

PRIVACY LEGISLATION CHECKLIST FOR OPTOMETRY PRACTICES

On January 01, 2004, Alberta (as well as the rest of Canada) joined the majority of the rest of the world in setting standards regarding the collection, use and disclosure of personal information.

The principles involved are fairly straight forward: Do not take more information than you need to do the job; use the information for the purposes for which it was collected; make sure the information is accurate; let patients see what information you have on them; keep the information secure; and, ensure proper measures are taken when the information is disposed of.

In order to ensure that your practice complies with the various privacy and confidentiality legislation, you should review the following checklist and make procedural and policy changes as required. The Alberta College of Optometrists (ACO) wish to advise that the information contained in this checklist is not exhaustive and is only intended as a guideline. Each recipient of this checklist is advised to obtain their own independent legal advice regarding privacy matters and legislation.

1) **ORGANIZE**

- Make an organizational commitment to privacy.
- Make a plan that will take your practice to compliance.
- Review and become familiar with this checklist as well as other privacy templates and policy statements.
- Designate an individual who is ultimately responsible for your practice's compliance with the Privacy Legislation.

It is anticipated that in most offices, one of the optometrists or the office manager will be assigned the responsibility of being the designated Office Privacy Officer. Each individual clinic or office must have their own privacy officer. Therefore, multi-office practices will need to designate a privacy officer in each location. Ensure that this individual has the authority, support and resources to do a proper job. This individual will be the contact person for patients and/or employees when privacy issues arise.

2) CONDUCT AN INTERNAL AUDIT

- Review and amend arrangements, contracts and agreements between your practice and any consultants, advisors or other parties who may have access to personal information to require them to honor your privacy policy.
- Perform a systematic review of your practice's operating policies and identify gaps where further direction and/or amendments are required.
- Identify what personal information is being collected, used, held or disclosed
- Examine why and how information is collected.
- Determine the location of the patient records, who has access to them, why they are kept, where and in what format they are kept.
- Examine how personal information is used, handled, secured and disclosed.
- Examine who has access to the personal information and who has the need to have such access.
- Examine when and how personal information is disposed of.
- Examine whether consent to the collection, use and/or distribution of personal information has been obtained from the patient or legal guardian.
- Examine your practice's existing policies and procedures respecting privacy and confidentiality.
- Determine whether your current policies are compliant with privacy legislation, industry standards, and best practices.
- Consider risk management and insurance issues.

3) CREATE POLICIES AND PROCEDURES

- Develop a list of approved purposes for the collection, use or distribution of personal information.
- Decide on type of consent required in specific areas.

- Develop a Privacy Statement and an Office Privacy Manual.
- Identify mandatory disclosure obligations (i.e. statutory, banking etc.)
- Establish policies, guidelines and procedures regarding:
 - Approved purposes for and limitations concerning the collection, use or disclosure of personal information.
 - Identification and documentation of your practice's purpose for the collection, use and disclosure of personal information.
 - How your practice can ensure personal information is complete, accurate and up-to-date.
 - Retention of personal information including minimum and maximum retention periods.
 - The destruction of personal information.
 - How your practice will receive and respond to complaints and inquiries about your policies or practices.
 - Methods to be used to obtain consent.
 - How individuals will be allowed to access their own personal information.
 - Personal information used for recruitment and employment purposes.
 - The correction of personal information.
 - Fees for access to personal information.
 - Responses to commissioner's requests.
- Establish policies and procedures regarding the safeguarding of personal information. Outline steps your practice will take and determine how your practice can ensure these steps are successfully implemented. Specifically, practices should address physical measures necessary to protect personal information (example locks), organizational measures in order to protect personal information (example security clearance), and technological measures to protect personal information (example passwords, encryption).

Possible Suggestions Include:

- Restricting specific areas to staff only.
- Ensuring that non-staff are supervised at all times when in areas that have access to personal information.
- Obtaining privacy and confidentiality oaths from both staff and non-staff who have access to information.
- Ensuring that personal information is adequately safeguarded at home or in transit.
- Ensuring that personal information stored in electronic form is protected (eg., passwords, encryption, firewalls, anti-virus protection).
- Ensuring that the fax machine is located in a secure area so that incoming faxes cannot be improperly accessed.
- Equipping fax machines with a keylock or confidential mailbox, if necessary.
- When sending outgoing faxes, the fax cover sheet should identify the sender and intended recipient, and indicate that the recipient has approved the fax number and ensured the privacy of their incoming fax machine. The fax cover sheets should also include a confidentiality clause.
- Ensuring that correspondence containing personal information is marked private and confidential.
- Avoiding regular e-mail when transferring sensitive personal information (unless the person about whom the personal information relates so consents or the file is password protected and the information is encrypted).
- Keeping a clean desk and office if patients and/or other non-staff members enter office.
- Amending messages sent by e-mail or fax such that identifying information is removed so the person's identity is made anonymous, or alternatively encryption should be used.
- Ensuring that appropriate security measures are in place when practices collect personal information over the internet.
- Shredding documents containing personal information.

- Developing practice brochures concerning privacy policies.
- Developing practice consent forms.

4) **IMPLEMENTATION**

- Train staff regarding your practice's policies and practices (emphasizing confidentiality).
- Ensure that the following information is available to the public:
 - Name or title, phone number and address of person accountable for policies, complaints or inquiries.
 - The means of gaining access to personal information.
 - A description of the type of personal information under your practice's custody or control.
 - A general description of your practice's purpose for collection and its use of personal information.
 - Brochures or other information explaining your practice's policies, standards or codes.
 - A description of the personal information made available to related practices, organizations (example, a subsidiary) or other parties.
- Emphasize to employees that those who remove information from the office must adequately safeguard the information.
- Implement and advertise you practice's privacy policies and practices.
- Insert privacy clauses in Agreements.
- Have employees and other necessary parties sign privacy statements and take privacy oaths.
- Identify privileged materials.
- Amend insurance coverage (if required).

Use the enclosed templates and documents to develop an office manual for in-office and internet use. Post your Office Privacy Policy in a conspicuous place in the office.

5) MAINTAIN COMPLIANCE

- Maintain compliance with privacy legislation.
- Ensure ongoing training and education.
- Monitor and enforce policies and procedures.
- Respond to complaints and access requests.
- Respond to enforcement authorities.
- Be proactive, and review and revise plans on a regular basis.

The training of optometrists and staff is not considered a one-time event. We encourage each practice to hold periodic updates at your regular staff meetings to ensure that everyone understands their responsibilities. We also encourage each office to notify patients of your office privacy policy in any mass mailings, notices or newsletters you send out. **Remember that all mailings to patients are to be sent in a sealed envelope.**

If you have any further questions, please feel free to contact:

The Alberta College of Optometrists – (780) 466-5999

- or -

The Alberta Government Privacy Help Desk – privacyhelpdesk@gov.ab.ca