DUTIES OF A CUSTODIAN

SUMMARY OF CUSTODIAN DUTIES UNDER THE *PERSONAL HEALTH INFORMATION ACT*

Custodians have legislated duties as outlined in the *Act*. A custodian is required to:

1. prepare and make readily available a *notice of purposes*. This is a notice or poster describing the purpose of the custodian's collection, use and disclosure of personal health information (section 15);

2. have a written *retention and destruction* schedule for personal health information (section 50);

3. put in place *information practices* that:

    a. meet the requirements of the *Act* and the regulations;

    b. are reasonable in the circumstances; and

    c. ensure that personal health information in the custodian's custody or under its control is protected against

        i. theft or loss of the information, and

        ii. unauthorized access to or use, disclosure, copying or modification of the information. (section 62(1)) [1]

4. implement, maintain and comply with a *complaints policy* for an individual to make a complaint under this *Act* (section 62(2));

5. have the ability to create and maintain a *record of user activity* for any electronic information system it uses to maintain personal health information (section 63);

6. designate a *contact person* to perform the functions set out in the *Act* (section 67).

> ***Note: If the custodian is a "natural person" (i.e. an individual health care practitioner), the practitioner may act as the contact person;***

[1] "Information practices" defined on page 8

7. prepare and make available a *written privacy statement* about the custodian's information practices, how to reach the contact person, how to request access and correction of the individual's record, and how to make a complaint (section 68).

Items 1-3 and 6-7 are described in detail below. Item 3 (complaint policy) is described in detail in Chapter 9: *Complaints under PHIA* and Item 5 (record of user activity) is described in detail in Chapter 8: *Electronic Health Records/Electronic Information Systems.*

Custodians may review Template 3-1 *Compliance Checklist*, a list of high-level requirements in the legislation to assess their readiness for *PHIA.*

1. NOTICE OF CUSTODIAN'S PURPOSES

Under section 12 of *PHIA,* unless the *Act* requires express consent or makes exception to the requirement for consent, a custodian may accept knowledgeable implied consent as consent for the collection, use and disclosure of personal health information. Knowledgeable implied consent is the consent required for the provision of health care.

(See also Chapter 4 of the Toolkit – *Consent, Capacity and Substitute Decision-Making*).

A component of knowledgeable implied consent is the ability for a custodian to reasonably infer that the individual understands the custodian's purpose for collecting, using or disclosing the individual's personal health information.

Section 15(1) outlines the requirement to reach that inference. The custodian may either:

a) make readily available a notice describing the purpose in a manner that the purpose is likely to come to the individual's attention ("notice of purposes"); or

b) explain the purpose(s) to the individual.

The use of the term "readily available" suggests that a notice of purposes should be placed in a location where an individual would easily be able to locate and read it.

Posters and notices in waiting rooms are options for the posting of a notice of purposes.

CONTENT OF A NOTICE OF PURPOSES

A notice of purposes must provide enough information for the individual to understand:

- why their personal health information is being collected;
- how it will be used;
- why it would be disclosed;
- the individual's rights under the *Act;*
- where the individual can obtain more information about the *Act*; and
- how the individual can make a complaint or ask for a review under the *Act*.

The Ontario Information and Privacy Commissioner and the Ontario Bar Association (Health and Privacy Law sections) have jointly produced what they have called "short notices" for custodians covered by the Ontario *Personal Health Information Protection Act*. [2] The information they have produced is generally applicable to Nova Scotia's *PHIA.*

In summary, a notice of purposes under *PHIA* should include:

1. A statement about the purpose of the *Act:*
    - The purpose is stated in *PHIA* as "to govern the collection, use, disclosure, retention, disposal and destruction of personal health information in a manner that recognizes both the right of individuals to protect their personal health information and the need of custodians to collect, use and disclose personal health information to provide, support and manage health care".

    - A statement that includes a reference to the balance between the two objectives – privacy rights and use – would be sufficient.

2. A general statement about how the information will be used and disclosed, including:
    - to provide the individual with health care
    - to communicate with or consult with other providers about the individual's health care
    - to communicate with students in training with the custodian to support the individual's health care
    - to obtain payment for the individual's health care, including payment through the Medical Services Insurance Program administered by Medavie Blue Cross, and payment from the individual's private insurance

[2] The Ontario Information and Privacy Commissioner produced the short notice information in conjunction with the Ontario Bar Association (Health and Privacy Law Sections), the Ontario Ministry of Health and Long Term Care, and the Ontario Dental Associations. The sample short notices are available at http://www.ipc.on.ca/ under "Resources".

- to report issues as required or permitted by provincial or federal law including the *Prescription Monitoring Act*

3. A statement about the individual's rights under *PHIA:*
   - to request and receive or view a copy of the individual's personal health information (with exceptions)
   - to request that corrections be made to personal health information that is not accurate, complete or up-to-date
   - to request a record of who has accessed the individual's personal health information on an electronic information system (a record of user activity)
   - to request that specific personal health information not be provided to other health care providers
   - to be advised if a breach of the individual's personal health information has occurred [3]
   - to make a complaint to the custodian about a concern related to access, correction or another privacy issue under the *Act*
   - to request a review by the Review Officer of the custodian's decision or actions

See Template 3 – 2 *Template for a Notice of Purposes.*

EXCEPTIONS TO AN INFERENCE OF KNOWLEDGEABLE IMPLIED CONSENT

Section 15(2) states that a custodian cannot infer that the individual understands the purposes if the custodian should have known that:

a) the individual has a limited ability to read or understand the language in which the notice or explanation is presented; or

b) has a disability or condition that impairs the individual's ability to read or understand the notice.

If this is the case, section 15(3) requires the custodian to make "reasonable efforts" to assist with the individual's understanding of the purposes. This may include verbally explaining the purpose(s) to the individual, or facilitating an explanation – verbally or in writing - in the individual's language.

[3] See Template 3-5 *Breach Reporting Form*

EXAMPLE

Edward, a physiotherapist, produces a poster that outlines:

- the purpose of *PHIA*
- the patient's basic rights under *PHIA* (including the right to make a complaint)
- why the physiotherapist collects personal health information
- how the personal health information will be used and disclosed
- the right of a patient to request that disclosure of their information be limited or revoked
- the right of a patient to make a complaint about the physiotherapist's use and disclosure of information
- the name and contact information for the physiotherapist's privacy contact person under the legislation

The poster is in English, and is posted on the counter where all patients are required to check in with the receptionist, and where they pay for any services or purchases.

Candace shows up for her physiotherapy appointment. She is obviously able to read the notice and asks no questions about it.

In this case, it would be reasonable for Edward to infer that Candace is providing "knowledgeable implied consent" to him – that is, she understands the information and by proceeding with requesting services, she is consenting to Edward's collection, use and disclose of her personal health information.

If another client came to the clinic and it was obvious that the client did not read or speak English, Edward would be required to make a reasonable effort to assist the client's understanding of the notice. This could include asking if anyone in the clinic could help with translation, or using an online translator.

2. RETENTION AND DESTRUCTION SCHEDULE

RETENTION

"Retention" is described as "[t]he process of holding data or information in a secure or intact manner usually for a defined period of time after which it may be permanently discarded".[4]

A custodian under *PHIA* is required to have a written retention schedule for personal health information in its custody or under its control (section 50(1)). The *Act* does not set out a specific period for which records must be retained by a custodian, but does provide that the schedule set out all legitimate purposes for retaining the information, and the retention and destruction schedules associate for each purpose.

The regulatory bodies for regulated professions and professional associations may also provide guidance on the issue of retention specific to each profession.

The COACH Guidelines also note the following specific issues to consider for retention:

- information is only retained for as long as is needed to fulfill the identified purpose(s);
- if information is used to make a decision about an individual, it must be retained long enough to allow the individual to access the information and challenge its accuracy;
- retention schedules must include a minimum and maximum retention time and must contemplate all forms of media on which patient information is stored (i.e. paper, electronic, microfiche);
- legislation affecting retention takes precedence over retention times tied to specific purposes;
- custodians should ensure that personal health information held by their agents or other third parties is retained and destroyed in accordance with the custodian's retention schedule; and
- an individual's right of access to personal health information continues until personal health information has been destroyed in accordance with a destruction/disposition schedule. [5]

See Template 3 – 3 *Template for Retention Schedule*.

---

[4] *COACH Guidelines for the Protection of Health Information* (December 15, 2006) at p. 157. COACH is Canada's health informatics association. See www.coachorg.com or the Appendix 4: *Resources* section for information about purchasing the *Guidelines.*

[5] *COACH Guidelines for the Protection of Health Information* (December 15, 2006) at p. 168.

DESTRUCTION, DISPOSAL AND DE-IDENTIFICATION

Once the relevant retention period expires, PHIA section 49(2) states that the personal health information must be securely destroyed, erased or de-identified.

Under *PHIA*, "securely destroyed" means "destroyed in such a manner that reconstruction is not reasonably foreseeable in the circumstances" (section 49(1)). This would include shredding paper records in a manner that prevents the reassembling of the record (cross-cut shredding or pulverizing), or wiping the hard drive of any electronic devices.

ARMA's Generally Accepted Recordkeeping Principles recommend that *"destruction must always be performed in a manner that renders the records completely and irreversibly destroyed"*.[6]

The Ontario Information and Privacy Commissioner has developed a Fact Sheet on Secure Destruction of Personal Information.[7] It provides guidance on secure destruction for both paper and electronic records. This includes:

- securely destroying all copies of a record, including duplicate copies, personal copies of records, and records on all media (paper and electronic);
- ensuring that all electronic and wireless media (CDs, USB keys, personal digital assistants and hard drives) are securely destroyed by physically damaging and discarding them or wiping them when the medium is to be re-used; and
- remembering that office equipment– including photocopiers, fax machines, scanners and printers – may contain hard drives which retain information. Custodians should either disable the hard drives, or wipe them before disposing of the equipment.

Section 49(2) of *PHIA* also states that personal health information may be "de-identified". Section 3(g) of *PHIA* defines "de-identified information" as "information that has had all identifiers removed that

i. identify the individual, or

ii. where it is reasonably foreseeable in the circumstances, could be utilized, either alone or with other information, to identify the individual"

[6] ARMA (formerly Association of Records Managers and Administrators) Generally Accepted Recordkeeping Principles: Principle of Disposition. See http://www.armacanada.org/

[7] Fact Sheet #10 (December 2005) – see http://www.ipc.on.ca/ under "Resources"

Appropriate de-identification is important where identifying personal health information is no longer required for a custodian's primary purpose, but de-identified health information continues to be necessary for a custodian's secondary purposes.

EXAMPLE

Identifying personal health information is collected from Eleanor by her dentist to provide her with dental care. Once the retention period is reached for the identifying health information, the dentist may retain Eleanor's information in a de-identified form for research, quality or other management purposes.

Note: Section 5(2)(a) of PHIA provides that the Act does not apply to statistical, aggregate or de-identified health information. This permits a custodian to retain de-identified information beyond the retention schedule in effect for identifying personal health information

3. INFORMATION PRACTICES

A custodian is required to implement, maintain and comply with "information practices" that ensure personal health information in the custodian's custody or control is protected against theft or loss of the information and unauthorized access to or use, disclosure, copying or modification of the information (section 62(1)).

Section 3(n) of *PHIA* defines "information practices" as "the policies of a custodian or a prescribed entity[8] for actions in relation to personal health information, including:

- when, how and the purposes for which the custodian routinely collects, uses, discloses, retains, de-identifies, destroys or disposes of personal health information; and
- the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information.

As part of complying with *PHIA*, a custodian may choose to develop a written *PHIA* policy specific to the custodian's organization, its information practices and its patients, clients or residents. This policy may include the following:

[8] See Chapter 5 - *Collection, Use and Disclosure* at p. 19 - Prescribed Entity

- when and how the custodian collects personal health information;
- when and how the custodian uses personal health information;
- when and how the custodian discloses personal health information;
- the purposes for all of the above collections, uses and disclosures;
- any uses and disclosures the custodian may routinely make without the individual's consent (see. *PHIA* section 35 for permitted uses without consent, and sections 38(1) and (7), and section 39 for permitted disclosures without consent);
- a summary of the custodian's retention policy, including the custodian's destruction and/or disposition practices; and/or
- the name and contact information of the custodian's *PHIA* contact person(s).

The custodian should also develop, maintain and comply with policies related to administrative, technical and physical safeguards for personal health information, both paper and electronic.

These policies may include the following:

- physical security of the custodian's records when in paper form, including policies for taking information away from the workplace, and managing documents at a photocopier or fax machine;
- security standards for physical access to areas when personal health information is used or stored;
- required training on the requirements under *PHIA* for all employees, volunteers and other agents;
- "clean desk" policies for employees; and
- guidelines for appropriate conversations in public areas.

See Chapter 8 – *Electronic Health Record/ Electronic Information Systems* for detail related to personal health information held in electronic form.

4. COMPLAINTS POLICY

PRIVACY COMPLAINTS UNDER *PHIA*

Under section 62(2), every custodian is required to implement, maintain and comply with a complaints policy which outlines the process under which an individual may make a complaint. This requirement is part of the custodian's responsibilities to protect the personal health information of the individuals it serves.

An individual may make a complaint about any aspect of the custodian's conduct in relation to the privacy provisions of *PHIA*. Pursuant to section 92(1)(a) of *PHIA*, the "privacy provisions" of the Act are sections 11-70. These sections include:

- consent (sections 11 - 20)
- substitute decision-maker (sections 21-23)
- collection, use and disclosure - general (sections 24-29)
- collection (sections 30- 32)
- use (sections 33-35)
- disclosure (sections 36 - 46)
- retention, destruction, disposal and de-identification (sections 47 - 51)
- research (sections 52-60)
- practices to protect personal health information (sections 61 - 68)
- reporting of a privacy breach (sections 69 - 70)

ACCESS AND CORRECTION COMPLAINTS

Complaints related to a request for access and/or correction would follow the review process outlined in Chapter 10 – *The Review Officer, Reviews and Mediation.*

DEVELOPING A COMPLAINTS POLICY

The details of suggested content of a complaints policy and best practices for developing a policy are outlined in Chapter 9 – *Privacy Complaints under PHIA.*

5. DESIGNATION OF A CONTACT PERSON

A custodian is required to designate a contact person under *PHIA* to enhance accountability. If appropriate, the custodian can take on the contact person role. For example, if a physiotherapist is practicing as a sole practitioner, he can be the contact person.

Under section 67, the contact person's duties are to:

- facilitate the custodian's compliance with the *Act;*
- ensure that all agents of the custodian are informed of their duties under the *Act*;
- respond to inquiries about the custodian's information practices;
- respond to requests for access to and correction of records;
- receive and process complaints under the *Act*;
- facilitate the communications to and the training of the custodian's staff about the custodian's policies and procedures and about the *Act*; and
- develop information to explain the organization's policies and procedures.

The *PHIA* contact person does not have to have any specific education or professional background to fulfill the requirement in section 67. However, the contact person must have sufficient knowledge about the duties outlined below to be able to assist individuals who have questions about their personal health information and how it is managed by the custodian.

The contact person must also understand the requirements in *PHIA* to a level that would support their training of the custodian's staff and providing information to the custodian's agents and to the public.

The contact person duties can also be shared by more than one person in the custodian's organization.

The name and contact information for the contact person must be included in all privacy notices under *PHIA*. If more than one person is designated as being *PHIA* contacts, each contact person, their contact information and their duties under *PHIA* should be included.

For example, if one person is responsible for responding to requests for access and correction, and another is responsible for all other duties under *PHIA*, both would be listed with their individual contact information and their specific duties.

6. WRITTEN PRIVACY STATEMENT

Section 68 of the *Act* requires that a custodian make available to the public a written privacy statement explaining:

- the custodian's information practices;
- how to contact the designated contact person;
- how to obtain access to or request correction of a record; and
- how to make a complaint under *PHIA* to the custodian and to the Review Officer.

The written privacy statement is a more detailed version of the notice of purposes required under section 15(1)(a). It provides additional information about the custodian's management of personal health information. It may include specific details about the complaints process (e.g. the custodian's timelines for responding to the complaint), or set out the exceptions to a request for access to the individual's personal health information as permitted in section 72.

PHIA does not specify exactly how to make the written privacy statement available to the public; it states that it must make it available to the public "in a manner that is practical in the circumstances". This may include all or a combination of the following:

- providing brochures to patients;
- putting a poster on the wall of the office; and/or
- placing information on the custodian's website.

The written privacy statement must be available to the public on request.

See Template 3 – 4 *Template for a Written Privacy Statement.*

7. REPORTING OF A PRIVACY BREACH

Section 69 of *PHIA* requires a custodian to notify an individual at the *"first reasonable opportunity"* if the *custodian "believes on a reasonable basis that*

a) the information is stolen, lost or subject to unauthorized access, use, disclosure, copying or modification; and

b) as a result, there is potential for harm or embarrassment to the individual".

"FIRST REASONABLE OPPORTUNITY"

The definition of when the *"first reasonable opportunity"* is reached will vary depending on each custodian. If a custodian has a policy on how to report a breach, the policy should outline the steps to be taken between the time a breach is confirmed, and the time a decision is made to contact the individual(s) whose personal health information was the subject-matter of the breach.

The person who was responsible for committing the breach should not contact the individual immediately upon discovering the breach. The policy should indicate whether further action, investigation, and documentation are required before an individual is contacted about the breach of his/her personal health information.

CONTENTS OF A PRIVACY BREACH POLICY

Although *PHIA* does not specifically require that a custodian develop and maintain a breach policy, the Act does require that every custodian have information practices to protect personal health information in its custody or under its control:

> *62 (1) A custodian shall implement, maintain and comply with information practices that*
>
> *a) meet the requirements of this Act and the regulations;*
>
> *b) are reasonable in the circumstances; and*
>
> *c) ensure that personal health information in the custodian's custody or under its control is protected against*
>
> *(i) theft or loss of the information, and*
>
> *(ii) unauthorized access to or use, disclosure, copying or modification of the information.*

Privacy oversight bodies in other provinces have developed helpful material for the custodians in their jurisdictions.[9]

[9] See Information and Privacy Commissioner of Ontario *What to do When Faced with a Privacy Breach: Guidelines for the Health Sector* and *Privacy Breach Protocol & Guidelines for Government Organizations* at www.ipc.on.ca. Also Newfoundland and Labrador Health and Community Services *The Personal Health Information Act: Frequently Asked Questions,* at p. 48-50 at www.health.gov.nl.ca/health/phia/PHIA_FAQs_Feb_2011.pdf

The basic components of a privacy breach policy may include:

1. Containment of the privacy breach

Once a privacy breach has been discovered, the person who discovered the breach must act quickly to ensure that the breach is contained.

EXAMPLE

Leon, a nurse working in a large medical practice, sent a fax containing personal health information to the wrong fax address. Leon should immediately send a fax to the address where the information was sent asking the receiver to destroy the information and confirm with Leon that it has been destroyed.

Other examples of containment include:

- retracting an e-mail sent in error (where possible);
- contacting a person who has received personal health information in error to request that they return or destroy the information; and
- in the case of a lost mobile device, requesting that the device be remotely wiped of all information.

2. Notify all relevant individuals

Each custodian's breach policy should set out who should be contacted when a breach has occurred. In most cases, the person discovering the breach should notify both their immediate supervisor and the person designated by the custodian as the contact person for breaches reportable under *PHIA.* The custodian may develop a breach reporting form to accompany the policy. See Template 3-5 *Personal Health Information Breach Reporting Form* as an example.

Others who may need to be contacted include the custodian's legal counsel and the head of the custodian.

Notifying the individual whose personal health information was the subject of the breach should occur after a full investigation of the breach. As the legislation requires notification at the *"first reasonable opportunity"* the investigation should be commenced as soon as possible after the breach is discovered.

3. Investigate the breach

The individual who discovered the breach should work with whoever is designated in the breach policy to complete the investigation. Part of the investigation would include a determination of the two factors identified in s. 70(1); specifically that, despite the fact that the information has been stolen, lost or subject to unauthorized access, use, disclosure, copying or modification:

a) it unlikely that a breach of the information has occurred; or

b) there is no potential for harm or embarrassment to the individual.

There may be cases where personal health information has lost or stolen, but it is unlikely that the information was breached.

EXAMPLE

Priscilla, a physician with a small clinic, keeps a small number of medical records on her laptop in order to be able to review them at home. The laptop is encrypted, and requires one strong password to access the laptop's operating system and another to access the file. Priscilla's laptop is stolen out of her car.

When Priscilla reports it as required by her breach policy, she should provide the information about the encryption and the double passwords. The decision may be that it is unlikely that a breach of the information could have occurred.

In other cases, a thorough review of the incident may lead to a determination that there is no potential for harm or embarrassment to the individual.

EXAMPLE

Jane, a care coordinator with a district health authority, wants to review the health records of her four clients with continuing care assessments the next day. She takes the paper files home in her briefcase, and leaves for her bus. When she reaches her apartment, she realizes that she left her briefcase on the bus. The bus company was unable to locate it.

There was information in three of the four records that Jane believes on a reasonable basis would cause embarrassment to each of her clients, including previous treatment for addiction, status of relationship with children and information about the client's ongoing treatment for depression. The fourth record included only the client's name and address; however, the

presence of the record with the other three does suggest that the individual is being considered for a continuing care assessment.

Jane should inform her supervisor and the *PHIA* contact person about the loss of the records, indicating the specifics of the personal health information in each record. The *PHIA* contact person would make a recommendation to the Chief Executive Officer for the district health authority on which of the clients should be contacted.

4. Follow-up with recommendations on how to avoid future breaches

The individual who committed the breach and the contact person for *PHIA* should review the incident to determine if any further policies or procedures are needed to prevent future breaches. For example:

- if an unencrypted mobile device was lost, mandatory encryption may be recommended;
- if files were lost, the custodian may require that no records leave the custodian's premises; or
- if an e-mail was sent to the wrong address, the custodian may recommend that every e-mail address is checked before it is sent.