

# 5 EASY STEPS

## The Guide for Dentists to Implement Ontario Health Privacy Requirements and Policies

OCTOBER 2004



Royal College of  
Dental Surgeons of Ontario

*Ensuring Continued Trust*

## About this Guide

This Guide is not intended to provide legal advice. It provides practical suggestions for how dentists can review their information handling practices and develop a Privacy Policy.

The descriptions provided in this Guide are based on current information and may change as experience with the legislation and its enforcement and regulations develop. 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* (PHIPA) is quite new and is detailed and complex. It is enforced by the Ontario Information and Privacy Commissioner.

This Guide is not intended to provide a comprehensive explanation of PHIPA. Accordingly, some provisions in these Acts are simplified for the purpose of identifying issues for consideration. For further clarification, do not hesitate to contact the College.

The College is grateful to the Federation of Health Regulatory Colleges of Ontario and Richard Steinecke for their contributions to this Guide on Ontario health privacy legislation.



Royal College of  
Dental Surgeons of Ontario

*Ensuring Continued Trust*

6 Crescent Road  
Toronto, ON M4W 1T1

We hope this Guide makes the transition straightforward. However, questions always come up. Do not hesitate to get in touch with any of the following College staff for help.

**Dr. Robert Carroll**  
*Manager, Professional Practice*  
phone: 416-934-5611  
toll-free: 1-800-565-4591  
e-mail: rcarroll@rcdso.org

**Dr. Lesia Waschuk**  
*Practice Advisor*  
phone: 416-961-6555, ext. 3348  
toll-free: 1-800-565-4591  
e-mail: lwaschuk@rcdso.org

**Dayna Simon**  
*Assistant to the Registrar, Legal*  
phone: 416-934-5618  
toll-free: 1-800-565-4591  
e-mail: dsimon@rcdso.org

**Irwin Fefergrad**  
*Registrar*  
phone: 416-934-5625  
toll-free: 1-800-565-4591  
e-mail: ifefergrad@rcdso.org

*Supplement to RCDSO DISPATCH  
October/November 2004*

# Made-In-Ontario Health Privacy Legislation

## A MESSAGE FROM IRWIN FEFERGRAD • REGISTRAR

Welcome to health privacy in Ontario! Ontario's new *Personal Health Information Protection Act, 2004*, (PHIPA) comes into force on November 1, 2004.

Rest assured that all of your hard work has not been in vain. The transition to the Ontario health privacy regime should be virtually seamless.

It is anticipated that dentists who have developed privacy policies under the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), following the College's recommendations, will only have to make minor adjustments to comply with PHIPA.

The purpose of this Guide to the new provincial health privacy legislation is to supplement the existing College tool kit on the federal privacy legislation (PIPEDA) that you received in 2003, so that you will be able to comply with both statutes.

In fact, compliance with the Ontario legislation should be even easier since it was designed specifically to address the unique needs of the health-care field.

Compliance is made simple by following the Guide's 5 easy steps – and if you complied with the federal legislation, you've already done some of them.

1. Appoint a Privacy Information Officer and post a Privacy Statement.
2. Understand collection, use, and disclosure of personal health information.
3. Obtain knowledgeable consent.
4. Implement safeguards, retention, and destruction.
5. Address requests for access, correction, and the complaints system.

This Guide provides information in 5 easy steps on how the new Ontario *Personal Health Information Protection Act, 2004*, (PHIPA) might affect the privacy practices of dentists in Ontario.

In addition, we have included other tools:

- A poster that you may wish to use in your office. It has the support of the staff at the office of the Information and Privacy Commission.
- There is also a checklist from the Ministry of Health and Long-Term Care that helps you double-check that everything is in place in your office.

# What's New with this Ontario Health Privacy Legislation?

Ontario's *Personal Health Information Protection Act, 2004*, (PHIPA) comes into force on November 1, 2004. Generally, PHIPA follows the same principles as the federal privacy legislation *Personal Information Protection and Electronic Documents Act* (PIPEDA).

However, it provides more specific guidance about the handling of personal health information. PHIPA also has some minor differences from PIPEDA.

The Ontario government anticipates that the federal government will deem PHIPA to be substantially similar to PIPEDA. If that occurs, dentists will only have to comply with PHIPA in respect to personal health information in Ontario.

Dentists and health profession corporations (HPC) would still have to comply with PIPEDA in respect to other types of personal information that is non-health information.

In the meantime, dentists should comply with both the federal and provincial Acts.

PHIPA is helpful to health-care providers in that it provides more detailed rules than the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) and eliminates a lot of ambiguity that existed under PIPEDA.

Under PHIPA, dentists are designated as health information custodians, or as they are simply called, custodians.

PHIPA applies to any personal health information collected, used or disclosed by a custodian, regardless as to whether the custodian engages in commercial activities.

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 and communication with other health-care providers.

Dentists can assume that a signed consent form relating to personal health information is valid, such as the one you may have used under PIPEDA.

PHIPA also provides more options for using and disclosing personal health information without the patient's consent. These limited exceptions to consent include using the information for health-care planning and delivery, risk management, delivery to the College, education, for serious safety issues, and to successor custodians.

Like PIPEDA, PHIPA requires that reasonable safeguards must be taken to protect personal health information. Each custodian must appoint an information officer, called a contact person, whose duties are the same as the privacy officer designated under PIPEDA.

One new feature is that patients have the right to be advised of privacy breaches.

PHIPA also provides a more health-specific system for client access and correction of records. Dentists may deny correction requests of professional opinions or observations.

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 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.

When this Guide was prepared, there were some proposed regulations for PHIPA under discussion. Of course, the College will keep you informed of these developments and of any changes that might result.

The *Quality of Care Information Protection Act, 2004*, was enacted by the provincial government at the same time as PHIPA. Its purpose is to protect practitioners or facilities engaging in or co-operating 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*. If you are interested, this Act can be accessed on the College's Web site.

As a final note, throughout this Guide reference is made to section numbers in brackets such as (ss. 3(1)). These are references to the provisions of PHIPA, unless otherwise indicated. Links to the provincial and federal legislation can be found on the College's Web site at [www.rcdso.org](http://www.rcdso.org).

# STEP 1

## Appoint a Privacy Information Officer and Post a Privacy Statement

Under PHIPA, dentists and other health-care practitioners are designated as custodians.

Custodians must appoint a privacy information officer, called the contact person under PHIPA (s. 15). The College strongly suggests that this person be a dentist in the office.

Like PIPEDA, the information officer under PHIPA is responsible for ensuring that the custodian has privacy policies in place and a written public statement about their privacy practices. It is advisable to post this public statement in your office and have extra copies available upon request.

You can use the privacy code already in place under PIPEDA. In addition, you should post the enclosed privacy poster in a visible place in your office. The poster is on the back cover of this Guide and can be easily detached for posting in your office.

Under PHIPA, the contact person shall:

- 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;
- make available to the public the written information practices (s. 15 and 16).

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. In this situation, the facility would be the custodian and the individual dentist would be an agent of the custodian. Specific rules are set out in PHIPA for agents of custodians (s. 17).

As a custodian, it is important to identify your agents, if any, and educate them of their duties under PHIPA.

# STEP 2

## Understand Collection, Use, and Disclosure of Personal Health Information

As you know, 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 custodian (s. 7).

As a dentist, it is important to know when you are dealing with personal health information. Personal health information is 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 to then identify the individual.
- It can be in oral or recorded format.
- It relates to the individual's
  - physical or mental condition, including his/her family health history;
  - health care, including maintenance, preventative or palliative measures;
  - provider of health-care service;
  - payment for the health service, including health card number;
  - substitute decision-maker;
  - 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. (s. 9)

PHIPA is usually paramount over any inconsistent provincial statute (ss. 7(2)(3)). However, PHIPA has a number of exceptions within it. For example, PHIPA is not intended to interfere with the regulatory activities of the College (ss. (9)(2)(e)).

# STEP 3

## Obtain Knowledgeable Consent

### **Using a Poster to Identify Purposes and Obtain 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 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 an individual knows the purpose of the collection, use or disclosure, and his/her right to give or withhold consent.

Practitioners and facilities can assume there is implied consent for disclosing information to another custodian for the provision of health care unless you are told otherwise (s. 18-20).

The office of the Information and Privacy Commissioner of Ontario advised the College that signed consent is still the best. Accordingly, if you wish to continue using a signed consent form, as you did under PIPEDA, feel free to do so.

However, PHIPA states that if the purposes of collection, use, and disclosure of personal information are stated in a poster or brochure that is readily available, and likely to be seen by the individual, one can assume the individual knows the purposes (ss. 18(6)).

Enclosed for your convenience is a poster to display prominently in your dental office. The poster is on the back cover of this Guide and can be easily detached along the perforation and hung in your office.

There is one additional step to obtain knowledgeable consent according to the advice the College received from the Commissioner's office. You must ensure that the poster is brought to the attention of your patients so that they can read it. Once the poster has specifically been brought to a patient's attention, dentists are advised to have any discussion necessary with the patient and to note the consent in the patient's chart.

Express consent (verbal or written) is needed, however, to disclose personal health information to a non-custodian, such as an insurance carrier. 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 or marketing (s. 18-20, 33).

Practitioners can assume that previously written consent is valid, unless provided with information grounds to the contrary. (s. 1-20). So, if you used the College's template consent form under PIPEDA, you can assume it is valid and you do not need to obtain a new one.

### **Understanding the Lock Box Provisions**

Some typically tricky issues regarding consent have been addressed by PHIPA. For example, a direction from a patient not to record pertinent health information is invalid (ss. 19(2)).

However, if a patient directs that part of his/her chart is not to be given to another custodian, and the dentist feels that the other custodian needs the information, the dentist can advise the receiving custodian that some relevant information has been withheld at the direction of the patient (ss. 20(3)). This is referred to as a lock box provision.

### **Be Familiar with Rules for Substituted Consent**

PHIPA also provides detailed rules for obtaining substitute consent where the individual is not capable of understanding the information issue or appreciating its reasonably

foreseeable consequences. The rules for substitute consent are similar to those for treatment of incapable persons and are set out in detail in PHIPA.

One can presume an individual is capable until it becomes apparent that he/she is not capable (s. 21). The substitute decision-maker for handling of treatment information issues is generally the same as the substitute decision-maker for treatment decisions. If the information issue is not related directly to treatment, the list of substitute decision-makers is 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/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/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)).

#### **Understand Principles of Use and Disclosure of Personal Health Information**

PHIPA 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 the purpose of planning or delivering programs, risk management, educating practitioners, and in some research situations (ss. 37(1)).

Similarly, PHIPA (ss. 38-47) provides greater flexibility than PIPEDA for the disclosure of personal health information without consent, including disclosure:

- to other practitioners or facilities for the provision of health care when it is not reasonably possible to obtain consent in a timely manner;
- 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;
- with respect to a deceased individual for the purpose of identifying him/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 reasonable effect must be made to notify affected individuals 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 co-operate with a statutorily authorized inspection, investigation or similar proceeding;
- in some research situations;
- for 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;
- if permitted by law, not just if required by law.

PHIPA also provides rules for disclosure of personal health information outside of Ontario (s. 50).

# STEP 4

## Implement Safeguards, Retention, and Destruction

### **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)). If this happens, you may want to contact the College for advice as to how to fulfill this requirement.

Records can be kept off-site with consent of the patient if it is done reasonably and in accordance with professional standards, such as the College's Guidelines on Dental Recordkeeping (s. 14).

Dentists should ensure that confidentiality agreements are in place with non-custodians who may have access to patient health information, including bookkeepers, landlords, cleaning staff, and ensure that you have seen their own written privacy policies.

Feel free to use and modify the template (Form D/Confidentiality Agreement With Independent Contractors and Suppliers) provided to you by the College in the 2003 federal privacy compliance tool kit. If acceptable agreements are already in place, you do not need to enter into new ones. PHIPA sets out specific rules for access given to information technology suppliers (s. 10 of PHIPA and s. 6 of the proposed regulations).

### **Retention and Destruction of Personal Information**

Personal health information should be securely retained in accordance with College Guidelines and must be disposed of with reasonable security (s. 12) and in compliance with the College's Guidelines.

# STEP 5

## Addressing Requests for Access, Correction, and the Complaints System

### **Access Rights**

Like PIPEDA, PHIPA provides a broad right of access to the personal health information held by a custodian about 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.
- It is raw data from standardized psychological tests or assessments.
- Information was collected or created for a proceeding or during an inspection or investigation.
- There is a risk of serious harm to the treatment or recovery of the individual or of serious bodily harm to another person.
- Access would reveal the identity of a confidential source of information (s. 51-52).
- A legal privilege restricting disclosure applies. In these circumstances, the part of the record to which the exception applies should be severed and access can be provided to the rest of the record.

PHIPA also provides 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, he/she 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/her right to complain to the Information and Privacy Commissioner if the request for access is refused (along with the reasons for the refusal). 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 himself/herself of the identity of the individual before granting him/her access.
- The custodian can only charge a reasonable cost recovery fee for access and must provide an estimate of the fee in advance (ss. 54(10)).

### **Correction Rights**

Like PIPEDA, PHIPA provides for a broad right of individuals to seek to correct errors in their records (s. 55). In general, the custodian is obligated to correct a record he/she created if the record is not accurate or complete. However, PHIPA provides additional grounds for refusing such requests:

- where the request is frivolous, vexatious or made in bad faith (ss. 55(6));
- where the custodian did not create the record and the custodian does not have sufficient knowledge, expertise or authority to make the correction (ss. 55(9)(a));

- where the information consists of a professional opinion or observation, such as a diagnosis, made in good faith (ss. 55(9)(b)).

PHIPA also provides additional procedures for handling correction requests including the following:

- While the custodian can informally make the correction, he/she can also insist upon a formal written request.
- In accordance with College Guidelines, the correction should not obliterate the original entry (ss. 55 (10)).
- Any notice of refusal must advise the individual of his/her right to include a concise statement of disagreement in the record and of his/her right to complain to the Information and Privacy Commissioner (ss. 55 (11)).

PHIPA also places 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.
- 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.

### **Complaints System**

Like PIPEDA, PHIPA does not provide much detail about the nature of the custodian's internal complaints system. The custodian 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 one for PIPEDA. 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)(a)). Where an order is made by the Commissioner, the individual can sue for actual damages and up to \$10,000 for mental anguish (s. 65).

PHIPA also creates 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. As is the insecure disposal of such information e.g., throwing documents in the blue box without first shredding them. Individuals may be fined up to \$50,000 and corporations/organizations may be fined up to \$250,000 if they are found guilty of an offence under PHIPA.

PHIPA has similar provisions to PIPEDA with respect to ensuring publicly available access to the custodian's privacy policies/information practices. This means that you do not have to hand each patient your written privacy policy but it must be available upon request. A good idea is to post a copy in the waiting room and keep extra copies at the reception desk.

# SUMMARY

Most of the provisions of existing privacy policies/information practices that comply with PIPEDA will be sufficient under PHIPA as well. However, practitioners should review this Guide and identify changes that might need to be made.

Some examples of likely areas in which updating will be required include:

- describing when implied consent will be relied upon, if it is not already adequately covered;
- outlining substitute consent procedures, where applicable;
- providing for notification of affected individuals of a privacy breach (ss. 12(2));
- providing for lock box requests;
- ensuring that all of the practitioner's usual uses and disclosures of personal health information are mentioned in their privacy policy;
- alluding to the additional exceptions and grounds for refusal to the individual's access and correction rights that would most commonly apply in a dental practice.

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, these changes are optional.

Further information, questions and answers about the legislation, updates, and Web links to the legislation, Ministry of Health and Long-Term Care, and the Office of the Ontario Information and Privacy Commissioner are available on the College Web site at [www.rcdso.org](http://www.rcdso.org).

If you have any questions regarding this easy implementation strategy or about the legislation, please do not hesitate to contact the College:

**Dr. Robert Carroll**

*Manager, Professional Practice*

phone: 416-934-5611  
toll-free: 1-800-565-4591  
e-mail: [rcarroll@rcdso.org](mailto:rcarroll@rcdso.org)

**Dr. Lesia Waschuk**

*Practice Advisor*

phone: 416-961-6555, ext. 3348  
toll-free: 1-800-565-4591  
e-mail: [lwaschuk@rcdso.org](mailto:lwaschuk@rcdso.org)

**Dayna Simon**

*Assistant to the Registrar, Legal*

phone: 416-934-5618  
toll-free: 1-800-565-4591  
e-mail: [dsimon@rcdso.org](mailto:dsimon@rcdso.org)

**Irwin Fefergrad**

*Registrar*

phone: 416-934-5625  
toll-free: 1-800-565-4591  
e-mail: [ifefergrad@rcdso.org](mailto:ifefergrad@rcdso.org)

# CHECKLIST

The *Personal Health Information Protection Act, 2004*, will come into force on November 1, 2004. To be ready for that date, consider whether you have fulfilled these preliminary requirements for health information custodians under the Act.

The Ministry of Health and Long-Term Care has issued this helpful checklist.

## Health information custodians are required to:

- Put in place information practices, as defined in subsection 2(1), that comply with the Act and regulations [s. 10(1)].
- Prepare and make available a written public statement about the custodian's information practices that fulfills the requirements of the Act [s. 16 (1)].
- Prepare a notice to post or make available describing the purposes of the custodian's collections, uses, and disclosures of personal health information. This is required where the custodian intends to rely on subsection 18(6) of the Act.
- Designate a contact person to perform the functions set out in the Act. This is unnecessary if the custodian is a "natural person", for example an individual health-care practitioner, and is acting as the contact person. [s. 15(2)]
- Ensure that employees and all other agents of the custodian are appropriately informed of their duties under the Act [s. 15(3)].
- Take reasonable steps to ensure personal health information in the custodian's custody or control is protected against theft, loss, unauthorized use, disclosure, copying, modification, and disposal [s. 12(1)].
- Ensure that personal health information records in the custodian's custody or control are retained, transferred, and disposed of in a secure manner and in accordance with the regulations, if any [s. 13(1)].

For more details, please refer to the *Personal Health Information Protection Act, 2004*, and any regulations made under the Act.

# HOW OUR OFFICE COLLECTS, USES AND DISCLOSES PATIENTS' PERSONAL INFORMATION

Our office understands the importance of protecting your personal information. To help you understand how we are doing that, we have outlined below how our office is collecting, using and disclosing your personal information.

This office will collect, use and disclose information about you for the following purposes:

- To assess your health needs and provide safe and efficient dental care.
- To enable us to contact and maintain communication with you to distribute health-care information and to book and confirm appointments.
- To communicate with other treating health-care providers, including other dentists, physicians, pharmacists and lab technicians.
- For teaching and demonstrating purposes on an anonymous basis.
- To complete and submit dental claims for third party adjudication and payment.
- To comply with legal and regulatory requirements.
- To deliver your charts and records to the dentist's insurance carrier to enable the insurance company to assess liability and quantify damages, as necessary.
- To invoice for goods and services.
- To process credit card payments.
- To collect unpaid accounts.

Thank you for your support and understanding in helping our office to comply with all regulatory requirements, and generally with the law.