be retrieved.

For hard copy records, secure disposal may mean shredding or burning them; and

For electronic records, secure disposal may include either physically destroying the media they are stored on (such as a CD) or magnetically erasing or overwriting the information in such a way that the information cannot be recovered.

Custodians should keep a record of disposal dates and the names of individuals whose records were disposed of.

Great care should also be taken to secure personal health information when moving offices.⁵ Files should not be left behind or tossed in the garbage without first being securely destroyed. If computers are to be sold, all personal health information must first be erased in such a way that it cannot be recovered.

Resources and links

This fact sheet has set out some of the basic requirements under the *Act* in relation to safeguarding, retaining, transferring and disposing of personal health information. Custodians are encouraged to consult additional resources in order to ensure full compliance with these requirements.

Here are links to the *Physician Privacy Toolkit* and the *Hospital Privacy Toolkit*.

As well as a number of publications specifically addressing the *Personal Health Information*

Protection Act, a general IPC privacy publication may also be useful in managing personal health information:

- *Moving Information: Privacy and Security Guidelines*

Other health privacy materials available from the IPC include:

- Frequently Asked Questions: *Personal Health Information Protection Act*;
- *A Guide to the Personal Health Information Protection Act*;
- *The Personal Health Information Protection Act and Your Privacy*;
- *Frequently Asked Questions: Health Cards and Health Numbers*;
- *Your Health Information: Your Rights*;
- *Collection, Use, Disclosure and Other Complaints: Personal Health Information Protection Act*; and
- *Access and Correction Complaints: Personal Health Information Protection Act*

For more information, please call, write or e-mail:

Information and Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Telephone: 416-326-3333 or 1-800-387-0073
Facsimile: 416-325-9195
TTY: 416-325-7539
Website: www.ipc.on.ca
Email address: info@ipc.on.ca