College of Opticians of Ontario

Chapter 2:
Record Keeping, Confidentiality and Privacy

Table of Contents

Chapter Two:
Record Keeping, Confidentiality and Privacy

Introduction

The purpose of this module is to assist members in understanding the concepts of record keeping, privacy and confidentiality and their importance. This module will also help members develop practical skills for making, maintaining, using and disclosing patient records.

Foundational Concepts

In order to understand the expectations of members for record keeping, privacy and confidentiality, it is useful to begin with the following basic principles.

1. Personal health information belongs to the patient. It is theirs to provide. Once provided, the information is (with a few exceptions) theirs to control.
2. The reason a patient reveals his or her personal health information to a member is so that member can provide the best possible services to the patient.
3. The reason a member collects personal health information from a patient is so that the member can provide the best possible services to the patient.
4. It is necessary for members to record all relevant personal health information about their patients. Such a record,
    a. enables members to accurately recall and use the information for healthcare services now or in the future,
    b. enables others who may be treating the patient to use the information if the member is not available,
    c. enables members to explain their actions if concerns are raised in the future (e.g., by the patient, the College or a payer), and
    d. can occasionally be used for other valid purposes (e.g., research).
5. There are a few secondary uses of personal health information. For example, the College uses a member's patient records for quality assurance purposes to enhance the care provided to all patients of the member. Sometimes the information is used by society for compelling reasons that outweigh the usual rights of the patient (e.g., to protect a child in need of protection; to help prove a criminal offence like fraud).

These foundational concepts have numerous significant implications. Because the information belongs to the patient and is to be used for the patient's benefit, the member must obtain informed consent to collect, use and disclose the information. The member has to carefully safeguard the information. Patients have the right to look at and, where appropriate, correct the information held by the member.

This module describes how the above basic principles are applied in actual practice.

Record Keeping

One important aspect of the standards of practice of the profession is record-keeping. Keeping records is essential for providing good patient care; even members with excellent memories cannot recall all of the details of their patients' health status, measurements and treatment. Records permit the monitoring of changes in patients. Records assist other practitioners who may see the patient afterwards. Records also enable a member to explain what they did for patients if any questions arise. Records help members defend themselves if a patient recalls things differently than the member. Failure to make and keep adequate records can be a failure to maintain minimum professional standards and is professional misconduct.

The College has a Standard of Practice on Record Keeping (Standard 5) and accompanying Guidelines that deal with matters such as:

- The information that must be recorded;
- The form in which records can be kept (e.g., written, computerized);
- How long the information must be kept;
- Maintaining or transferring records upon leaving a practice or retiring;
- Confidentiality and privacy issues; and
- Patient access to records.

Record keeping expectations apply to various types of records including:

- Patient file;
- Billing records; and
- Patient consent (e.g., for treatment, billing and release of patient information).

Daily appointment schedules and equipment and supply records should also be kept to support the services provided by members.

The Information that Must be Recorded

The patient file is intended to record what was done and what was considered by the member. It acts as a communication aid to ensure that there is continuity of care for the patient. Proper records also improve patient safety.

The College's Standard 5 on Record Keeping states that an optician must retain complete and accurate patient records that meets the following content criteria:

A patient record must clearly and legibly include the following information appropriate to the appliance that you are dispensing:

a) The patient's contact information.
b) A patient history, including information about the patient's general and optical health, occupation, and avocation(s).
c) Complete details of a patient's prescription, including the name of the prescriber, and the date of examination.
d) All details of the ophthalmic appliance dispensed.
e) The identity of the optician who fit, verified, and delivered the optical appliance.
f) The ongoing management plan for the patient, including the program or schedule for follow up.
g) If a patient fails to attend or respond to follow up notifications, a notation to this effect.
h) If eyeglasses were duplicated from those currently worn by the patient, a notation to this effect.

The patient's identifying information should be on each document in the record (whether paper or electronic) so that a particular document may be returned to the record if separated.

The record should include all relevant subjective and objective information gathered regarding the patient. This includes all relevant information provided by the patient (or his or her authorized representative, or other health care professionals involved in the patient's care) to the optician regardless of the medium or format in which the information was provided (e.g., communicated in person, on paper, email, fax, telephone, etc.). The record also includes any findings from assessments or other observations made even if they were not part of the formal assessment (e.g., if the patient was not able to read the invoice).

The results of any testing done by the member should be recorded. If a patient discloses test results from another health professional, it should be noted in the record. However, members do not have to ask for copies of reports if they are not needed.

The management plan should be recorded. Then the actual eyewear and services provided should be noted. The record should also include any follow up visits or calls, any changes in the patient's condition, or any reassessments of the patient or any modifications of the appliance. It should be clear to any practitioner reading the record what happened.

If the patient was referred to the optician, the person who made the referral and the reason for the referral should be in the record.

Any consent that is obtained should be included in the record. This includes consent to treatment, consent relating to the collection, use and disclosure of the patient's personal health information and any agreement as to billing.

The Form in Which Records Can be Kept

Records must be legible. Failure to maintain a legible record would defeat the purpose of maintaining a complete and accurate record.
Records can be on paper or on computer. Computerized records should be printable and viewable and should have an audit trail of changes made. These requirements are discussed further in the discussion of the *Personal Health Information Protection Act (PHIPA)* below.

It should be clear who made each entry into the health record and when that entry was made. Any change or amendment to the record should be indicated, the date of which the change was made should be noted, and who made the change should be recorded. Importantly, any changes to the record should still permit the reader to read the original entry.

Members cannot falsify records; this means that if an error is made in a previous entry it cannot be removed (e.g., 'whited-out', or deleted). The record should be maintained with correction to the error (usually a simple line through the error with the date and initial of the person correcting the error).

The record should be in English or French. The information can be recorded in other languages so long as all the information is also recorded in English or French. The generally accepted languages in the health care system in Ontario are English or French. This permits other health care providers on the patient's health care team (e.g., other opticians, other health care providers) to understand the record.

How Long the Information must be Maintained

Relevant personal health information should not only be recorded, it must also be kept until it is unlikely to be needed again. The College has established guidance to the profession to ensure that the information is not only available for future services to the patient, but is also available for other purposes including responding to concerns or complaints about the member's services and conduct.

The College's Standard 5 on Record Keeping states that a member must retain records as follows:

2. Retaining Records
   a) An optician must ensure that all patient records are retained for seven years from the date of the last entry.
   b) An optician must maintain his or her records in a manner that ensures that a patient or authorized College investigator, assessor or representative has access to the records.

c) An optician who is a health information custodian[1] must ensure that files are not abandoned when the optician retires or sells his or her practice. The optician must ensure that files are transferred securely and in accordance with applicable privacy legislation.

The member (or health information custodian for whom the member works) needs to keep the record for seven years from the last interaction with the patient (as all interactions are expected to be recorded). An interaction can involve any contact with the patient, including a phone call or an email.

The rule regarding keeping records for seven years applies to clinical, financial, appointment and attendance records.

The following guidelines published by the College apply when a member stores patient records at a third-party storage site:

i. The storage facility should have a privacy policy that is consistent with PHIPA and the College's record keeping requirements.
ii. The optician should obtain written assurance that the facility will safeguard the information and only disclose it if the optician specifically requests this.
iii. If the facility will destroy the records at a later date, the optician should contract with the facility to retain the records for the seven years and destroy the records in a secure manner.
iv. The optician should keep the account with the storage facility current at all times to ensure that records are not destroyed prematurely.
v. The optician should keep records of what files are retained at the third-party site.
vi. If the optician is in active practice, the optician's privacy policy should state that the optician uses a third-party storage site.

Maintaining or Transferring Records upon Leaving a Practice or Retiring

The entire original record should be kept by the member (or the health information custodian for whom the member works) and only copies should be supplied to others.

Even when a member retires or leaves the practice (i.e., resigns as a member of the College) the original record should be kept for the seven year retention period, unless the record has been transferred to another practitioner who will maintain the record. The patient must be notified

[1] The concept of a "health information custodian" is discussed below.

of the transfer. In those circumstances, the original record (and not just a copy) can be transferred to the new practitioner.

However, if just the patient has been referred to another health care professional and the patient record has not been transferred, then the retention period of the entire original record (i.e., seven years from last contact) is still mandatory.

An exception to keeping the original record is where there is some legal duty to provide the original record to someone (i.e., in a police investigation, Coroner's or College investigation, or where there is a summons). If this circumstance occurs, the member should keep a legible copy of the record for themselves.

Special rules apply when opticians work with optometrists. Optometrists are expected to keep their own records when they leave a practice. Thus, even if the optician owns the practice location, separate files should be kept so that the optometrist can take his or her own files when he or she leaves. Members need to be careful not to pressure or require an optometrist to breach his or her own standards of practice even when the optician owns the practice location. For example, optometrists are required to retain their records for at least ten years (not seven as for opticians) and to retain access to the records even after they leave the practice location. In addition, opticians have no right to access optometry records for marketing purposes even if they own the practice location.

When the time period for keeping the record has expired, the destruction of the records should be done in a secure manner that prevents anyone from obtaining the information (i.e., shredding, complete electronic destruction). If a member destroys any records, a good practice would be to keep a list of the names of the files that were destroyed and the date they were destroyed.

When transferring from paper records to an electronic record keeping system, the original may be destroyed after it has been scanned and stored. The electronic version of the document becomes the original.

Confidentiality and Privacy Issues

Members should take reasonable steps to keep records safe and secure. In general, no one outside of the authorized circle of care of health professionals should be able to have access to the records. Privacy protections must be in place to ensure the records cannot be seen, changed or taken by others. Paper records should be kept under lock and key. Computer records need to be password protected on computers that have firewall and virus protections and must be backed up regularly. Particular privacy issues are discussed in more detail below.

Patient Access to Records

Generally, a patient has the right to review and receive a copy of all clinical records kept by a member unless access would significantly jeopardize the health or safety of a person. Although the member may own the health care record and be responsible for it, patients are authorized by the *Personal Health Information Protection Act* to access the record. The information in the record really belongs to the patient. Also, the patient has the right to correct any errors in the health record. If a patient requests any relevant parts of the record, the member should provide them with a copy and not the original.

Record Keeping Scenario

David has been practising for 45 years and has built up a busy and successful practice. He decides he is ready for retirement but wonders what he is supposed to do with his patient records. Does he have to retain them himself? Ordinarily he would have to retain patient records for seven years from the last interaction with the patient. But in this case David may be selling his practice to another optician who will take over the business and patients. The buying optician will likely agree to keep the records for the seven year period. If this is the case, David does not have to retain the records himself, but needs to notify the patients of the transfer of their patient records. This can be done through a combination of telling patients on their next visit, sending out letters and placing a notice in the local newspaper.

Sample Exam Question

Which one of the following does not need to be recorded in the patient's record?

i) The patient's birth date.
ii) The person who recommended the patient to you.
iii) The patient's health concerns.
iv) The management plan for the patient.

The best answer is ii). Only if the patient was referred by another health care provider must there be a record of who recommended the patient. If another patient referred the person or the person found out about your office through advertising, that does not have to be recorded (although in some cases it would be helpful to record this information). Answer i) is not the best answer because members need to record the patient's birth date. It is relevant to many management decisions. Answer iii) is not the best answer because members need to record the patient's health concerns (sometimes called history). It is relevant to many management decisions. Answer iv) is not the best answer because members need to record the management plan for the patient. It is relevant to following up on future visits and for justifying one's actions should questions be raised later.

Confidentiality and Privacy

Personal Health Information

The concepts of privacy and confidentiality are similar, but not identical. Confidentiality is a professional obligation owed by members to their patients. The regulations make the following to be professional misconduct:

> 10. Giving information about a patient to a person other than the patient or his or her authorized representative except with the consent of the patient or his or her authorized representative or as required or allowed by law.

Confidentiality obligations are enforced by the College and, to lesser extent, the courts.

Privacy on the other hand, goes much further. Privacy provisions begin with the concept that all personal health information belongs to the patient and that the member holds it in trust for the benefit of the patient. Members have a duty to protect the privacy of patients' personal health information. Privacy principles are set out in the *Personal Health Information Protection Act* (*PHIPA*). *PHIPA* looks at the collection, use and disclosure by members. It also looks at the access given to patients to their own personal health information. Privacy obligations are enforced by the Information and Privacy Commissioner of Ontario. Failing to meet privacy obligations is also likely to be a breach of the College's record keeping standard and may be professional misconduct.

Personal health information refers to almost anything that would be in a member's files on a patient. It is defined in *PHIPA* as written or oral identifying information about a person, if the information:

i. Relates to the person's physical or mental health, including the person's family health history;
ii. Relates to the providing of health care to the person, including the identification of a person as someone who provided health care to the person;
iii. Is a plan of service within the meaning of the *Home Care and Community Services Act, 1994* for the person;
iv. Relates to the person's payments or eligibility for health care, or eligibility for coverage for health care;
v. Relates to the donation by the individual of any body part or bodily substance of the person or is derived from the testing or examination of any such body part or bodily substance;
vi. Is the person's health number; or

vii. Identifies a person's substitute decision-maker.

Identifying information about a person is also considered to be personal health information when it is contained in a record of personal health information.

Health Information Custodians

PHIPA places significant obligations on Health Information Custodians (a Custodian). A Custodian is the person or organization responsible for all health records. The Custodian must create, implement and oversee a privacy policy that meets the requirements of *PHIPA*.

A sole practitioner would be the Custodian of any health information and records that the member collects. If a member works for a health services organization such as a clinic or chain of offices, the organization is usually the Custodian of health records.

Many members work for organizations like department stores. Typically the organization is the Custodian. However, even where the member is not the Custodian, the member has privacy obligations. For example, the member needs to follow the privacy policies that protect patients (e.g., security policies and safeguards such as using complex passwords). In addition, the member has to work with the Custodian to ensure that the member's record keeping obligations are met. College publications and professional standards of practice still apply to the member even if the member's employer is not regulated by the College. Members cannot work for employers who disregard professional standards. For example, the member must ensure that all required information is recorded and that the record is retained for the required period of time (i.e., seven years).

Two or more members who work together may decide to act as a single organization for the purposes of *PHIPA*. This may be helpful because the members can create a single privacy policy. This would allow for consistent health record keeping practices. In this case the members will have shared responsibility for complying with *PHIPA*.

Information Officers

PHIPA requires every Custodian to appoint a contact person (often called an Information Officer). An Information Officer is the person who makes sure everyone follows the requirements of *PHIPA*. The Information Officer reviews the organization's privacy practices, provides training, and monitors compliance. The Information Officer is also the contact person for requests for information from the public.

A sole practitioner usually acts as Information Officer himself or herself. An organization may appoint a person within the organization, or may hire a person outside of the organization to be its Information Officer.

PHIPA Scenario

Three members work together in an office. They decide they will act as an organization for privacy purposes. Their organization is the Health Information Custodian. The members create a privacy policy together. The members decide to appoint the most senior optician to be the Information Officer. The Information Officer creates a procedure to protect personal information, develops a privacy complaints procedure, and ensures that all members *comply with the privacy policy.*

Protecting Personal Health Information

Custodians must put in place practices to protect personal health information in their custody or control. They must take appropriate measures to protect personal health information from unauthorized access, disclosure, use or tampering. The nature of those safeguards will vary depending on the sensitivity of the information and the circumstances. Personal health information is generally considered highly sensitive. Those safeguards must include the following components:

- physical measures (For example, restricted access area and/or locked filing cabinets);
- organizational measures (For example, need-to-know and other employee policies and/or staff training); and
- technological measures (For example, passwords or encryption and/or virus protection or firewalls).

For example, the Information and Privacy Commissioner has made numerous orders and issued bulletins and fact sheets indicating that health practitioners cannot store personal health information on mobile devices unless the devices are encrypted. Simply using password protection to enter the device is insufficient. See www.coptont.org/docs/Privacy/ipc_004.pdf for more information.

Members need to systematically review all of the places where they may temporarily or permanently hold personal health information (including laptops, smartphones and other handheld devices) and assess the adequacy of the safeguards. Almost every organization that has not done this before will find that it needs to make changes.

Members storing their information in the "cloud" should try to avoid using a cloud company that has servers in the United States as their laws allow extensive government access to the information. In addition, members should ensure that the cloud company has a trustee that will hold the information if the company goes bankrupt so that the cloud company's creditors do not then take possession of the information.

If there is a privacy breach, members should take the following steps:

- Take immediate steps to contain the breach. The member should try to retrieve the compromised information if it is still outside of the member's control. If the information has been stolen, the police may need to be called. The Information and Privacy Commissioner may be able to assist the member in doing so.
- Notify the individuals whose information has been compromised of the breach. This disclosure is now required by *PHIPA*. If the member is not the custodian, the member must notify the custodian of the privacy breach so that the custodian can notify the patients. This step will often involve making an apology and, sometimes, making amends.[2]
- Notify the College if certain types of disciplinary actions (e.g., suspensions, terminations, resignations) are taken against a member or another registered health practitioner for the unauthorized collection, use, disclosure, retention or disposal of personal health information.
- Review and revise the member's policies and procedures. Assess what went wrong and what steps need to be taken so that this sort of privacy breach (and another other privacy breach) does not recur in the future.

As noted above, members also need to securely keep, transfer and dispose of records in accordance with the College's expectations.

A member's or organization's privacy policy should explain how health information will be protected.

Collection, Use and Disclosure of Personal Health Information

A member or organization must only collect, use, or disclose a person's personal health information if the person consents or if the collection, use or disclosure is otherwise permitted or required by law. A member should collect, use or disclose no more information than is reasonably required in the circumstances.

A member's or an organization's privacy policy should clearly explain how and when personal health information will be collected, used and disclosed.

Under *PHIPA*, collection, use and disclosure of personal health information is permitted without a patient's consent in limited circumstances. Below are some common situations where the rules about collection, use and disclosure of the personal health information may arise.

[2] Once regulations are made, the custodian would also have to inform the Information and Privacy Commissioner of many privacy breaches.

Circle of Care

A member can share personal health information with other individuals within a patient's "circle of care" for the purposes of providing health care, without the patient's express consent. A circle of care may include other health professionals who provide care to the same patient (e.g., a physician, an optometrist). A member is generally permitted to assume that he or she has a patient's implied consent to disclose personal health information to other health providers in the patient's circle of care.

A member who is working in a multidisciplinary setting may, for the purpose of treatment, share personal health information with other health care professionals who are providing care to the same patient because these other health care professionals are within the patient's circle of care.

A member who refers a patient to another health professional may consider that health professional to be within the patient's circle of care. The circle of care of a member's patient may also include other health care providers in other institutions if it is necessary for providing health care to the individual and it is not reasonably possible for consent to be obtained in a timely manner.

However, many practitioners do not share information with others in the health care team without the patient's explicit consent unless it is an emergency so as to avoid misunderstandings. This is especially important where the information is sensitive (e.g., the patient is worried that their vision limitations may place their job in jeopardy).

An exception to the circle of care rule is if a patient says that he or she does not want the information to be shared. The information must then not be shared unless another provision in *PHIPA* permits it (this direction from a patient is often referred to as placing the information in a "lock box").

Circle of Care Scenario

> *Donna, an optician, receives a telephone call from an optician in cottage country. A patient has lost their glasses in a boating accident and cannot drive without a replacement pair. The patient is in the hospital and is not accessible. The cottage country optician wonders if Donna can provide her pupillary distance measurements for the patient and any other relevant information. While Donna could insist on speaking with the patient to obtain express consent to share this information, Donna would be entitled to disclose the information without express consent by relying on the circle of care concept.*

Family and Friends

Generally speaking, consent should be obtained before sharing personal health information with members of a person's family.

However, personal health information may be disclosed for the purposes of contacting family members, friends, or other persons who may be potential substitute decision-makers if the patient cannot provide consent (e.g., the patient is incapable).

Disclosure Related to Risk

A member may disclose a person's personal health information if the member believes on reasonable grounds that the disclosure is necessary to eliminate or reduce a significant risk of serious bodily harm to the person or anyone else.

For example, if a patient has threatened to kill someone, the member can warn the person being threatened and call the police. The member could share any information about the patient that will help the police to deal with the threat. In some circumstances this principle can apply to patient-harm as well (e.g., where the patient is suicidal).

Perhaps the most common example of where this might happen is where the optician is concerned about the patient's ability to drive safely. While not covered by the same mandatory reporting requirements as an optometrist, a member may feel that in some rare circumstances they are in the best position to disclose the risk in order to avoid a serious risk of harm.

Other Laws

PHIPA allows disclosure of personal health information that is permitted or required by many other Acts, including the following:

- The *Health Care Consent Act* or *Substitute Decisions Act* for the purposes of determining, assessing or confirming capacity;
- Disclosure to a College acting under the *Regulated Health Professions Act* (e.g., in relation to a peer assessment or a complaint against a member); and
- Disclosure to an investigator or inspector who is authorized by a warrant or by any provincial or federal law, for the purposes of complying with the warrant or facilitating the investigation or inspection.

Additionally, there are some circumstances in which there is a mandatory reporting duty to disclose personal health information. For example, where a member reports to the College that

a colleague is leaving the practice because of the colleague's incompetence, the report will contain some personal health information about affected patients.

Access to Personal Health Information

Every patient has a right to access his or her own personal health information. There are very few exceptions. One important exception is if granting access would likely result in a risk of serious harm to the patient's treatment or recovery, or a risk of serious bodily harm to the patient or another person.

If a person makes a request to access personal health information, the member or organization must:

- permit the person to see the record and provide a copy at the person's request;
- determine after a reasonable search that the record is unavailable, and notify the person of this in writing as well as his or her right to complain to the Information and Privacy Commissioner of Ontario; or
- determine that the person does not have a right of access, and notify the person of this as well as his or her right to complain to the Information and Privacy Commissioner of Ontario.

The Information and Privacy Commissioner, a government appointed official administering *PHIPA*, may review the member's or organization's refusal to provide a record, and may overrule the decision.

Where some, but not all of the information can be withheld, the member should black out (on a copy, not the original) those parts that should be withheld, so that the patient may see the rest of the record.

Sample Exam Question

A patient asks an optician to provide the patient's pupillary distance. How should the optician respond?

i) Refuse to provide the information because it would put the health and safety of the patient in jeopardy.
ii) Provide the information because it belongs to the patient.
iii) Refuse to provide the information because it is the product of the optician's own measurements and was not provided by the patient.
iv) Provide the information only if the patient promises not to order lenses online.

The best answer is answer ii). A patient's right to access his or her health information is broad and would almost certainly cover this request. Answer i) is not the best answer because the risk of harm, if there is one, is likely not significant. Answer iii) is not the best

answer because even a member's measurement results constitute patient health information covered by the right of patient access. Answer iv) is not the best answer because the right of patient access does not depend on how the patient plans to use the information.

Correction of Personal Health Information

Patients generally have a right to ask for corrections to their own personal health information. A member or organization receiving a written request must respond to it by either granting or refusing the request within 30 days. It is wise to respond to verbal requests as soon as possible as well. If the request cannot be fulfilled within 30 days the person should be advised of this in writing.

Corrections to records must always be made in a way that allows the original record to be seen. The original record should never be destroyed, deleted, or blacked out. If the record cannot be corrected on its face, the correction should be made so that any person accessing the record will see the correction or know where to find the correct information (e.g., by means of a footnote or link in an electronic record). The patient should also be notified of how the correction was made.

At the patient's request, the member should notify anyone to whom the member has disclosed the incorrect information of the correction. An exception to this is if the correction will not impact the person's health care or otherwise benefit the person.

The member or organization may refuse the request if the member or organization believes the request is frivolous or vexatious (e.g., it simply repeats a previous request that has already been denied); if the member did not create the record and does not have the knowledge, expertise and authority to correct it (e.g., a physician's diagnosis), or if the information consists of a professional opinion made in good faith (e.g., the optician documents a recommendation that a patient is not suitable for contact lenses). In other words, corrections are limited to factual information, not professional opinions.

A member who refuses to make a correction must notify the patient in writing, with reasons, and advise the patient that he or she may:

- prepare a concise statement of disagreement that sets out the correction that the member refused to make;
- require the member to attach the statement of disagreement to his or her clinical records and disclose the statement of disagreement whenever the member discloses related information;
- require the member to make all reasonable efforts to disclose the statement of disagreement to anyone to whom the member has previously disclosed the record; or

- make a complaint about the refusal to the Information and Privacy Commissioner.

Complaints

Every organization must have a system in place to deal with complaints regarding personal health information. Patients should also be aware of their right to complain to the College and/or to the Information and Privacy Commissioner.

PIPEDA

Another privacy law that members should know about is the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*). *PIPEDA* is a federal law that looks at the collection, use and disclosure of personal information in relation to commercial activity **outside of** health care.

PIPEDA applies only to commercial activities of members, such as the sale of non-health products at members' offices (e.g., the sale of non-prescription squash or scuba goggles, safety eyewear, designer sunglasses, readymade magnifiers) and the offering of educational sessions. Unlike *PHIPA*, which governs personal health information, *PIPEDA* governs all types of non-health personal information. Examples of personal information include the person's name, date of birth, and home address.

The following ten privacy principles apply to a member's commercial activities:

1. Accountability: Someone in an organization (the "privacy officer", sometimes called an "information officer") must be accountable for the collection, use and disclosure of personal information. The privacy officer must develop privacy policies and procedures and ensure that staff receive privacy training.
2. Identifying Purposes: An organization must identify the purposes for which personal information will be used at the time that the information is collected.
3. Consent: Consent is required to collect, use and disclose personal information, except in limited circumstances (e.g., in emergencies or where the law otherwise permits this).
4. Limiting Collection: An organization must only collect the information that is necessary to collect for the identified purposes.
5. Limiting Use, Disclosure and Retention: An organization must only use, disclose and retain personal information that is necessary for the identified purposes and is obtained with consent. It should be retained no longer than necessary.
6. Accuracy: An organization must make reasonable efforts to ensure that any personal information collected is accurate, complete and up-to-date.
7. Safeguards: An organization must protect personal information with appropriate safeguards in order to protect against loss, theft, unauthorized access, disclosure, copying, use, or modification.

8. Openness: An organization must make its privacy policies readily available.
9. Individual Access: Upon request, an individual must be informed of the existence, use and disclosure of his or her personal information, and be given access to it. An individual can request corrections to the information. Access may be prohibited in limited circumstances such as the privacy of other persons, if there is a prohibitive cost to provide it, or for other legal reasons.
10. Challenging Compliance: An organization must have a complaints procedure relating to personal information and must investigate all complaints.

As you can see, *PHIPA* and *PIPEDA* are based on the same principles. *PHIPA* simply provides more details about how to achieve those principles in the health care context.

Conclusion

Patients own their personal health information. Patients reveal this information to members so that the member can provide the most effective management of their vision possible. Thus members have a duty to record the information and then to hold it in trust for the patient. Members must safeguard the information and provide access to it when requested by the patient.