

**Getting Ready for
Ontario's Privacy Legislation**

GUIDE

**Privacy Requirements and Policies for
Health Practitioners**

**PUBLISHED BY THE COLLEGE OF OPTICIANS OF ONTARIO
SEPTEMBER 2004**

This booklet is not intended to provide legal advice. It provides some practical suggestions for how some organizations can review their information handling practices and develop a Privacy Policy. The *Personal Information Protection and Electronic Documents Act* is unclear in a number of areas and is enforced by the federal Information and Privacy Commissioner. The *Personal Health Information Protection Act* is quite new and is detailed and complex and is enforced by the provincial Information and Privacy Commissioner. Thus, the descriptions provided below are based on current information and may change as experience with the legislation and its enforcement develops. Some provisions in the Acts are simplified for the purpose of identifying issues for consideration. For legal advice, please speak to your own lawyer.

Adapted from the work of:
Richard Steinecke
Steinecke Maciura LeBlanc
Barristers & Solicitors

Original Work Copyright © 2004 by Steinecke Maciura LeBlanc
Used with permission

INDEX

	PAGE
Executive Summary	4
Introduction - Purpose of This Guide	6
Step 1 – Designating Your Organization’s Information Officer	7
Step 2 – Information and Activities Covered by the Privacy Plan	9
Step 3 – Collecting Personal (Health) Information	11
Step 4 – Safeguards, Retention and Destruction	14
Step 5 – Access, Correction, Complaints and Openness	15
Step 6 – Implementing Your Privacy Plan	18

Personal Health Information Protection Act, 2004

A Supplementary Guide

Executive Summary

This Guide provides information on how the new Ontario *Personal Health Information Protection Act, 2004* (PHIPA) might affect the privacy practices of health care practitioners and facilities. PHIPA provides more detailed rules than the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). PHIPA also provides some additional flexibility in privacy practices for the health sector.

In essence PHIPA applies to any personal health information collected, used or disclosed by a custodian (i.e., health practitioners and facilities) regardless of whether the custodian engages in commercial activities. Practitioners who work for a health facility or health agency will generally be able to fit under their information practices. Each custodian must appoint an information officer, called a “contact person”.

PHIPA provides more workable consent procedures for the collection, use and disclosure of personal health information. Generally implied consent will be sufficient for the provision of health care. Practitioners can usually assume that a signed consent form relating to personal health information is valid. The rules for substituted consent for the handling of personal health information are very similar to those for substituted consent for treatment.

PHIPA also provides for more options for using and disclosing personal health information without the client’s consent. These include using the information for health care planning and delivery, risk management and education. Disclosure of personal health information can generally be made without consent to others on the health care team, to provide basic status reports on those admitted to facilities, to support families and friends of a deceased client, for audit and accreditation purposes, for serious safety issues and to successor custodians.

PHIPA requires that reasonable safeguards be taken to protect personal health information. Clients have the right to be advised of privacy breaches. Information Technology (IT) suppliers to custodians must comply with certain standards. However, with client consent, records can be reasonably stored at the client’s home or an off-site storage facility.

PHIPA also provides for a more health-specific system for client access and correction of their records. For example, access requests can be refused in respect of quality assurance information, for raw data from psychological tests and where there is a risk of significant harm to either the client or others. Correction requests can be declined for professional opinions and observations and, in many circumstances, where the record was provided by another custodian. In addition, custodians do not have to provide copies of corrected

records (or statements of disagreements) to those the custodian has previously disclosed the personal health information to as often as they would under PIPEDA.

PHIPA is enforced by the Ontario Information and Privacy Commissioner. The Commissioner has broad powers of investigation and can order a custodian to comply with their PHIPA obligations. Custodians are also subject to prosecution for breaches of PHIPA and to civil actions for damages, including a maximum of \$10,000 for mental anguish.

Most practitioners who have developed privacy policies to comply with PIPEDA will only have to make minor adjustments to them as a result of PHIPA.

Introduction - Purpose of This Guide

In 2003 the College joined with the Federation of Health Regulatory Colleges of Ontario to prepare a Guide to the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). The College's adaptation of the Guide is currently found on the College's website. In 2004 Ontario enacted the *Personal Health Information Protection Act, 2004* (PHIPA). PHIPA follows the same principles of PIPEDA. However, it provides much more specific guidance about the handling of personal health information. PHIPA also has some minor differences from PIPEDA. The purpose of this PHIPA Guide is to supplement the existing PIPEDA Guide so that practitioners can comply with both statutes.

It is anticipated that most practitioners who have developed privacy policies and procedures under PIPEDA will only have to make minor adjustments in order to also comply with PHIPA. This Guide follows the same format as the PIPEDA Guide, thus it should be easy to continue to use the PIPEDA Guide and its accompanying Checklist.

PHIPA comes into force on November 1, 2004. At the time of preparing this Guide, there are some proposed regulations for PHIPA under discussion. Those proposed regulations may be revised before they are enacted, so readers should be cautious about any changes that might result.

PHIPA is a provincial statute. PIPEDA is a federal statute. If there is any conflicts between the two statutes (in the sense that it is impossible to comply with both of them at the same time) PIPEDA is paramount. However, if it is possible to comply with both statutes at the same time, one should do so. The Ontario government anticipates that the federal government will deem PHIPA to be substantially similar to PIPEDA. If that occurs, then one will only have to comply with PHIPA in respect of personal health information in Ontario. One would still have to comply with PIPEDA in respect of other types (i.e., non-health) of personal information.

Throughout this Guide reference will be made to section numbers in brackets such as: "(ss. 3(1))". These are references to the provisions of the PHIPA unless otherwise indicated. The *Personal Health Information Protection Act, 2004* can be found at: www.e-laws.gov.on.ca/DBLaws/Statutes/English/04p03_e.htm. The *Personal Information Protection and Electronic Documents Act* can be found at: <http://lois.justice.gc.ca/en/P-8.6/index.html>.

The *Quality of Care Information Protection Act, 2004* 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 to sue them. This Guide does not deal with the *Quality of Care Information Protection Act, 2004*. A copy of that Act can be found at: www.e-laws.gov.on.ca/DBLaws/Statutes/English/04q03_e.htm.

Step 1 – Designating Your Organization’s Information Officer

(a) Identifying Your “Organization”

Under PHIPA, the basic organization is the “health information custodian”. Unlike PIPEDA, however, what constitutes the custodian is specifically described in the Act (s. 3) and is not left to the choice of the parties. PHIPA provides a list of custodians, including the following:

- health care practitioners, including all those registered under the *Regulated Health Professions Act*, naturopaths, registered social workers and social service workers, unregistered health care practitioners and unregistered persons operating a group health care practice,
- community service providers under the *Long Term Care Act*,
- community care access centres (CCAC’s), 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 an organizational custodian (i.e., 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 there are not competing custodians competing 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 CCAC’s a custodian can only have one physical site unless special permission is obtained from the Minister of Health and Long Term Care.

(b) Selecting Your Information Officer / Contact Person

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

Like PIPEDA, the information officer under PHIPA is responsible for ensuring that the custodian has a privacy policy (called “information practices”). However, PHIPA goes further and places an explicit duty on the custodian to follow its own information practices (s. 10).

The contact person shall 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,

- handle privacy complaints, and
- make available to the public the custodian's written information practices (ss. 15 and 16).

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 the use or disclosure.

Step 2 – Information and Activities Covered by the Privacy Plan

(a) Commercial Activities vs. Personal Health Information

PIPEDA applies principally to any personal information about an individual collected, used or disclosed in the course of a commercial activity. The approach taken in PHIPA is quite different. In essence, PHIPA applies to any collection, use or disclosure of personal health information by a health information custodian (s. 7). The scope of PHIPA is both narrower and broader than PIPEDA. The scope of PHIPA is narrower in the sense that it generally applies only to personal health information and not other sorts of personal information (e.g., financial information, conduct history, opinions and views, culture, race, etc.). However, the scope of PHIPA is also broader in that, for the most part, it does not matter whether the custodian is collecting, using or disclosing personal information for commercial purposes.

Thus it is important to know whether one is dealing with personal health information. Personal health information is very broadly defined (s. 4) and includes the following components:

- 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
 - i. physical or mental condition, including his or her family health history,
 - ii. health care (including maintenance, preventative or palliative measures),
 - iii. provider of health care service,
 - iv. payment for the health service including health card number,
 - v. substituted decision maker, or
 - vi. non-health care information (e.g., home contact information) mixed in with other personal health information.

PHIPA does not apply 120 years after collecting the information or 50 years after the death of the individual.

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

(b) Inventory of Personal Information Collected

The existing inventory is still valid except that it also contains personal non-health information (which would be covered by PIPEDA rather than PHIPA).

Step 3 – Collecting Personal (Health) Information

(a) Principles of Identifying Purposes and Obtaining Consent

Like PIPEDA, PHIPA generally requires consent for the collection, use and disclosure of personal health information (s. 29). One of the major differences between PIPEDA and PHIPA is that PHIPA provides specific guidance as to what constitutes a valid consent for the collection, use and disclosure of such information.

For example, under PHIPA implied consent is generally permitted where it is reasonable to assume that individual knows the purpose of the collection, use or disclose and their right to give or withhold consent. Practitioners and facilities can assume there is implied consent for the provision of health care. In addition, if the purposes are stated in a poster or brochure readily available and likely to be seen by the individual, one can assume the individual knows the purpose. One can even assume implied consent for disclosure to other custodians of personal health information for the purpose of providing health care. (s. 18-20, 33)

Express consent (verbal or written) is needed, however, to disclose personal health information to a non-custodian. Express consent is also needed to disclose personal health information to another custodian for purposes other than the provision of health care (e.g., research, marketing). (s. 18-20, 33)

Practitioners can assume that a written consent is valid unless provided with grounds to the contrary. (s. 18-20, 33)

Some recurring problem areas are also addressed by PHIPA. For example, a direction from a client not to record pertinent information is invalid (ss. 19(2)). Also, if a client directs that part of the file not be given to another custodian and the custodian feels that the other custodian needs the information, the disclosing custodian can advise the receiving custodian that some relevant information has been withheld at the direction of the client (ss. 20(3)).

PHIPA also provides greater flexibility for collecting 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 also 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 (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 also 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 privacy policy) is permitted in limited circumstances (e.g., one can only use the name and mailing address for a charitable purpose 60 days or more after discharge from a facility with an easy opt out process and the fundraising request must not reveal anything about the individual's health) (s. 32 of the Act and s. 9 of the proposed 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. Regulations can be made respecting fees for collecting, using and disclosing personal health information, but none have been proposed to date (s. 35).

(b) Primary Purpose and Consent / Other Legal Authority Checklist

These checklists are still applicable. Keep in mind that the checklist covers both personal health information (covered by PHIPA) and other types of personal information (covered by PIPEDA for commercial activities).

(c) Related and Secondary Purposes Checklists

For the most part these checklists are still applicable. It may not be necessary to obtain express consent for disclosure to a successor of the custodian because PHIPA permits this to occur without consent (s. 42). Similarly and as discussed below, use and some disclosure of the information for quality assurance and billing purposes may also not require express consent.

(d) Principles of Use and Disclosure

PHIPA also provides a bit more flexibility than PIPEDA 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 greater flexibility than PIPEDA 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,

- confirming 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 another 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* and the *Substitute Decisions Act*,
- to a health regulatory College,
- in order to cooperate with a statutorily authorized inspection, investigation or similar proceeding,
- in some research situations,
- in some health planning and management purposes,
- to assist in the monitoring of public health funding,
- to a health data institute under various rules and restrictions, and
- if permitted by law (not just if 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 received the information while investigating a complaint, the College could then use that same information for prosecuting 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).

Step 4 – Safeguards, Retention and Destruction

(a) 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)). However, one difference from PIPEDA is that under PHIPA there is a positive obligation to notify affected individuals of a privacy breach (ss. 12(2)).

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 for Information Technology (IT) suppliers to custodians. IT suppliers must only use personal health information for the purpose of providing its services to the custodians. They must also provide the following:

- disclosure 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 (s. 10 of PHIPA and s. 6 of the proposed regulations).

(b) Retention and Destruction of Personal Information

Personal health information must be disposed of with reasonable security (s. 12).

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)). This provision is more specific than PIPEDA.

Step 5 – Access, Correction, Complaints and Openness

(a) Access Rights

Like PIPEDA, PHIPA provides a broad right of access to the personal health information held by a custodian on an individual. However, PHIPA provides some additional 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,
- 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 also provides some additional 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 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, and
- the custodian can only charge a reasonable cost recovery fee for access and must provide an estimate of the fee in advance (s. 53-54).

(b) Correction Rights

Like PIPEDA, PHIPA provides for a broad right of individuals to correct errors in their records (s. 55). However, PHIPA provides additional 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 also provides some additional 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 about the refusal (s. 55).

PHIPA also places some limits on the duty of custodians to notify others who have received the incorrect or disputed information. Those limits include the following:

- the individual must request it,
- 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.

(c) Complaints System

Like PIPEDA, PHIPA does not provide much detail about the nature of the custodian's internal complaints system; it simply has to have one (s. 16).

PHIPA does, however, provide detailed provisions for an external complaints system involving the Information and Privacy Commissioner of Ontario. The PHIPA external complaint system is stronger than the PIPEDA one. For example, 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 (e.g., the College) (ss. 61(3)). Where an order is made, the individual can sue in court for actual damages and up to \$10,000 of mental anguish (s. 65).

PHIPA also provides more comprehensive whistle-blowing protections than PIPEDA. It also provides 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 more offences for deliberately breaching the Act than PIPEDA does (s. 72). For example, wilfully collecting, using or disclosing personal health information contrary to the Act is an offence. So is the insecure disposal of such information (e.g., throwing documents in the blue box without first shredding it).

(d) Openness

PHIPA has similar provisions to PIPEDA in respect of ensuring publicly available access to the custodian's privacy policies / information practices.

Step 6 – Implementing Your Privacy Plan

Most of the provisions of existing privacy policies / information practices that comply with PIPEDA should be sufficient under PHIPA as well. However, practitioners should review this Guide and identify changes that might have to be made. Some examples of likely areas in which updating will be required include the following:

- Describing when implied consent will be relied upon (if it is not already adequately covered),
- Outlining substituted consent procedures, where applicable,
- Providing for the notification of affected individuals of a privacy breach (ss. 12(2)),
- Ensuring that all of the practitioner’s usual uses and disclosures of personal health information are mentioned in their privacy policy to avoid the added duties under ss. 16(2) of PHIPA (e.g., duty to inform individual of the use or disclosure), and
- Alluding to the additional exceptions and grounds for refusal to the individual’s access and correction rights that would most commonly apply in the particular practice or facility.

In addition, some practitioners may wish to change some of the terminology in their documents to conform with the PHIPA language (e.g., “privacy policy” becomes “information practices” and “privacy officer / information officer” becomes “contact person”). However, those changes are clearly optional.