College of Dietitians of Ontario

Privacy of Personal Information

Dietetic Practice Tool Kit

for Registered Dietitians in Ontario

Updated July 2016

Contents

Introduction - Purpose of This Guide

There are two laws dealing with the protection of personal information:

- PHIPA (Provincial Law) – The *Personal Health Information Protection Act, 2004*, is Ontario legislation. It provides a consistent set of rules for the collection, use, disclosure and security of personal health information for custodians of health care information in Ontario.

- PIPEDA (Federal Law) – The *Personal Information Protection and Electronic Documents Act, 2000,* is Federal legislation that applies to commercial activities involving the collection, use and disclosure of personal information outside of the province of Ontario within Canada.

This Guide addresses PHIPA only as it is the primary law that governs the handling of personal information by health professionals. However, RDs 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).

The intention of this guide is to provide direction for RDs in Ontario on how to comply with PHIPA. It is not intended to provide legal advice. For legal advice, please speak to a lawyer.

This Privacy of Personal Information Practice Toolkit is a critical resource for:

a) RDs who are involved in developing or modifying their organization's personal health information privacy policies in keeping with PHIPA;
b) RDs in administrative roles who participate in the development of their organizational personal health information policies and procedures; and
c) RDs in private practice who act as Health Information Custodians to comply with the requirements set out in PHIPA.

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 to the resources that may be available in larger organizations.

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

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

court-created obligation protecting individuals from an "intrusion into their seclusion."[2] Health professionals also need to comply with Canada's anti-spam legislation if they send electronic messages of a commercial nature.[3]

PHIPA was amended in 2016 to add a framework for a province-wide system of electronic health records. As of the time of writing this Guide, those provisions are not yet in force.[4]

The *Quality of Care Information Protection Act, 2004*[5] was enacted at the same time as PHIPA. When PHIPA was amended in 2016, a new *Quality of Care Information Protection Act, 2016* was passed, but as of the date of this Guide it has not yet been proclaimed into force. The purpose of this legislation is to allow health practitioners and facilities to engage in confidential formal quality improvement discussions without fear of retaliation. This Guide does not deal with the *Quality of Care Information Protection Act, 2004*.

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, nutritional 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(s));
- 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).

[2] *Jones v. Tsige*, 2012 ONCA 32
[3] For more information on Canada's anti-spam legislation see: http://fightspam.gc.ca/eic/site/030.nsf/eng/home
[4] PHIPA, Part V.1
[5] S.O. 2004, c. 3, Schedule B, available online: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04q03_e.htm

How to Use this Guide

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

For each step, this Guide provides a summary of the key principles under PHIPA, as well as instructions 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/dietetic practice. 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 Health Information Custodian

If you are a private practice RD 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 (HIC) for the purposes of PHIPA. The HIC is ultimately responsible for the personal health information in their custody or control. If you work for another HIC (such as another regulated health professional, a group practice or a hospital), then you are considered an agent of that HIC.

RDs have different levels of privacy obligations depending on whether they are the HIC at their organization responsible for personal health information or whether they work as an agent. Agents must also comply with PHIPA and with the policies set by the HIC(s) on whose behalf they work.

The key obligations of both HICs and agents include:

1. to obtain consent to collect, use or disclose an individual's personal health information (except in limited situations discussed below);
2. 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);
3. to ensure the accuracy of personal health information;
4. to collect, use or disclose only as much personal health information as is necessary in the circumstances;
5. 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
6. 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).

Additional obligations of HICs include:

1. to develop and comply with policies (known as "information practices") with respect to:
   - when, how and the purposes for which the HIC routinely collects, uses, modifies, discloses, retains or disposes of personal health information; and
   - the administrative, technical and physical safeguards and practices that the HIC maintains with respect to personal health information.

2. to designate a contact person to:
   - facilitate the HIC's compliance with PHIPA;
   - ensure that all agents are informed of their duties under PHIPA;
   - respond to public inquiries about the HIC's policies;
   - respond to requests for access or correction; and
   - receive public complaints about alleged privacy breaches.

3. to display or make available a written public statement that:
   - provides a general description of the HIC's privacy policies (including the purposes for which personal health information is collected, used and disclosed);

- describes how to contact the HIC or other designated contact person;
- describes how an individual can seek access to or correction of a record; and
- describes how an individual can make a complaint to the HIC and to the Information and Privacy Commissioner of Ontario.

The designated HIC must comply with PHIPA. PHIPA provides a list of HICs, including the following:

- health care practitioners or persons who operate a group practice of health care practitioners (this includes all those professions under the *Regulated Health Professions Act, 1991* registered social workers and social service workers, and other unregulated health care providers);
- community service providers under the *Home Care and Community Services Act, 1994;*
- Community Care Access Centres (CCACs); and
- most health facilities including public hospitals, long-term care homes, retirement homes, pharmacies, family health teams, laboratories, ambulance services and community health centres.

Where a potential HIC is an RD who acts as an agent for another HIC (e.g., a group practice or a hospital), the organization, not the individual RD is the HIC. For example, an RD who acts as an agent for a hospital is not a HIC; the hospital is the HIC and the RD is an agent. The purpose of this rule is to ensure that HICs and agents do not need to compete for control over the privacy policies for the organization. Individual RD agents must comply with the HIC's privacy practices when acting on the HIC's behalf, unless otherwise permitted by law. In particular, an agent must ensure that the collection, use, disclosure, retention or disposal of personal health information is permitted by the HIC, is necessary for the purposes of carrying out the agent's duties, is not contrary to law and complies with any specific restrictions imposed by the custodian (s. 17).[6]

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

b) Select Your Information Officer/Contact Person (e.g., this could be an individual RD if you work in a sole practice or a clinic if you belong to a group practice).

The information officer (called the "contact person" under PHIPA) need not be a practitioner. The information officer is responsible for ensuring that the HIC puts in place and follows information practices. In solo practice, an RD is the HIC and the Information Officer/Contact Person.

[6] Additional requirements may be set out in regulations, but none were in place at the time of writing this Guide: PHIPA, s. 17.

The contact person must do the following:

1. facilitate compliance with PHIPA by the HIC;
2. educate the agents of the HIC;
3. respond to public inquiries about the HIC's information practices;
4. oversee access and correction requests; and
5. handle privacy complaints.

The HIC is responsible for displaying a written public statement about its information practices. A sample written public statement is provided as **Form 1**.

It is important that the HIC's information practices are fairly complete because there are special obligations on the HIC where it uses or discloses personal health information in a manner not described in the information practices. For example, the HIC must notify the individual at the first available opportunity of that use or disclosure.

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 HIC. Under PHIPA, personal health information is very broadly defined and includes the following:

- it must relate to an identifiable individual, including information that can be combined with other data (e.g., an ID number, code or 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; and/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. However, PHIPA has a number of exceptions within it. For example, PHIPA does not apply to the regulatory activities of a health College.

b) Inventory of Personal Health Information Collected

RDs should conduct an inventory of all of the personal health information that they collect in the course of providing dietetic services. RDs may use the lists below as a guide to the types of information that may be collected and determine what is relevant to their specific area of dietetic practice.

<u>Personal Characteristics</u>

- 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

- 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
- Identity 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. 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.

RDs 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 HIC;
- 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 HIC; 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."

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

RDs can assume that a written consent is valid unless provided with grounds to the contrary. A direction from a client not to record pertinent information is invalid. However, a client may direct that part of his or her file not be given to another HIC or agent. This is commonly referred to as placing that information in a "lock-box". If the HIC/agent believes that another HIC/agent needs the "locked" information, the disclosing HIC/agent must advise the receiving HIC/agent that some relevant information has been withheld at the direction of the client (but not what that withheld information is).

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.

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.

The substituted decision-maker (SDM) for handling of treatment information issues is generally the same as the SDM for treatment decisions. If the information issue is not related directly to treatment, the list of SDMs is very similar to that under section 23 of the Health Care Consent Act, 1996. 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. A third difference is that a guardian or attorney for property can act as a substitute decision-maker.

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 HIC can only use the name and mailing address of the individual, the fundraising must be for a charitable purpose related to the HIC'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).

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). The Information and Privacy Commissioner of Ontario has established guidelines for charging fees. According to decisions made by the Information and Privacy Commissioner, it is reasonable to charge $30.00 for processing a request and copying the first 20 pages, and then 25 cents for every additional page.[7]

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.

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

[7] Information and Privacy Commissioner of Ontario, Order HO-009, October 2010, available online: http://www.ipc.on.ca/images/Findings/ho-009_1.pdf ; *London Health Sciences Centre (Re)*, 2015 CanLII 13169 (ON IPC), Order HO-14, March 2015, available online: https://www.ipc.on.ca/images/Findings/HO-14.pdf. In Order HO-14, the Commissioner confirmed that the same fees should apply to both requests for disclosure and requests for access.

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

In a rare application of PHIPA to non-HICs, non-HICs are restricted in their ability to use personal health information disclosed to them by a HIC. Non-HICs 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. For example, if the College (a non-HIC) 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.

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 treatment 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 (e.g., Registered Dietitians) are regulated by (e.g., the College of Dietitians of Ontario (CDO)) who may inspect our records and interview our staff as a part of its regulatory activities in the public interest. The CDO 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 and Long-Term Care, 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

HICs 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)). HICs 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 (e.g., 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 HICs 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, HICs must ensure that their staff are 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, complaints to the Information and Privacy Commissioner or prosecutions for deliberate offences.[8]

Given the prevalent use of mobile devices (e.g., laptops, tablets, smart phones, USB keys) in workplaces today, HICs 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."[9] Password protection is not enough. The Information and Privacy Commissioner of Ontario has stated that if personal health information on a mobile device is

---

[8] Up until 2016, no individual had been successfully prosecuted for an offence under PHIPA. That changed with the conviction of two hospital workers that "snooped" into former mayor Rob Ford's health records in 2016. Amendments were made to PHIPA in 2016 to facilitate the prosecution of offences by removing the limitation period for such offences: *Health Information Protection Act, 2016*, S.O. 2016, c. 6 (Bill 119).

[9] 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, See also: "Safeguarding

appropriately encrypted, the loss or theft of that device would not constitute a privacy breach.

HICs should also implement policies regarding the appropriate use of social media. At a minimum, health professionals should never disclose personal health information on social 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 an Internet research). Health professionals must also be prudent not to post pictures of their workplaces that may include images of clients, without client consent.

Records can be kept at the client's home or off-site (e.g., in a storage facility not controlled by the HIC) 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-HICs is in relation to Information Technology (IT) providers to HICs. IT providers must only use personal health information for the purpose of providing their services to the HICs; 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 HIC 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 HICs 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 are 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[10]
- 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: _____

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: _____

[10] 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.

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, tablets, smartphones, 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
  - sensitivity in handling personal health information on mobile devices where other might be able to read ("shoulder-surfing)
  - 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)
  - the fact that the organization needs to be notified about an breaches, who must be notified and that notification must be made at the first reasonable opportunity
  - 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 and may result in a complaint to the Information and Privacy Commissioner or a provincial prosecution
- 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

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

PHIPA requires HICs 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 for complying with PHIPA until he or she is able to transfer the information to another HIC (ss. 3(11) and 3(12)). Refer to section 34 of the Record Keeping Guidelines for RDs in Ontario.

Step 5 – Develop Practices Regarding Access, Correction and Complaints

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

a) Access Rights

PHIPA provides a broad right of access to the personal health information held by a HIC 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 HIC must assist the individual in making a meaningful request, if necessary;
- while the HIC can informally provide access, it can also insist upon a formal written request;
- the HIC should, where reasonably practical, explain terms, codes and abbreviations;
- the HIC 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 HIC;
- the HIC can refuse frivolous, vexatious and bad faith requests for access;
- the HIC must satisfy itself of the identity of the individual before granting him or her access;
- the HIC 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 HIC did not create the record and the HIC 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 HIC 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, HICs must notify others who have received the incorrect or disputed information. However, the notification need only be made where reasonably possible, and the HIC 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 HIC'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.

- 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. Upon receipt of a complaint, the Commissioner can take no action, try to mediate or resolve the complaint, or 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 HIC's regulator (e.g., the College of Dietitians of Ontario) (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).[11]

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, willfully collecting, using (which includes viewing) 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 $100,000 and an organization can face a fine of up $500,000.

[11] The courts have clarified that individuals may also sue for damages under the common law even if the Commissioner has not made an order: *Hopkins v. Kay*, 2015 ONCA 112.

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 use or disclosure of personal health information) (ss. 12(2)). Since June 2016, HICs are also required to notify such individuals of their right to make a complaint to the Information and Privacy Commissioner.

While the focus of this Guide has been on preventing such breaches, HICs should develop policies on how to handle breaches if and when they do occur. The Information and Privacy Commissioner of Ontario has developed the following resource: What to do When Faced with a Privacy Breach: Guidelines for the Health Sector.[12]

Develop a privacy breach protocol for your organization, using the following checklist as a guide. The checklist below is based on the Information and Privacy Commissioner of Ontario's Guidelines.

Privacy Breach Checklist

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

Step 1: Respond immediately by implementing the privacy breach protocol.

- Inform the necessary staff within the organization.
- Consider whether the Commissioner must or should be notified (PHIPA provides that regulations may be passed setting out certain kinds of breaches that must be reported to the Commissioner: s. 12(3). As of the date of this Guide, no such regulations have been passed.)

Step 2: Containment - Identify the scope of the potential breach and take steps to contain it.

- Assess what and how much information was breached and in what manner (e.g., paper format, electronic format).
- Determine whether copies were made.
- Implement any necessary action to contain further unauthorized access (e.g., change passwords, identification numbers and/or temporarily shut down a system).

[12] 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

Step 3: Notification - Identify those individuals whose privacy was breached and notify them of the breach.

- Notify all individuals whose personal health information has been compromised in the most appropriate way possible in light of the sensitivity of the information (e.g., by phone, in writing, at the next appointment, etc.).
- Inform all individuals of the steps that have or will be taken to address the privacy breach and that the Information and Privacy Commissioner's Office, Ontario has been informed.
- Provide the individuals with the organization's and the Information and Privacy Commissioner's Office, Ontario contact information in case individuals have further questions
- Advise the individual of their right to make a complaint to the Commissioner (s. 12).

Step 4: Investigation and Remediation

- Conduct an internal investigation into the matter to identify how and why the privacy breach occurred.
- Take the necessary steps to implement a plan that strives to avoid a similar privacy breach from occurring in the future.
- HICs should advise the Information and Privacy Commissioner's Office, Ontario of the investigation findings, proposed future prevention plan and work together to make any necessary changes.
- Report the results of investigation to the relevant regulatory College if appropriate or required (PHIPA requires HICss to report certain events to the relevant regulatory College, including when a member is suspended, terminated or otherwise disciplined or has had their privileges or business affiliation revoked or restricted as a result of a privacy breach: s. 17.1. The organization may also be required to report the circumstances to a regulatory College under the *Regulated Health Professions Act, 1991* in cases of professional misconduct, incompetence or incapacity.)
- Ensure staff are appropriately trained and conduct further training if required.

Step 7 – Implement Your Privacy Plan

Implementing your Privacy Policy will have two stages:

Stage 1: Complete your review of how you handle personal information and to prepare and roll out your Privacy Policy.

Stage 2: 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 implement a regular review system. 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, Ontario requires this information.

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

Initial Implementation Checklist

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

Ongoing Review

1. Monitor compliance with Privacy Policy document (prepare a report annually)
2. External information technology audit (annual)
3. Training for new staff provided (as needed)
4. Refresher training session for all staff (annual)
5. 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 the College of Dietitians of Ontario
- 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 health information 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 of 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 Professionals

This sample privacy policy should be modified to fit your organization's/private practice needs. In particular, you will need to tailor the document to reflect the types of personal health information that your organization/private practice 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 or private practice]. 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, nutritional 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(s));
- 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 nutrition care needs are, to advise them of their options and then to provide the nutrition 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 [e.g., the College of Dietitians of Ontario] who may inspect our records and interview our staff as a part of its regulatory activities in the public interest. The College of Dietitians of Ontario 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., the Ministry of Health, and Long-Term Care, children's aid societies, Canada Customs and Revenue Agency, Information and Privacy Commissioner, Ontario, 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.
- External consultants and agencies with access to personal information must enter into privacy agreements with us.

Openness about the Personal Information Process

The organization must make its personal information Privacy Policy available to the public. Individuals must be able to obtain and understand this Privacy Policy without unreasonable effort.

Procedure

1. Staff are trained to provide the Privacy Policy document to anyone who requests it.
2. The Privacy Policy document will be posted in the reception area(s) of our organization.
3. The Privacy Policy will be posted on our organization's website, where applicable.
4. A brochure summarizing the Privacy Policy document is provided to each new client at the time the consent form is signed.

Right to Access Personal Information

Individuals have the right (with some exceptions) to access personal information about themselves held by the organization and to know what the organization has done with it. This ensures that the personal information is adequate, correct and up to date.

The suggestions below were written by the College of Dietitians of Ontario specifically for RDs to simplify the process of developing information privacy policies for their practices.

The suggested privacy practices translate some of the central requirements of law into statements for RDs providing dietetic services. They deal with some of the most significant personal health information privacy issues in a practical and understandable way, reflecting the professional values and requirements of dietetic practice. (e.g., client centered practice, informed consent, client confidentiality). However, they are simply suggestions and guides for RDs. Users of this guide will need to adapt them to their unique circumstances.

Procedure

1. Staff know where to refer a request or inquiry for access if they are not able to answer it themselves;
2. The organization can require the request to be in writing (verbal request can be answered);
3. The organization will help a person make an access request if asked (e.g., to explain the filing system at the organization);
4. The organization provides access upon request within 30 days unless grounds of refusal exist;
5. The organization normally provides access not only to personal information on record, but also to how the organization has used and disclosed it. Thus, reasonable records should be kept;
6. The organization keeps reasonable records of any unusual uses or disclosure of personal information (e.g., systematically filing a cover letter, fax sheet or email in the relevant file);
7. The organization confirms the identity of the individual requesting the information before disclosing it;
8. The organization takes reasonable and necessary steps to ensure that the individual requesting information can understand it (e.g., explain short forms or codes, provide it in an alternative format where the requester has a sensory disability);
9. Access must be provided, despite a ground for refusal (except law enforcement) where the individual's life, health or security is threatened. Grounds for refusal to access personal information would include:
    - 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).

10. Even if the organization refuses the request, it cannot destroy the information until the individual has had a chance to challenge the refusal.

11. Additional procedures for handling access requests:
    - The Health Information Custodian (HIC) 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 HIC;
    - The HIC can refuse frivolous, vexatious and bad faith requests for access; and
    - The HIC can only charge a reasonable cost recovery fee for access and must provide an estimate of the fee in advance (s. 53-54). The Information & Privacy Commissioner's Office of Ontario suggests a charge of $30.00 for the first twenty pages of records and 25 cents for each additional page.

Correction Requests

Clients have the right to request a correction of erroneous information held by the organization. The purpose is to maintain appropriate and accurate information on clients.

Procedure

1. The organization's process for handling correction requests is fair to the individual.

2. Correction requests are restricted to factual information. Professional observations and opinions are not generally subject to correction requests.

3. Corrections are made without obliterating the original entry.

4. A notice of the disagreement is filed with the record where the organization does not agree that the information is incorrect. Any notice of refusal must advise the individual of his or her right to complain to the Information and Privacy Commissioner about the refusal (s. 55).

5. Corrections or notice of the disagreement are sent to third parties who have received the erroneous information unless doing so is not appropriate. However, there are limits that may include the following:
   - the individual must request it;
   - the notification need only be made where reasonably possible; and
   - the HIC 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.

6. The individual is given a timely response (usually within 30 days) to a request to correct, along with reasons for any refusal to do so and notice of any recourse.

7. Grounds to refuse correction may include requests where:
    - the request is frivolous, vexatious or made in bad faith; or
    - the HIC did not create the record and the HIC does not have sufficient knowledge, expertise or authority to make the correction.

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.

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.

Complaints System

The organization develops and maintains an internal complaint system and makes external recourse publicly available in order to be able to receive, investigate and respond to complaints. Every effort is made to investigate and decide a simple complaint within 30 days. For more complex complaints, the person investigating or deciding the complaint will advise the person making the complaint within 30 days of how long it will likely take to investigate and decide it.

Procedure

1. The individual who is designated to investigate complaints will:
    a) receive and promptly acknowledge receipt of a complaint;
    b) investigate the complaint;
    c) decide on the complaint.

2. In addition, the individual who decides on the complaint has the authority to:
    a) ensure compliance with the organization's policies in respect of the complaint;
    b) change the organization's information handling policies (after consultation with other leaders of the organization);
    c) award a refund, credit or financial compensation to the individual (after consultation with other leaders of the organization).

3. The Complainant has recourse to external bodies as follows:
    a) the regulatory body(ies) for the organization or members of the organization (e.g., College of Dietitian of Ontario);

b) the Office of the Privacy Commissioner of Canada;
c) the Information and Privacy Commissioner of Ontario to the extent that the Personal Health Information Protection Act, 2004 applies.

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, as applicable:

Step 1: Respond immediately by implementing the organization's privacy breach protocol.

- Inform the necessary staff within the organization.
- Consider whether the Commissioner must or should be notified (PHIPA provides that regulations may be passed setting out certain kinds of breaches that must be reported to the Commissioner: s. 12(3). As of the date of this Guide, no such regulations have been passed.)

Step 2: Containment - Identify the scope of the potential breach and take steps to contain it.

- Assess what and how much information was breached and in what manner (e.g., paper format, electronic format).
- Determine whether copies were made.
- Implement any necessary action to contain further unauthorized access (e.g., change passwords, identification numbers and/or temporarily shut down a system).

Step 3: Notification - Identify those individuals whose privacy was breached and notify them of the breach.

- Notify all individuals whose personal health information has been compromised in the most appropriate way possible in light of the sensitivity of the information (e.g., by phone, in writing, at your next appointment, etc.).
- Inform all individuals of the steps that have or will be taken to address the privacy breach and that the Information and Privacy Commissioner's Office, Ontario has been informed.
- Provide the individuals with the organization's and the Information and Privacy Commissioner's Office of Ontario contact information in case individuals have further questions.
- Advise the individual of their right to make a complaint to the Commissioner (s. 12).

Step 4: Investigation and Remediation

- Conduct an internal investigation into the matter to identify how and why the privacy breach occurred.
- Take the necessary steps to implement a plan that strives to avoid a similar privacy

breach from occurring in the future.

- We will advise the Information and Privacy Commissioner's Office of Ontario of the investigation findings and proposed future prevention plan and work together to make any necessary changes.
- Report the results of investigation to the relevant regulatory College if appropriate or required (PHIPA requires HICss to report certain events to the relevant regulatory College, including when a member is suspended, terminated or otherwise disciplined or has had their privileges or business affiliation revoked or restricted as a result of a privacy breach: s. 17.1. The organization may also be required to report the circumstances to a regulatory College under the *Regulated Health Professions Act, 1991* in cases of professional misconduct, incompetence or incapacity.)
- Ensure all staff are 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. If we take disciplinary action against one of our practitioners (or revoke or restrict the privileges or affiliation of one of our practitioners) for a privacy breach, we are required to report that to the practitioner's regulatory College. We may also report the breach to the relevant regulatory College if we believe that it was the result of professional misconduct, incompetence or incapacity.

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 (please 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: [insert contact person].

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

Signature: _____ Date: _____

Printed Name: _____

Privacy Resources

1. Ontario
   - *Personal Health Information Protection Act, 2004*
   - Information and Privacy Commissioner of Ontario

2. Canada
   - *Personal Information Protection and Electronic Documents Act, 2000*
   - Office of the Privacy Commissioner of Canada

3. College of Dietitians of Ontario

   Visit the College's website at www.collegeofdietitians.org. Enter key word, "privacy" in the search box.

   Please feel free to contact the College's Practice Advisory Service

   practiceadvisor@collegeofdietitians.org

   416-598-1725 / 1-800-668-4990, ext. 397