The *Personal Health Information Protection Act, 2004*: A Guide for Regulated Health Professionals

[May 6, 2013]

This Guide was originally prepared by Richard Steinecke in 2004 and has been updated by Erica Richler.

Introduction - Purpose of This Guide

This is intended as a general guide for regulated health professionals in Ontario on how to comply with the *Personal Health Information Protection Act, 2004* ("PHIPA" or the "Act"). It is not intended to provide legal advice. For legal advice, please speak to a lawyer.

The hope is that this Guide will be particularly useful for health professionals working in small organizations or on their own and who do not have access the resources that may be available in larger organizations.

This Guide addresses PHIPA only as it is the primary law that governs the handling of personal information by health professionals. However, health professionals should be aware that they may need to comply with the federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA")[1] if they engage in the following types of activities:

- commercial activities involving the collection, use or disclosure of personal information outside of Ontario; or
- commercial activities involving the collection of personal information that is not health information (for example if you collect a home address and credit card number to process a sale that is unrelated to your duties as a health care practitioner).

Many of the obligations under PHIPA and PIPEDA overlap, however.

In addition, health professionals should realize that they have confidentiality and privacy obligations that arise from other sources including the definition of professional misconduct made by their regulatory College, their contracts with their clients and, sometimes, their employer, and by the new court-created obligation protecting individuals from an "intrusion into their seclusion."[2]

The *Quality of Care Information Protection Act, 2004*[3] was enacted at the same time as PHIPA. Its purpose is to protect practitioners or facilities engaging in or cooperating with formal quality assurance programs from the use of such information for the purpose of suing them. This Guide does not deal with the *Quality of Care Information Protection Act, 2004*.

How to Use this Guide

This Guide sets out seven basic steps for developing policies in order to comply with PHIPA:

---

[1] S.C. 2000, c. 5, available online: http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html
[2] *Jones v. Tsige*, 2012 ONCA 32
[3] S.O. 2004, c. 3, Schedule B, available online: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04q03_e.htm

Step 1 – Designate Your Organization's Contact Person

Step 2 – Inventory the Information to be Covered by the Privacy Plan

Step 3 – Identify the Purposes for which you Collect, Use and Disclose Personal Health Information

Step 4 – Develop Practices Regarding Safeguards, Retention and Destruction

Step 5 – Develop Practices Regarding Access, Correction and Complaints

Step 6 – Establish a Privacy Breach Protocol

Step 7 – Implement Your Privacy Plan

For each step, this Guide provides a summary of the key principles under PHIPA, as well as instructions (italicized in text boxes) for completing that step.

At the end of the Guide, there are sample forms that can be used as templates for creating your organization's Written Public Statement (Form 1), Privacy Policy (Form 2) and Consent Form (Form 3) – all based on the information you will have gathered while completing steps one through seven. The forms are generic templates and will have to be modified to fit the particular circumstances of your organization. It is strongly recommended that you consult with a lawyer before implementing your privacy policies.

Step 1 – Designate Your Organization's Contact Person

(a) Identifying Your Organization

The basic organization that must comply with PHIPA is the "health information custodian". PHIPA provides a list of custodians, including the following:

- health care practitioners or persons who operate a group practice of health care practitioners (this includes all those registered under the *Regulated Health Professions Act*, naturopaths, registered social workers and social service workers, and unregistered health care practitioners);
- community service providers under the *Long Term Care Act*;
- community care access centres (CCACs); and
- most health facilities including public hospitals, long term care facilities, ambulance, laboratories, ambulance services and community health centres.

However, where a potential custodian is an individual practitioner who acts as an agent for another custodian (e.g., a group practice or a hospital), the organizational custodian and not the individual practitioner becomes the custodian. For example, a practitioner who acts as an agent for a hospital, CCAC or long term care facility is not a custodian. The purpose of this rule is to ensure that custodians do not need to compete for control over the privacy policies for the organization. However, the individual practitioner must then comply with the custodian's privacy practices when acting on the custodian's behalf unless otherwise permitted by law (s. 17).

Except for public hospitals and CCACs, a custodian can only have one physical site unless special permission is obtained from the Minister of Health and Long Term Care.

Identify your organization (e.g., this could be an individual regulated health professional if you are in a sole practice or a clinic if you belong to a group practice).

(b) Selecting Your Information Officer / Contact Person

The information officer (called the "contact person" under PHIPA) need not be a practitioner (s. 15).

The information officer is responsible for ensuring that the custodian puts in place and follows information practices (s. 10).

The contact person must do the following:

- facilitate compliance with PHIPA by the custodian,
- educate the agents of the custodian,
- respond to public inquiries about the custodian's information practices,
- oversee access and correction requests, and
- handle privacy complaints (s. 15).

The custodian is responsible for displaying a written public statement about its information practices (s. 16). A sample written public statement is attached as **Form 1**.

It is important that the custodian's information practices are fairly complete because there are special obligations on the custodian where it uses or discloses personal health information in a manner not described in the information practices (ss. 16(2)). For example, the custodian must normally try to notify the individual of that use or disclosure.

Select your organization's contact person.

Step 2 – Inventory the Information to be Covered by the Privacy Plan

(a) Personal Health Information

PHIPA applies to any collection, use or disclosure of personal health information by a health information custodian (s. 7).

Personal health information is very broadly defined (s. 4) and includes the following:

- it must relate to an identifiable individual, including information that can be combined with other data (e.g., a code or a key) to then identify the individual,
- it can be in oral or recorded format (thus simply asking a question even if the answer is not recorded can constitute collecting personal health information), and
- it relates to the individual's
    - physical or mental condition, including his or her family health history,
    - health care (including maintenance, preventative or palliative measures),
    - health care provider,
    - payment for the health service including health card number,
    - substituted decision maker, or
    - non-health care information (e.g., home contact information) mixed in with other personal health information.

PHIPA is usually paramount over any inconsistent provincial statute (s. 7). However, PHIPA has a number of exceptions within it. For example, PHIPA does not apply to the regulatory activities of a health College (cl. (9)(2)(e)).

(b) Inventory of Personal Health Information Collected

Conduct an inventory of all of the personal health information that you collect in the course of providing health care. You may use the lists below as a guide to the types of information that you collect.

Personal characteristics

- ☐ Name
- ☐ Home address, telephone number, email address
- ☐ Gender
- ☐ Age
- ☐ Language

- ☐ Ethnicity, race or country of origin
- ☐ Religion
- ☐ Education or training
- ☐ Occupation/profession
- ☐ Marital status, sexual history or sexual orientation
- ☐ Credit card or other payment information
- ☐ Income
- ☐ Other: _____
- ☐ Other: _____
- ☐ Other: _____

Heath information

- ☐ Health history of individual
- ☐ Family health history
- ☐ Health measurements, samples or examination results
- ☐ Health conditions, assessment results or diagnoses
- ☐ Health services provided to or received by the individual
- ☐ Prognosis or other opinions formed during assessment and treatment
- ☐ Compliance with assessment and treatment
- ☐ Reasons for discharge and discharge condition and recommendations
- ☐ Body part or bodily substance donation activities or plans for donations
- ☐ Identify of individual's substitute decision maker
- ☐ Identity of individual's health care providers
- ☐ OHIP number or eligibility for OHIP
- ☐ Insurance benefit coverage or eligibility
- ☐ Other: _____
- ☐ Other: _____
- ☐ Other: _____

Step 3 – Identify the Purposes for which you Collect, Use and Disclose Personal Health Information

(a) Principles of Identifying Purposes and Obtaining Consent

PHIPA generally requires consent for the collection, use and disclosure of personal health information (s. 29). PHIPA provides specific guidance as to what constitutes a valid consent for the collection, use and disclosure of such information.

For example, implied consent is generally permitted where it is reasonable to assume that the individual knows the purpose of the collection, use or disclose and their right to give or withhold consent. If the purposes are stated in a poster or brochure readily available and likely to be seen by the individual (for an example, see Form 1), one can assume the individual knows the purpose.

Importantly, health care practitioners can assume that they have an individual's implied consent to collect, use or disclose personal health information for the provision of health care if the following conditions are met:

- the information was received from the individual, the individual's substitute decision-maker or another health information custodian;
- the information was received for the purpose of providing health care to the individual;
- the information is collected, used or disclosed for the purpose of providing health care to the individual;
- if information is being disclosed, it must only be disclosed to another health information custodian; and
- the individual has not withheld or withdrawn consent.

While this term is not defined in PHIPA, this is commonly referred to as sharing personal health information within the "circle of care" (s. 18-20).

Express consent (verbal or written) is needed, however, to disclose personal health information to a non-custodian and to disclose personal health information to another custodian for purposes other than the provision of health care. In addition, express consent is required for certain fundraising and marketing activities (s. 18-20, 32-33).

Practitioners can assume that a written consent is valid unless provided with grounds to the contrary (s. 20).

A direction from a client not to record pertinent information is invalid (ss. 19(2)). However, a client may direct that part of his or her file not be given to another custodian. This is commonly referred to as placing that information in a "lock-box".[4] If the custodian feels that the other custodian needs the "locked" information, the disclosing custodian must advise the receiving custodian that some relevant information has been withheld at the direction of the client (but not what that withheld information is) (ss. 20(2) and 20(3)).

PHIPA also provides for the collection of personal health information from someone other than the client. Indirect collection is permitted, even without consent, if necessary for health care where obtaining consent would affect the accuracy or timeliness of the information (s. 36).

PHIPA provides detailed rules for obtaining substituted consent where the individual is not capable of understanding the information issue or appreciating its reasonably foreseeable consequences. The rules for substituted consent are very similar to those for treatment of incapable persons. One can presume an individual is capable until it becomes apparent that he or she is not capable (s. 21). The substituted decision maker for handling of treatment information issues is generally the same as the substituted decision maker for treatment decisions (s. 5). If the information issue is not related directly to treatment, the list of substituted decision makers is very similar to that under the *Health Care Consent Act, 1996* (s. 23). One minor difference is that a capable person can authorize someone in writing to act on his or her behalf. Another difference is that a custodial parent can authorize decisions affecting the personal health information of their child 15 years or younger unless the child disagrees, the child consented to the original treatment on his or her own or for some family counselling situations (s. 23). A third difference is that a guardian or attorney for property can act as a substitute (ss. 26(1)).

PHIPA has specific rules about fundraising. Generally express consent is required to use the information from a client chart for fundraising. Implied consent (perhaps through a posted written public statement) is permitted in limited circumstances (e.g., the custodian can only use the name and mailing address of the individual, the fundraising must be for a charitable purpose related to the custodian's operations, the individual must be provided with an easy way to opt out and the fundraising request must not reveal anything about the individual's health) (s. 32 of PHIPA and s. 10 of the regulations).

Fees cannot be charged for collecting and using personal health information. Only reasonable fees can be charged for the disclosure of personal health information (s. 35). In a decision regarding a patient's request for access, the Information and Privacy Commissioner of Ontario

[4] For more information, see the Information and Privacy Commissioner's "Fact Sheet #08 - Lock-box Fact Sheet", available online: http://www.ipc.on.ca/images/Resources/fact-08-e.pdf

established guidelines for charging fees. In that context, a reasonable fee was held to be $30.00 for the first 20 pages and 25 cents for every additional page.[5]

(b) Principles of Use and Disclosure

PHIPA provides some flexibility for the use of personal health information without consent. For example, personal health information can be used without consent for a purpose of planning or delivering programs, risk management, educating practitioners and some research situations (ss. 37(1)).

Similarly, PHIPA provides for the disclosure of personal health information without consent, including disclosure in the following circumstances:

- to other practitioners or facilities for the provision of health care, if it is not reasonably possible to obtain consent in a timely manner so long as the client has not objected to such disclosure;
- to confirm the presence, location and general health status (e.g., critical, poor, fair) of a client in a facility so long as the client has not objected when offered an opportunity to do so;
- in respect of a deceased individual for the purpose of identifying him or her, notifying family and friends of the death and to permit relatives to make relevant decisions about their own health;
- for audit and accreditation purposes;
- to address a significant risk of serious bodily harm to a person or group;
- to potential and actual successors of the custodian (although potential successors must provide a written confidentiality assurance and affected individuals must be notified of any actual transfer of records to a successor);
- to assess capacity under the *Health Care Consent Act, 1996* and the *Substitute Decisions Act, 1992*;
- to a health regulatory College;
- in order to cooperate with a statutorily authorized inspection, investigation or similar proceeding;
- in legal proceedings where the custodian or agent is or is expected to be a party or witness;
- in some research situations (subject to approval by a research ethics board);
- in some health planning and management purposes;
- to assist in the monitoring of public health funding;

[5] Information and Privacy Commissioner of Ontario, Order HO-009, October 2010, available online: http://www.ipc.on.ca/images/Findings/ho-009_1.pdf

- to a health data institute under various rules and restrictions; and
- if permitted or required by law (ss.38-47).

In a rare application of PHIPA to non-custodians, non-custodians are restricted in their ability to use personal health information disclosed to them by a custodian. Non-custodians can only use or disclose the information for the purpose for which they have received it or for the purpose of carrying out their statutory duties (s. 49). For example, if the College (a non-custodian) received information while investigating a complaint, the College could then use that same information to prosecute an unregistered person performing a controlled act.

PHIPA also provides rules for disclosure of personal health information outside of Ontario without consent. Such disclosure is possible for the provision of health care (unless the individual expressly refuses the disclosure), to a regulator of health practitioners, for payment purposes and if permitted by statute (s. 50).

(c) Primary Purpose for Collecting, Using and Disclosing Personal Health Information

Generally, the primary purpose for which a health professional collects, uses and discloses personal information is to provide clients with health services. This might be described as follows: "We collect, use and disclose information about your health history, your physical condition and function and your social situation in order to help us assess what your needs are, to advise you of your options and then to provide the health care you choose to have." A second primary purpose may be to obtain a baseline of health and social information so that in providing ongoing health services, changes can be identified. Identify the primary purposes for which you collect, use and disclose personal health information.

Primary Purpose #1: _____

Brief Description of the Purpose: _____
_____
_____

Primary Purpose #2: _____

Brief Description of the Purpose: _____
_____
_____

Primary Purpose #3: _____

Brief Description of the Purpose: _____
_____
_____

(d) Related and Secondary Purposes

Identify the related or secondary purposes for which you collect, use and disclose personal health information. Some examples are set out below.

Related Purpose #1: To obtain payment for services or goods provided

Brief Description: To obtain payment for health related services or goods provided. Payment may be obtained from the individual, OHIP, WSIB, private insurers or others.

Notes: Consent is not required (s. 37(1)(i))

Related Purpose #2: To conduct quality improvement and risk management activities

Brief Description: To review client files to ensure that we provide high quality services, including assessing the performance of our staff. External consultants (e.g. auditors, lawyers, practice consultants, voluntary accreditation programs) may conduct audits and quality improvement reviews on our behalf.

Notes: Consent is not required (s. 37(1)(d))

Related Purpose #3: To promote our clinic, special events and opportunities

Brief Description: To promote new services or goods available at our clinic or to advise clients of special events and opportunities (e.g. a seminar or conference) that we have available.

Notes: Express consent from the client must be obtained for all marketing and market research activities (s. 33)

Related Purpose #4: To comply with external regulators

Brief Description: Our professionals are regulated by [name of College] who may inspect our records and interview our staff as a part of its regulatory activities in the public interest. The [College] has its own strict confidentiality and privacy obligations. In addition, as professionals, we will report serious misconduct, incompetence or incapacity of other practitioners, whether they belong to other organizations or our own. Also, our organization believes that it should report information suggesting illegal behaviour to the authorities. In addition, we may be required by law to disclose personal health information to various government agencies (e.g. Ministry of Health, children's aid societies, Canada Customs and Revenue Agency, Information and Privacy Commissioner, etc.).

Notes: Consent is not required (ss. 43, 46, 60)

Related Purpose #5: To educate our staff and students

Brief Description: We value the education and development of future and current professionals. We will review client records in order to educate our staff and students about the provision of health care.

Notes: Consent is not required (s. 37(1)(e))

Related Purpose #6: To fundraise for our organization

Brief Description: To contact clients in order to raise funds for the operations of our organization.

Notes: Express or implied consent is required. If we rely on implied consent, we will post this on our written public statement (see Form 1 below), we will only use the client's name and address, we will provide clients with an easy opt-out option, and we will not reveal anything about our client's health in the request (s. 32 of PHIPA and s. 10 of the regulations).

Related Purpose #7: To facilitate the sale of our organization

Brief Description: If the organization or its assets were to be sold, the potential purchaser would want to conduct a "due diligence" review of the organization's records to ensure that it is a viable business that has been honestly portrayed. The potential purchaser must first enter into an agreement with the organization to keep the information confidential and secure and not to retain any of the information longer than necessary to conduct the due diligence. Once a sale has been finalized, the organization may transfer records to the purchaser, but it will make reasonable efforts to provide notice to the individual before doing so.

Notes: Consent is not required to disclose to a potential purchaser, but notice must be given to individuals in order to transfer records to a purchaser (s. 42).

Related Purpose #8: _____

Brief Description: _____

_____

_____

Notes: _____

Related Purpose #9: _____

Brief Description: _____

_____

_____

Notes: _____

(d) Review of Personal Health Information Collected

Review the personal health information that your organization collects that you identified in Step 2 above. If any of that information is not required for a purpose you have listed in Step 3, then you should stop collecting that information as it is unnecessary (s. 30).

Step 4 – Develop Practices Regarding Safeguards, Retention and Destruction

(a) Principles of Safeguarding Personal Information

Custodians must take reasonable steps to protect personal health information against theft, loss, unauthorized use, disclosure, copying, modification or disposal (ss. 12(1) and 13(1)). Custodians must put in place administrative (e.g., policies, training), physical (e.g., locked filing cabinets), and technical (e.g., passwords, encryption) safeguards and practices to ensure the security of personal health information. The nature of the required safeguards will vary depending on the circumstances, including the sensitivity of the information and the type of organization (for example, a hospital will require different safeguards than a small office). Examples of safeguards that can be implemented are set out in Section 4(b) of the Guide, below.

The Information and Privacy Commissioner of Ontario has issued orders against custodians where employees have accessed personal health information in the context of family or personal disputes (e.g., employee accessing records of her boyfriend's estranged spouse). In addition to the other safeguards discussed below, custodians must ensure that their staff is adequately trained on the appropriate collection, use and disclosure of personal health information. Staff members must also be aware that breaches can result in discipline, as well as reports to their governing regulatory College.

Given the prevalent use of mobile devices (e.g., laptops, PDAs, USB keys) in workplaces today, custodians must have practices in place to protect any personal health information that is stored on them. Practitioners should always consider whether it is necessary to store personal health information on a mobile device or whether an alternative, such as de-identifying the information or accessing the information through a secure remote connection, would suffice. If it is necessary to store personal health information on a mobile device, the information must be secured using "strong encryption."[6] Password protection is not enough. The Information and Privacy Commissioner of Ontario has stated that if personal health information on a mobile device is appropriately encrypted, the loss or theft of that device would not constitute a privacy breach.

Custodians should also implement policies regarding the appropriate use of social media. At a minimum, health professionals should never disclose personal health information on social

[6] For more information on the encryption of personal health information on mobile devices, see the Information and Privacy Commissioner of Ontario's Fact Sheets, "Health-Care Requirement for Strong Encryption", available online: http://www.ipc.on.ca/images/Resources/fact-16-e.pdf and "Encrypting Personal Health Information on Mobile Devices", available online: http://www.ipc.on.ca/images/Resources/up-4fact_12_e.pdf

media sites, unless they have the individual's consent to do so. If information is de-identified prior to being posted, the health professional must ensure that the individual's identify cannot be reasonably determined (e.g., in a small community or through Internet research). Health professionals must also be prudent not to post pictures of their workplaces that may include images of clients.

Records can be kept at the client's home or off-site (e.g., in a storage facility not controlled by the custodian) if the individual consents and it is done reasonably and in accordance with professional standards (s. 14).

Another rare example of where PHIPA applies to non-custodians is in relation to Information Technology (IT) providers to custodians. IT providers must only use personal health information for the purpose of providing their services to the custodians; IT providers cannot disclose any personal health information to which they have access. They must also provide the following:

- notification of any privacy breach to the custodian as soon as possible,
- a plain language description of their services,
- an audit trail feature to track the use of the database,
- a written risk assessment of the system, and
- their own written privacy policies.

IT providers and custodians must enter into written agreements that describe the services being provided, describe the safeguards in place and require the IT provider to comply with PHIPA and the regulations (s. 10 of PHIPA and s. 6 of the regulations).

(b) Administrative, Technical and Physical Safeguards

Identify the administrative, technical and physical safeguards that your organization has in place to protect the security of personal health information and consider whether any additional safeguards are required. It is not necessary to employ every safeguard listed below; a selection of safeguards is offered but not all are appropriate for every case (indeed, some of the options listed are inconsistent alternatives). In addition to the generic safeguards described below, special safeguards may be required for extremely sensitive information.

Physical Safeguards

Office area restricted to staff:

- ☐ no staff permitted without continuous supervision

- ☐ for larger organizations, use security badges or sign-in sheets
- ☐ all files with personal health information locked away after hours
- ☐ all files with personal health information locked away before non-staff permitted entry (e.g. cleaners)
- ☐ all non-staff who require entry (e.g. cleaners) must sign confidentiality agreement
- ☐ other: _____

Office area open to non-staff:

- ☐ area must be supervised at all times
- ☐ all files with personal health information must be locked away when staff not present (e.g., after hours)
- ☐ all files with personal health information must be locked away or supervised when staff person leaves their desk
- ☐ other: _____

Home office:

- ☐ files with personal health information must be locked away in a desk, filing cabinet or separate room when unattended
- ☐ other: _____

Transfer of physical files:

- ☐ in a sealed envelope, marked private and confidential, sent by Canada Post or reputable courier with a strong privacy policy[7]
- ☐ in a sealed envelope, marked private and confidential, delivered by staff
- ☐ in a sealed envelope to be picked up by recipient or person authorized by recipient (identity to be confirmed)
- ☐ other: _____

General:

- ☐ office equipped with alarm/security system
- ☐ other: _____

[7] Note that the Information and Privacy Commissioner of Ontario held that it was inappropriate for Cancer Care Ontario to use a courier service to transfer paper records containing colon cancer screening information relating to over 7000 individuals to physicians. The Commissioner held that in the particular circumstances (i.e., the sophistication of the organization and of the recipients, the number of individuals affected, the volume and frequency of the transfers and the availability of alternatives), the organization should have transferred the records using secure electronic means. For more information, see the Commissioner's Fact Sheet, "The Secure Transfer of Personal Health Information", available online: http://www.ipc.on.ca/images/Resources/fact-18-e.pdf.

Technical Safeguards

Office area restricted to staff:

- ☐ no non-staff permitted without continuous supervision
- ☐ for larger organizations, use security badges or sign-in sheets
- ☐ all non-staff who require entry (e.g. cleaners) must sign confidentiality agreement
- ☐ a strong login password is required on each terminal/device
- ☐ other: _____

Office area open to non-staff:

- ☐ area must be supervised at all times
- ☐ no personal health information can be left on a screen when person leaves workstation (log off, shut down or lock computer)
- ☐ a strong login password is required on each terminal/device
- ☐ other: _____

Mobile devices (e.g. laptops, PDAs, USB keys) and remote access:

- ☐ must have strong encryption
- ☐ must have strong login password
- ☐ identifying information should not be used in cell phone conversations, text messages or email messages
- ☐ remote access available only through secure remote network or virtual private network
- ☐ other: _____

Transfer of electronic information:

- ☐ by using an encrypted USB drive or other encrypted storage device
- ☐ by using a secure web portal
- ☐ by email if:
    - consent is obtained,
    - the message is anonymized, or
    - the information is encrypted
- ☐ by fax if:
    - a cover sheet identifies the recipient and includes a privacy clause,
    - the fax number has been approved by the recipient,
    - the recipient is expecting the fax,
    - the recipient has advised that the fax machine is securely located, and

  - the recipient confirms that all pages have been received
- ☐ other: _____

General:

- ☐ networks/computers must be protected by up-to-date virus scanners and firewalls
- ☐ appropriate file back-up systems must be in place
- ☐ for more sophisticated networks, unique user identifiers, audit trails, and intrusion detection systems
- ☐ for wireless networks, up-to-date transmission encryption should be used
- ☐ other: _____

Administrative Safeguards

- ☐ staff (including temporary staff) is trained in the following:
  - the importance of protecting the privacy of personal health information
  - access to personal health information within the organization is on a need-to-know basis
  - the organization's Privacy Policy
  - the appropriate use of social media
  - sensitivity in collecting or using personal health information verbally where others might hear
  - when providing copies of personal health information internally or externally, to remove or redact unnecessary personal health information
  - to recognize and avoid being "pumped" for information
  - to ensure that any personal information is not accidentally discarded in the regular garbage or blue box disposal system, but rather is cross-cut shredded
  - to ensure that when electronic data is deleted or hardware is discarded, the data cannot be recovered
  - to avoid discussing personal information in public places (e.g., elevators, restaurants, washrooms, public transit)
  - that breach of the organization's policies will result in discipline up to and including dismissal, as well as a report to the relevant regulatory College
- ☐ regular (at least annual) review and updating of staff through a continuing education program
- ☐ privacy and security agreements with the following consultants and outsourced providers:
  - temporary workers
  - cleaners

  - information technology providers
  - marketers
  - legal
  - bookkeeping and accounting
  - file storage
  - credit card companies
  - website manager
  - office security
  - building maintenance
  - landlord
  - other: _____

- ☐ regular and systematic monitoring of compliance with the organization's policies by the Contact Person or his or her delegate (which should be documented)
- ☐ regular reminders to staff to change their passwords and to have strong passwords
- ☐ regular and systematic auditing of the electronic safeguards by an external company (which should be documented)
- ☐ review physical layout and procedures appropriate to the context (e.g., use rooms rather than cubicles or curtains for sensitive interviews, keep people in the waiting room for as short a time as possible)
- ☐ other: _____

(c) Retention and Destruction of Personal Information

PHIPA requires custodians to establish retention and destruction policies, but it does not prescribe how long records must be kept. Health practitioners should abide by their professional standards, as well as any other applicable laws. Typically, professional standards require health practitioners to retain clinical records for 10 years after the last client interaction or 10 years after the client turns 18 years of age. Circumstances may require an organization to retain clinical records for a longer period, such as where litigation is contemplated or ongoing or where a request for access to the record is outstanding.

Personal health information must be disposed of in a secure manner, such that the records cannot be reconstructed (s. 13 of the Act and s. 1(5.1) of the regulations). For example, paper records should be cross-cut shredded and electronic files or hardware must be deleted or destroyed in a way that the information cannot be recovered. The practices of external shredding services should be reviewed closely as many complaints have come in to the

Information and Privacy Commissioner about failed shredding security (e.g., containers falling off a truck).

Where an individual practitioner dies, the person responsible for the estate of the practitioner is responsible to comply with PHIPA until he or she is able to transfer the information to another custodian (ss. 3(11) and 3(12)).

Determine the minimum period of time your organization will retain records containing personal health information.

Step 5 – Develop Practices Regarding Access, Correction and Complaints

(a) Access Rights

PHIPA provides a broad right of access to the personal health information held by a custodian about an individual. However, PHIPA provides some grounds for refusing such a request including the following:

- it is quality of care information or information generated for the College's quality assurance program,
- it is raw data from standardized psychological tests or assessments,
- there is a risk of serious harm to the treatment or recovery of the individual or of serious bodily harm to another person, or
- access would reveal the identity of a confidential source of information (s. 51-52).

PHIPA provides procedures for handling access requests including the following:

- the custodian must assist the individual in making a meaningful request, if necessary,
- while the custodian can informally provide access, it can also insist upon a formal written request,
- the custodian should, where reasonably practical, explain terms, codes and abbreviations,
- the custodian must notify the individual of his or her right to complain to the Information and Privacy Commissioner of Ontario if the request for access is refused (along with the reasons for the refusal) and the burden of justifying the refusal is on the custodian,
- the custodian can refuse frivolous, vexatious and bad faith requests for access,
- the custodian must satisfy itself of the identity of the individual before granting him or her access,
- the custodian can only charge a reasonable cost recovery fee for access and must provide an estimate of the fee in advance (the Information and Privacy Commissioner has held that a reasonable fee is $30.00 for the first 20 pages and 25 cents for every additional page), and
- the custodian must respond to a request for access as soon as possible and no later than 30 days after receiving the request, but the custodian can extend the time for a response by another 30 days if necessary (s. 53-54).

(b) Correction Rights

PHIPA provides for a broad right of individuals to correct errors in their records (s. 55). However, PHIPA provides grounds for refusing such requests including the following:

- where the request is frivolous, vexatious or made in bad faith,
- the custodian did not create the record and the custodian does not have sufficient knowledge, expertise or authority to make the correction, or
- the information consists of a professional opinion or observation made in good faith (s. 55).

PHIPA provides procedures for handling correction requests including the following:

- while the custodian can informally make the correction, it can also insist upon a formal written request,
- the correction should not obliterate the original entry, and
- any notice of refusal must advise the individual of his or her right to include a concise statement of disagreement in the record and of his or her right to complain to the Information and Privacy Commissioner of Ontario about the refusal (s. 55).

At an individual's request, custodians must notify others who have received the incorrect or disputed information. However, the notification need only be made where reasonably possible, and the custodian can refuse to give the notification if the correction cannot reasonably be expected to have an effect on the ongoing provision of health care or some other benefit to the individual (ss. 55(10)(c)).

(c) Complaints System

PHIPA does not provide much detail about the nature of the custodian's internal complaints system – it simply has to have one (s. 16). This provides organizations with a great deal of flexibility in terms of how they structure their internal complaints system.

Develop a process for dealing with internal complaints and determine who will perform each function.

- ☐ Designate the Contact Person as the recipient of internal complaints about privacy practices
- ☐ Ensure staff know where to direct complaints (i.e., to the Contact Person)
- ☐ When a complaint is received:
    - Acknowledge that the complaint has been received

        - performed by: _____ (e.g., Contact Person, staff working under Contact person)
    - Investigate the complaint (e.g., interview persons involved, conduct an audit of electronic systems)
        - performed by: _____
    - Determine what action, if any, will be taken
        - performed by: _____
    - Provide a response to the complainant, including a summary of any action taken
        - performed by: _____
    - Advise the complainant of their right to complain to the Information and Privacy Commissioner of Ontario
        - performed by: _____
    - other: _____

PHIPA does provide detailed provisions for an external complaints system led by the Information and Privacy Commissioner of Ontario. A person can make a complaint to the Commissioner. The Commissioner can take no action, try to mediate or resolve the complaint, or she can decide to review the Complaint. When conducting a review, the Commissioner has broad inspection powers.

After conducting a review, the Commissioner can directly issue a compliance order without first having to go to court (s. 61). A copy of any compliance order must be given to the custodian's regulator (i.e., the regulatory College) (ss. 61(3)). Where an order is made, the individual can sue in court for actual damages, as well as up to $10,000 for mental anguish damages (s. 65).

PHIPA also provides whistle-blowing protections, as well as broad protections for persons who disregard their employer's or other's wishes in order to comply with PHIPA (s. 70-72).

PHIPA also creates many offences for deliberately breaching the Act (s. 72). For example, wilfully collecting, using or disclosing personal health information contrary to the Act is an offence. So is the deliberate disposal of such information in an insecure manner (e.g., throwing documents in the blue box without first shredding them). An individual who is found guilty of an offence can face a fine of up to $50,000 and an organization can face a fine of up $250,000.

Step 6 – Establish a Privacy Breach Protocol

There is a positive obligation under PHIPA to notify affected individuals of a privacy breach (e.g. the theft, loss or unauthorized access of personal health information) (ss. 12(2)).

While the focus of this Guide has been on preventing such breaches, custodians should develop policies on how to handle breaches if and when they do occur. The Information and Privacy Commissioner of Ontario has developed Guidelines for the Health Care Sector on "What to do When Faced with a Privacy Breach."[8] The checklist below is based on the Commissioner's Guidelines.

Develop a privacy breach protocol for your organization, using the following checklist as a guide.

If a privacy breach is suspected or known to have occurred, take the following action:

- ☐ Implement the organization's privacy breach protocol
  - Ensure the Contact Person and appropriate staff/departments are informed of breach
  - Consider notifying the Commissioner of the breach
- ☐ Contain the breach
  - Retrieve hard copies of personal health information that have been disclosed
  - Ensure no copies have been made
  - Take steps to prevent unauthorized access to electronic information (e.g., restrict access, change passwords, temporarily shut down system)
- ☐ Notify affected individuals
  - Consider the most appropriate way to notify affected individuals in light of the sensitivity of the information (e.g., by phone, in writing, at the next appointment)
  - Provide the organization's contact information in case the individual has further questions
  - Provide the Commissioner's contact information
- ☐ Investigate and remediate the problem
  - Conduct an internal investigation
  - Determine what steps should be taken to prevent future breaches (e.g. changes to policies, additional safeguards required)

[8] Information and Privacy Commissioner of Ontario, "What to do When Faced With a Privacy Breach: Guidelines for the Health Care Sector", available online: http://www.ipc.on.ca/images/Resources/up-hprivbreach.pdf

- Consider advising the Commissioner of the results of your investigation
- Report the results of investigation to the relevant regulatory College if appropriate
- Ensure staff is appropriately trained and conduct further training if required

Step 7 – Implement Your Privacy Plan

Implementing your Privacy Policy will have two stages. The first stage will be to complete your review of how you handle personal information and to prepare and roll out your Privacy Policy. The second stage is to periodically monitor, review and update your Privacy Policy. During your first year, the monitoring, review and updating should be fairly frequent as issues arise. However, after that, you still must regularly review things. The Information and Privacy Commissioner of Ontario has criticized organizations for having a policy in writing that does not reflect what is actually happening. At a minimum, a specific date should be set each year (e.g., July) to monitor, review and update the Privacy Policy. That annual review should be documented in case the Information and Privacy Commissioner comes calling.

Use the following checklist to track the implementation of your organization's privacy plan.

Initial Implementation

- ☐ Written public statement (Form 1) completed and posted publicly
- ☐ Privacy Policy document (Form 2) prepared
- ☐ Consent form (Form 3) prepared
- ☐ Initial staff training completed
- ☐ Administrative, physical and technical safeguards implemented, including signed contracts with external consultants and outsourcing providers

Ongoing Review

- ☐ Monitoring compliance with Privacy Policy document (prepare a report annually)
- ☐ External information technology audit (annual)
- ☐ Refresher training session for all staff (annual)
- ☐ Training for new staff provided as needed
- ☐ Review and update of Privacy Policy document (annual)

Form 1: Sample Written Public Statement (s. 16)

This sample written public statement should be modified to fit your organization's needs. In particular, you may need to modify the types of personal health information that are collected or the purposes for which that information is collected.

The statement may be printed as a poster or brochure and should be posted or placed somewhere in your office where it is likely to come to your clients' attention (such as near the reception desk or waiting area) and may also be given to clients when they come under your care.

Our Privacy Commitment to You

We are committed to protecting your privacy and ensuring the confidentiality of your personal health information. The types of personal health information we collect may include your name, date of birth, health history, OHIP number and records of the care provided to you. We collect, use and disclose personal health information for the following purposes:

- to provide [type of health service or therapy] to our clients
- to obtain payment for services provided (from you, OHIP, WSIB, your private insurer or others)
- to teach students and to provide continuing education to our staff
- to fundraise for our organization (but you may opt-out of receiving fundraising solicitations by contacting us at the address below)
- [add: any other purposes relevant to organization]
- to conduct quality improvement and risk management activities
- to comply with our regulatory obligations to [name of College]
- to advise clients about special events or opportunities (but we will always obtain express consent to do so)
- for other purposes permitted by law

We will collect, use and disclose only as much personal health information as is needed to achieve these purposes. You can withhold or withdraw your consent to the collection, use or disclosure of your personal health information by contacting us (details below).

Access to Health Records

You have the right to seek access to your health records that we keep and to ask us to correct a record if you believe it is inaccurate or incomplete. Please contact us for more information.

Questions or Concerns?

If you have questions or want to make a complaint about our privacy practices, please contact: **[insert name of contact person or custodian]**

You also have the right to complain to the Information and Privacy Commissioner of Ontario at the address below if you have concerns about our privacy practices or how your personal health information has been handled:

Information and Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400, Toronto, Ontario M4W 1A8
Telephone: Toronto Area (416/local 905): (416) 326-3333
Long Distance: 1 (800) 387-0073 (within Ontario)
TDD/TTY: (416) 325-7539
FAX: (416) 325-9195
www.ipc.on.ca

Form 2: Sample Privacy Policy for Regulated Health Professional

This sample privacy should be modified to fit your organization's needs. In particular, you will need to tailor the document to reflect the types of personal health information that your organization collects, the purposes for which that information is collected, used and disclosed, and the safeguards that you have implemented.

Privacy of personal information is an important principle to the [name of organization]. We are committed to collecting, using and disclosing personal information responsibly and only to the extent necessary for the [goods and] services we provide. We try to be open and transparent about how we handle personal information. This document describes our privacy policies.

What is Personal Health Information?

Personal health information is information about an identifiable individual. Personal health information includes information that relates to:

- the physical or mental health of the individual (including family health history);
- the provision of health care to the individual (including identifying the individual's health care provider);
- a plan of service under the *Home Care and Community Services Act, 1994*;
- payments or eligibility for health care or coverage for health care;
- the donation or testing of an individual's body part or bodily substance;
- the individual's health number; or
- the identification of the individual's substitute decision-maker.

Who We Are

Our organization, [name of organization], includes at the time of writing [insert number of professionals and support staff]. We use a number of consultants and agencies that may, in the course of their duties, have limited access to personal health information we hold. These include computer consultants, office security and maintenance, bookkeepers and accountants, lawyers, temporary workers to cover holidays, credit card companies, website managers and cleaners. We restrict their access to any personal information we hold as much as is reasonably possible. We also have their assurance that they follow appropriate privacy principles.

Why We Collect Personal Health Information

We collect, use and disclose personal information in order to serve our clients. For our clients, the primary purpose for collecting personal health information is to provide [type of therapy or treatment]. For example, we collect information about a client's health history, including their family history, physical condition and function and social situation in order to help us assess what their health needs are, to advise them of their options and then to provide the health care they choose to have. A second primary purpose is to obtain a baseline of health and social information so that in providing ongoing health services we can identify changes that are occurring over time.

We also collect, use and disclose personal health information for purposes related to or secondary to our primary purposes. The most common examples of our related and secondary purposes are as follows:

Related Purpose #1: To obtain payment for services or goods provided. Payment may be obtained from the individual, OHIP, WSIB, private insurers or others.

Related Purpose #2: To conduct quality improvement and risk management activities. We review client files to ensure that we provide high quality services, including assessing the performance of our staff. External consultants (e.g. auditors, lawyers, practice consultants, voluntary accreditation programs) may conduct audits and quality improvement reviews on our behalf.

Related Purpose #3: To promote our clinic, new services, special events and opportunities (e.g. a seminar or conference) that we have available. We will always obtain express consent from the client prior to collecting or handling personal health information for this purpose.

Related Purpose #4: To comply with external regulators. Our professionals are regulated by [name of College(s)] who may inspect our records and interview our staff as a part of its regulatory activities in the public interest. The [College] has its own strict confidentiality and privacy obligations. In addition, as professionals, we will report serious misconduct, incompetence or incapacity of other practitioners, whether they belong to other organizations or our own. Also, our organization believes that it should report information suggesting illegal behaviour to the authorities. In addition, we may be required by law to disclose personal health information to various government agencies (e.g. Ministry of Health, children's aid societies, Canada Customs and Revenue Agency, Information and Privacy Commissioner, etc.).

Related Purpose #5: To educate our staff and students. We value the education and development of future and current professionals. We will review client records in order to educate our staff and students about the provision of health care.

Related Purpose #6: To fundraise for the operations of our organization, with the express or implied consent of our clients. If we rely on implied consent, we will only use the client's name and address, we will provide clients with an easy opt-out option, and we will not reveal anything about our client's health in the request.

Related Purpose #7: To facilitate the sale of our organization. If the organization or its assets were to be sold, the potential purchaser would want to conduct a "due diligence" review of the organization's records to ensure that it is a viable business that has been honestly portrayed. The potential purchaser must first enter into an agreement with the organization to keep the information confidential and secure and not to retain any of the information longer than necessary to conduct the due diligence. Once a sale has been finalized, the organization may transfer records to the purchaser, but it will make reasonable efforts to provide notice to the individual before doing so.

Protecting Personal Information

We understand the importance of protecting personal information. For that reason, we have taken the following steps:

- Paper information is either under supervision or secured in a locked or restricted area.
- Electronic hardware is either under supervision or secured in a locked or restricted area at all times. In addition, strong passwords are used on all computers and mobile devices.
- Personal health information is only stored on mobile devices if necessary. All personal health information stored on mobile devices is protected by strong encryption.
- We try to avoid taking personal health information home to work on there. However, when we do so, we transport, use and store the personal health information securely.
- Paper information is transferred through sealed, addressed envelopes or boxes by reputable companies with strong privacy policies.
- Electronic information is either anonymized or encrypted before being transmitted.
- Our staff members are trained to collect, use and disclose personal information only as necessary to fulfill their duties and in accordance with our privacy policy.
- We do not post any personal information about our clients on social media sites and our staff members are trained on the appropriate use of social media sites.
- External consultants and agencies with access to personal information must enter into privacy agreements with us.

Retention and Destruction of Personal Information

We need to retain personal information for some time to ensure that we can answer any questions you might have about the services provided and for our own accountability to

external regulatory bodies. However, in order to protect your privacy, we do not want to keep personal information for too long.

We keep our client files for at least ten years from the date of the last client interaction or from the date the client turns 18.

We destroy paper files containing personal health information by cross-cut shredding. We destroy electronic information by deleting it in a manner that it cannot be restored. When hardware is discarded, we ensure that the hardware is physically destroyed or the data is erased or overwritten in a manner that the information cannot be recovered.

You Can Look at Your Records

With only a few exceptions, you have the right to see what personal information we hold about you, by contacting [contact person]. We can help you identify what records we might have about you. We will also try to help you understand any information you do not understand (e.g., short forms, technical language, etc.). We will need to confirm your identity, if we do not know you, before providing you with this access. We reserve the right to charge $30.00 for the first twenty pages of records and 25 cents for each additional page.

We may ask you to put your request in writing. We will respond to your request as soon as possible and generally within 30 days, if at all possible. If we cannot give you access, we will tell you the reason, as best we can, as to why.

If you believe there is a mistake in the information, you have the right to ask for it to be corrected. This applies to factual information and not to any professional opinions we may have formed. We may ask you to provide documentation that our files are wrong. Where we agree that we made a mistake we will make the correction. At your request and where it is reasonably possible, we will notify anyone to whom we sent this information (but we may deny your request if it would not reasonably have an effect on the ongoing provision of health care). If we do not agree that we have made a mistake, we will still agree to include in our file a brief statement from you on the point.

If there is a Privacy Breach

While we will take precautions to avoid any breach of your privacy, if there is a loss, theft or unauthorized access of your personal health information we will notify you.

Upon learning of a possible or known breach, we will take the following steps:

- We will contain the breach to the best of our ability, including by taking the following steps

    - Retrieving hard copies of personal health information that have been disclosed
    - Ensuring no copies have been made
    - Taking steps to prevent unauthorized access to electronic information (e.g., change passwords, restrict access, temporarily shut down system)
- We will notify affected individuals
    - We will provide our contact information in case the individual has further questions
    - We will provide the Commissioner's contact information
- We will investigate and remediate the problem, by:
    - Conducting an internal investigation
    - Determining what steps should be taken to prevent future breaches (e.g. changes to policies, additional safeguards)
    - Ensuring staff is appropriately trained and conduct further training if required

Depending on the circumstances of the breach, we may notify and work with the Information and Privacy Commissioner of Ontario. In addition, we may report the breach to the relevant regulatory College if we believe that it was the result of professional misconduct, incompetence or incapacity.

Do You Have Questions or Concerns?

Our Information Officer, [name], can be reached at:

[contact information]

He/She will attempt to answer any questions or concerns you might have.

If you wish to make a formal complaint about our privacy practices, you may make it in writing to our Information Officer. He/She will acknowledge receipt of your complaint, and ensure that it is investigated promptly and that you are provided with a formal decision and reasons in writing.

You also have the right to complain to the Information and Privacy Commissioner of Ontario if you have concerns about our privacy practices or how your personal health information has been handled, by contacting:

Information and Privacy Commissioner/Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8
Telephone: Toronto Area (416/local 905): (416) 326-3333
Long Distance: 1 (800) 387-0073 (within Ontario)

TDD/TTY: (416) 325-7539
FAX: (416) 325-9195
www.ipc.on.ca

This policy is made under the *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3. It is a complex statute and provides some additional exceptions to the privacy principles that are too detailed to set out here.

Form 3: Sample Consent Form

This form can be used when your organization seeks express consent to collect, use or disclose personal health information. This form may be combined with your organization's usual consent to treatment and/or consent to the costs of services forms.

Consent to the Collection, Use and Disclosure of Personal Health Information

Note to client: We want your informed consent. We want you to understand what we do with the personal health information we collect about you. Please ensure that you have read and understood our written statement, "Our Privacy Commitment to You". If you have any questions, please ask.

I, _____, understand that to provide me with [type of health care goods or services], [name of organization] will collect personal information about me (e.g., birth date, home contact information, health history, etc.).

I have reviewed the [organization's] written statement on the collection, use and disclosure of personal health information. I understand how the written statement applies to me. I have been given a chance to ask questions about the [organization's] privacy policies and they have been answered to my satisfaction.

I understand that the [organization] will only collect, use or disclose my personal health information with my express or implied consent, unless a collection, use or disclosure without consent is permitted or required by law.

I authorize the [organization] to collect, use and disclose my personal health information for the following purposes (*indicate your consent by checking the applicable box(es)*):

- ☐ to fundraise for the organization
- ☐ to notify me of new services or goods available at the [organization]
- ☐ to notify me of special events and opportunities at the [organization] (e.g. a seminar or conference)
- ☐ [add any other purposes that require express consent]

I understand that I can withdraw my consent at any time by contacting: [contact person].

I agree to [organization] collecting, using and disclosing personal health information about me as set out above and in the written statement.

Signature: _____ Printed Name: _____
Date: _____