

WHAT EVERY OPTICIAN NEEDS TO KNOW ABOUT PRIVACY LEGISLATION

By Richard Steinecke

Over the past few years, there has been a lot of confusion about privacy legislation. Who does it apply to? When is it really coming? How much impact will it have? Busy opticians need to know what privacy legislation means for them. While there remains a fair degree of uncertainty, the outlines of what is going to happen are now becoming clearer.

When Does Privacy Legislation Take Effect?

For almost all opticians, the federal privacy act takes effect this coming January. On January 1, 2004, the *Personal Information Protection and Electronic Documents Act* comes fully into force. Ontario has circulated a draft *Privacy of Personal Information Act*, but it is highly unlikely that it will be enacted before this January. Opticians covered by the federal privacy act need to have their policies and procedures in place by then.

Who Does Privacy Legislation Apply To?

The privacy act is intended to cover the entire private sector. With very few exceptions, the privacy act applies to anyone who carries on “commercial activities”. That will include most opticians. Even if the government pays for the goods or services (e.g., social services), the privacy act will likely apply. Only opticians employed by a government body or a non-profit agency (e.g., a public hospital) that does not sell goods or services will be exempt.

The privacy act applies to any collection, use or disclosure of personal information. “Personal information” means any information about an identifiable individual that relates to their personal characteristics (e.g., gender, age, colour, ethnic background, education, family status), their health (e.g., health history, health conditions, health services received by them) or their activities and views (e.g., dealings with the optician, opinions expressed by an individual, religion, political involvement, a optician’s view or evaluation of an individual). Personal information is to be contrasted with business information (e.g., an individual’s business address and telephone number), which is not protected by the privacy act.

What Has To Be Done?

Each organization must appoint an Information Officer (sometimes called a Privacy Officer) and develop and publish its privacy policy. The Information Officer should be a senior person in the organization. The Information Officer can be an outsider hired by an organization to perform this role, but that may make it more difficult for the organization to develop a privacy policy that fits its office or practice.

The Information Officer is responsible for overseeing an organization's compliance with its privacy obligations. This privacy policy would cover the following issues:

- reviewing the organization's policies and practices for collecting, using and disclosing personal information (including conducting an audit of the current personal information practices of the organization);
- implementing procedures to safeguard personal information;
- ensuring individuals (e.g., clients) have the right to access and correct any personal information about themselves held by the organization;
- implementing a retention and destruction of information policy;
- training the organization's staff;
- acting as a contact person for inquiries from the public or clients; and
- ensuring there is a process for handling complaints made about the organization's information practices.

Opticians must also make sure that their organization has privacy policies dealing with all of these issues. These policies must be made available to the public. This public access obligation might be met by posting the policy on the organization's website or in its reception area. Alternatively, a copy can be provided to new clients on their first visit and to anyone else upon request. The policies have to be understandable.

Privacy policies apply on an "organizational" level. Often the identity of the organization is obvious because the sole operator, partnership or corporation is well defined. However, where a group of people or entities work together in a loose affiliation, there may be more than one way to define the organization. Opticians and their business associates can then decide who their organization will be. For example, every optician can have his or her own privacy policy. Or, opticians working with others (e.g., in a multidisciplinary clinic) can join together to form a broader organization with one privacy policy covering them all. It just depends on what is most convenient for everyone. Everyone within an organization has to agree to be monitored by the Information Officer. Also organizations will need special consent to disclose personal information outside of the organization.

What Are The Restrictions On The Collection, Use And Disclosure Of Personal Information?

As a general rule, opticians need to obtain informed consent for the collection, use and disclosure of personal information. This consent is distinct from the consent for treatment. Like any consent, it can be obtained in writing, verbally or by implied consent. In the traditional circumstance of a optician collecting information directly from the client solely for the purpose of providing services to the client, consent may be implied. However, any departure from this simple approach creates some new obligations for obtaining informed consent. In real life, the simple approach is not usually enough.

Areas in which some change may be required include the following:

- ❑ Where the optician collects information about other individuals (e.g., a family history).
- ❑ Where the optician collects information about the client from other persons (e.g., from previous opticians for the client, from family members of the client).
- ❑ Where the optician collects information to be shared with others who are also advising or providing services to the client (i.e., in a team treatment approach).
- ❑ Where there is the likelihood of an ongoing relationship and the information will be used for ongoing services, especially if this is not obvious to the client (e.g., collecting a baseline assessment of a client's health to ensure that one can provide broader treatment, if necessary, later on).
- ❑ Where third parties will have access to the information (e.g., for a legal, billing or financing purposes).
- ❑ Where the optician will use the information for related purposes (e.g., for billing the client or a third party later).
- ❑ Where the optician will use or disclose the information for secondary purposes (quality control by the organization, regulatory accountability, research).
- ❑ Where the optician might sell the practice later on and will need to provide prospective purchasers with access to client information to help the purchaser conduct a due diligence review.

In any of these circumstances, the optician should at a minimum explain the purposes for which the information is being collected and obtain some form of consent. Often the consent process can be a brief oral discussion with the client. Giving the client a handout setting out the optician's usual information practices and checking with the client that he or she understands the handout would often be sufficient. Alternatively, obtaining a written consent at a client's first visit may work in many circumstances. While the Information and Privacy Commissioner is leery of obtaining blanket consents, it may be that, for the usual private practice, this may be appropriate and sufficient.

There are some exceptions that permit opticians to collect information without consent. The most common example is where the purpose is to investigate a breach of law or contract and obtaining consent would compromise the investigation (e.g., suspected insurance fraud by a client; helping a client deal with a third party who injured the client). Certain emergency situations (e.g., medical crisis) may permit the collection, use or disclosure of information without consent as well.

Opticians are also obliged to collect the least amount of personal information that is consistent with the purposes for which it was collected. For example, collecting an individual's Social Insurance Number is usually not necessary. One should not routinely collect a client's home address (unless the client wants something to be sent there). Opticians should not collect financial information about a client who pays the full account at the time of service.

What Kind Of Safeguards Are Needed?

Most opticians are already careful to preserve their client's confidentiality. However, when setting out the safeguard policies in writing, opticians may wish to review some of their practices. For example, can people see confidential files or computer screens when walking through the office or clinic? Is all personal information shredded before being put in the recycling box? The Information and Privacy Commissioner strongly disapproves of sending personal information through regular email over the internet.

What Are Access And Correction Rights?

A fundamental principle of the privacy act is that any individual has the right to request and see any personal information opticians hold about them. In fact, opticians are required to help individuals make such a request (e.g., explain the filing system so the person knows what to ask for) and to assist them in understanding the information (e.g., explain abbreviations and technical terms). There are a few exceptions where access can be restricted (e.g., where the disclosure will reveal personal information about another individual or will reveal trade secrets), but these are narrow. Opticians will also have to tell individuals to whom the organization has sent or forwarded the personal information about them.

If the individual believes any of the personal information is wrong, he or she can ask that it be corrected. The organization must correct any information it agrees is wrong. The organization must also notify any third parties who received the wrong information of the correction. Where the client and the organization cannot agree that an error has been made then the organization must record the disagreement and notify any third parties who received the contested information. Disagreements about corrections can be taken to the Information and Privacy Commissioner who may review the situation.

What Should An Internal Complaint System Look Like?

Organizations must also have an internal complaints system to handle concerns about their privacy practices. The internal complaints system should have the following features:

- a designated individual in the organization (perhaps the Information Officer) to receive and ensure the prompt investigation and response to all complaints;
- an easily accessible and simple to use complaints procedure that at a minimum includes:
 - acknowledging receipt of the complaint,
 - investigating it, and
 - providing a decision with reasons;
- a process for the organization to respond appropriately to complaints that are justified including making changes to its privacy policies; and
- notifying the public of external recourses including the optician's College and the federal Information and Privacy Commissioner.

Who Ensures Compliance With The Privacy Legislation?

Opticians will be held accountable to both the federal Information and Privacy Commissioner and, to a lesser extent, their own College, in respect of their compliance with the privacy act.

The federal Information and Privacy Commissioner has oversight of the privacy act and functions as an ombudsman. The Commissioner has the following responsibilities:

- ❑ investigating complaints about an organization's personal information handling practices including entering the organization's premises and summoning documents and witnesses;
- ❑ mediating and conciliating such complaints;
- ❑ auditing the personal information handling practices of an organization;
- ❑ making a public report of poor personal information practices by an organization;
- ❑ seeking remedies for a breach of the privacy act in the Federal Court of Canada.

Once the Commissioner has issued a report, either the complainant or the Commissioner can then apply to the Federal Court of Canada for one or more of the following remedies:

- ❑ an order for the organization to correct its personal information handling practices;
- ❑ an order for the organization to publish a notice of corrective action; or
- ❑ an award of damages for any humiliation of the complainant.

All indications are that the current Information and Privacy Commissioner tends to be educational rather than punitive in his enforcement style. However, it is still better to avoid a complaint than having to deal with one.

The College may also hold the optician accountable for his or her privacy practices. Where the conduct involves a breach of core professional values, the College will have an additional reason to take regulatory action. Even where core professional values are not breached, every optician is generally obliged to comply with the law, especially those designed to protect the public or which reflect on the optician's suitability to be a member of the profession. Many breaches of the privacy act by an optician may warrant some regulatory action.

Where To Start?

The privacy act may seem like a lot of work. However, the key is for opticians to develop a privacy policy. A privacy policy provides a process for opticians to review and revise their organization's practices and to obtain the consent from clients in the future. With a few adjustments to existing practices and informed consent from clients, most opticians will be ready for the new privacy era.