COLLEGE OF DENTURISTS OF ONTARIO

# Guide to the Standard of Practice: Confidentiality and Privacy

## What You Need to Know About Privacy Law: An Overview of the *Personal Health Information Protection Act, 2004*[1]

### What privacy laws govern my practice?

All regulated health professionals in Ontario need to comply with the *Personal Health Information Protection Act, 2004* ("**PHIPA**").[2]

If you engage in **commercial activities** involving the collection, use or disclosure of personal information **outside of Ontario**, then you will also need to comply with the federal *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**").[3] PIPEDA may also apply if you collect, use or disclose information that is personal, but not health information, in the course of commercial activities in Ontario.

Health professionals also need to comply with Canada's anti-spam legislation, which requires consent to send electronic messages of a commercial nature.[4]

### What information is protected under PHIPA?

PHIPA protects **personal health information**. Personal health information is defined as information that can identify an individual (or can be combined with other information to identify an individual) and 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.

Personal health information can be either oral or recorded (in written or electronic form). PHIPA also covers mixed records that contain both personal health information and other non-health identifying information about an individual (for example, a record that contains an individual's home address, telephone number and health history).

---

[1] By Erica Richler. Original Work Copyright © 2016 by Steinecke Maciura LeBlanc. This document is intended as a general overview of the *Personal Health Information Protection Act, 2004* for regulated health professionals in Ontario. This is not intended to provide legal advice. For legal advice, please speak to a lawyer.

[2] S.O. 2004, c. 3, Schedule A, available online: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm.

[3] S.C. 2000, c. 5, available online: http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

[4] For more information on Canada's anti-spam legislation see: http://fightspam.gc.ca/eic/site/030.nsf/eng/home

## What are a Denturist's obligations under PHIPA?

The main obligations under PHIPA include:

- to obtain **consent** to collect, use or disclose an individual's personal health information (except in the ,limited situations discussed below);
- to maintain **security** over personal health information by taking reasonable steps to protect against theft, loss and unauthorized use or disclosure (this includes maintaining security on electronic devices, for example by encrypting data);
- to ensure the **accuracy** of personal health information;
- to collect, use, or disclose only as much personal health information as is necessary in the circumstances;
- to provide individuals with **access** to their personal health information upon request (except in limited situations, including where the information was created primarily for use in a legal proceeding or where providing access could result in a risk of serious harm); and
- to **correct** personal health information if the record is incomplete or inaccurate (except where one is not in a position to correct the information in a record created by another custodian or if the information consists of professional opinion or observation made in good faith).

## What is the Difference Between a Health Information Custodian or an Agent?

Health professionals have different levels of responsibility depending on whether they are the **health information custodian** or an **agent**. If you are a regulated health professional or you operate a group practice, and you have custody and control of personal health information in connection with your duties, then you are a health information custodian for purposes of PHIPA. However, even if you fall under the definition of a health information custodian, if you work for or on behalf of another custodian (such as another regulated health professional, a group practice or a hospital), then you are considered to be an agent of that health information custodian.

A health information custodian is **ultimately responsible** for the personal health information in his or her custody or control, but may permit an agent to collect, use, disclose, retain or dispose of the information if certain requirements are met. The agent must ensure that the collection, use, disclosure, retention or disposal of the information is permitted by the custodian, is necessary for purposes of carrying out the agent's duties, is not contrary to law and complies with any specific restrictions imposed by the custodian.[5]

**Health information custodians** have these additional administrative duties:

- to develop and comply with policies (known as "**information practices**") with respect to:
    - when, how and the purposes for which the custodian routinely collects, uses, modifies, discloses, retains or disposes of personal health information; and
    - the administrative, technical and physical safeguards and practices that the custodian maintains with respect to personal health information.
- to designate a **contact person** to:
    - facilitate the custodian's compliance with PHIPA;
    - ensure that all agents are informed of their duties under PHIPA;
    - respond to public inquiries about the custodian's policies;
    - respond to requests for access or correction; and

[5] See PHIPA, section 17.



365 Bloor Street East, Suite 1606, Toronto, ON M4W 3L4 • T: 416-925-6331 • F: 416-925-6332 • TF: 1-888-236-4326
Email: info@denturists-cdo.com • Website: www.denturists-cdo.com

- receive public complaints about alleged privacy breaches.

- to display or make available a **written public statement** that:
  - provides a general description of the custodian's privacy policies (including the purposes for which personal health information is collected, used and disclosed);
  - describes how to contact the contact person or the custodian;
  - describes how an individual can seek access to or correction of a record; and
  - describes how an individual can make a complaint to the custodian and to the Information and Privacy Commissioner of Ontario.
  - Health information custodians must also notify the individual about whom the information relates if the individual's personal health information is used or disclosed in a manner that is outside the scope of the description set out in the written public statement.
- to establish and monitor an electronic audit log to prevent privacy breaches and snooping.

## What is an electronic audit log? What do I have to keep in this log?

Health Information Custodians will be required to establish and monitor an audit log for any electronic health records to record who accesses which parts of which client's records when, so as to prevent snooping or other privacy breaches.

The electronic audit log must include, for every instance in which a record or part of a record of personal health information that is accessible by electronic means is viewed, handled, modified or otherwise dealt with,

(a) the type of information that was viewed, handled, modified or otherwise dealt with;
(b) the date and time on which the information was viewed, handled, modified or otherwise dealt with;
(c) the identity of all persons who viewed, handled, modified or otherwise dealt with the personal health information;
(d) the identity of the individual to whom the personal health information relates; and
(e) any other information that may be prescribed.

## Do I need to obtain express consent from the individual in every situation?

No, PHIPA provides that consent may be express or implied. **Express consent** is required where personal health information is disclosed to a person who is <u>not</u> a health information custodian (such as an insurance company) or it is <u>not</u> disclosed for the purpose of providing health care. Express consent is also required for certain fundraising, marketing and market research activities.[6]

In other situations, **implied consent** is sometimes sufficient. For example, when a patient answers questions about his or her health history – in a context where it is obvious that the information will be used to assess and treat the patient – a health professional can infer consent to collect that information.

Importantly, health professionals 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;

[6] See PHIPA, sections 32-33.



365 Bloor Street East, Suite 1606, Toronto, ON M4W 3L4 • T: 416-925-6331 • F: 416-925-6332 • TF: 1-888-236-4326
Email: info@denturists-cdo.com • Website: www.denturists-cdo.com

- if information is being disclosed, it must only be disclosed to another health information custodian; and
- the individual has not withheld or withdrawn consent.[7]

This is commonly referred to as sharing personal health information within the **circle of care**.[8]

In addition, there are limited exceptions where personal health information can be collected, used or disclosed **without consent**. For example, consent is not required in the following circumstances:

- to collect personal health information from an individual, even if the individual is incapable of consenting, if it is reasonably necessary to provide health care and consent cannot be obtained in a timely manner;
- to disclose personal health information about an individual if the custodian believes on reasonable grounds that disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm;
- to disclose personal health information in the context of a legal proceeding if the custodian or agent is a party or witness; or
- to disclose personal health information to a regulatory College (for example, in the context of an investigation of a complaint).[9]

## What should I do if there has been a privacy breach?

If personal health information has been stolen or lost or if it has been used or disclosed without authority (this includes the unauthorized viewing of health records):

- The health information custodian must notify the **individual** about whom the information relates at the first reasonable opportunity. The notice has to inform the individual that he or she is entitled to make a complaint to the Information and Privacy Commissioner of Ontario.
- As of October 1, 2017, in serious situations the health information custodians will also have to notify the Commissioner immediately. The Commissioner also needs to be notified of all privacy breaches in an annual report filed with the Commissioner's office.
- An agent that handled the information must notify the responsible health information custodian at the first reasonable opportunity.

Health information custodians have additional reporting obligations to **regulatory Colleges** (which include the Colleges under the *Regulated Health Professions Act, 1991* and the Ontario College of Social Workers and Social Service Workers) if the custodian takes disciplinary action against a member of a College for the unauthorized collection, use, disclosure, retention or disposal of personal health information.

## What are the situations where I must notify the Commissioner of a privacy breach?

As a custodian, you must report breaches to the Commissioner in seven categories described in the regulation and summarized by the IPC here. The categories are not mutually exclusive; more than one can apply to a single privacy breach. If at least one of the situations applies, you must report it.

1. Use or disclosure without authority
2. Stolen information

[7] For more information about your obligations when an individual withholds or withdraws consent, 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
[8] For more information on the exchange of information within the circle of care, see the Information and Privacy Commissioner's Guideline "Circle of Care: Sharing Personal Health Information for Health-Care Purposes", available online: http://www.ipc.on.ca/images/Resources/circle-care.pdf
[9] Health professionals should refer to PHIPA (in particular, sections 29-50) for a full listing of the exceptions to obtaining consent.



365 Bloor Street East, Suite 1606, Toronto, ON M4W 3L4 • T: 416-925-6331 • F: 416-925-6332 • TF: 1-888-236-4326
Email: info@denturists-cdo.com • Website: www.denturists-cdo.com

3. Further use or disclosure without authority after a breach
4. Pattern of similar breaches
5. Disciplinary action against a College Member
6. Disciplinary action against a Non-College Member
7. Significant breach

## What are the consequences of failing to comply with PHIPA?

If a health professional fails to comply with PHIPA, an individual may make a complaint to the organization's contact person (or directly to the custodian if there is no contact person), to the Information and Privacy Commissioner of Ontario or to the relevant regulatory College.

The Information and Privacy Commissioner can review complaints and order members to comply with PHIPA. The affected individual may also commence a civil action for damages.

Depending on the circumstances, a complaint to the College may result in a referral of allegations of professional misconduct to the Discipline Committee.

If a health professional's contravention of PHIPA was deliberate, he or she may be guilty of an offence, punishable by a fine of up to $200,000.

## When does PIPEDA apply to me?

Denturists may need to comply with PIPEDA if they engage in the following types of activities:

- commercial activities involving the collection, use or disclosure of personal information outside of Ontario (for example, if a denturist offers an online seminar to denturists across Canada for a fee, the denturist would have to comply with PIPEDA with respect to the personal information collected from the participants, such as their home address and credit card information); or
- commercial activities involving the collection of personal information that is not health information (for example, if a denturist collects a home address and credit card number to process a sale of a product or device that is unrelated to their duties as a denturist).

## Does Canada's Anti-spam Legislation Apply to Me? When?

Denturists need to comply with Canada's Anti-Spam Legislation ("CASL") if they send commercial electronic messages, such as emails and text messages, that are intended to encourage participation in a commercial activity (even if there is no expectation of profit). For example, this may apply to emails to patients or potential patients about new products or services, or electronic messages notifying patients of appointments. If denturists send these kinds of electronic messages, they must comply with the requirements of CASL, including obtaining consent and offering an unsubscribe option.

## Other Resources

The **Information and Privacy Commissioner of Ontario** website provides access to numerous monographs and fact sheets dealing with specific topics related to the *Personal Health Information Act.*
https://www.ipc.on.ca/?redirect=https://www.ipc.on.ca/

"Canada's Anti-Spam Legislation", Government of Canada:
http://fightspam.gc.ca

Report a Privacy Breach:
https://www.ipc.on.ca/health-organizations/report-a-privacy-breach/



365 Bloor Street East, Suite 1606, Toronto, ON M4W 3L4 • T: 416-925-6331 • F: 416-925-6332 • TF: 1-888-236-4326
Email: info@denturists-cdo.com • Website: www.denturists-cdo.com