Privacy of personal information is an important principle to Brisson Leis and Associates. We are committed to collecting, using and disclosing personal information responsibly and only to the extent necessary for the vision care services and products that we provide. We also try to be open and transparent as to how we handle personal information. This document describes our privacy policies.

Privacy Policy

Effective: January 1, 2004
Revised:
Information Officer: Judy Brisson

We are required to comply with the terms of this privacy policy while it is in effect. We reserve the right to modify the policy at any time and the revised privacy policy will apply to all protected health information that we currently have as well as to information that we may generate in the future. This policy will be in effect from January 1, 2004 until the date an amended policy is published. If we change the privacy policy, we will post the amendments in our office, have copies available and publish it on our website.

What is Personal Information?
Personal information is information about an identifiable individual. Personal information includes information that relates to their personal characteristics (e.g., gender, age, income, home address or phone number, ethnic background, family status), their health (e.g., health history, health conditions, health services received by them) or their activities and views (e.g., religion, politics, opinions expressed by an individual, an opinion 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 privacy legislation.

Who We Are

Brisson Leis and Associates includes any optometrist or health care professional, all employees, staff and student trainees authorized to collect, use or disclose personal information working in our office or under our supervision. We use a number of consultants and agencies that may, in the course of their duties, have limited access to personal information we hold. These include, but are not limited to, computer consultants, office security and maintenance, bookkeepers and accountants, temporary workers to cover holidays, credit card companies, collection agencies, website managers, cleaners and lawyers. We restrict their access to any personal information we hold as much as is reasonably possible. We ave their assurance that they follow appropriate privacy principles or we have signed privacy agreements with them

We Collect Personal Information: Primary Purposes

Personal Information About Patients

Brisson Leis and Associates collects, uses and discloses personal information in order to serve our patients. For our patients, the primary purpose for collecting personal information is to provide vision care services. We collect personal information in order to help us assess what their eye care needs are, to advise them of their options and then to provide the eye 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 may communicate this information to other regulated health practitioners, technicians, or individuals authorized to work in our practice as part of a patient's continuing care. It would be rare for us to collect information without the patient's implied consent, but this might occur in an emergency (e.g., the patient cannot communicate) or where we believe the patient would consent if asked and it is impractical to obtain consent (e.g., a family member passing a message on from our patient where we have no reason to believe that the message is not genuine).

The personal information we collect about patients for these primary purposes may include:

- Name and home contact information
- Date of Birth
- Identifying features such as eye colour
- Gender, colour, languare, ethnicity
- Education, occupation, hobbies, work hours,
- Marital status, sexual history, sexual orientation
- Social Status
- Personal and family health history
- Health measurements, examination results, samples
- Health conditions, assessment results, diagnoses
- Health information collected in the course of providing services
- Prognosis or other opinions formed during assessment and treatment
- Compliance with assessment and treatment
- Reasons for discharge, discharge condition and recommendations
- Transaction history
- Opinions expressed by the person
- Community involvements
- Religion
- Political involvement
- Website cookies
- Existence of a dispute with us
- Intentions to obtain goods or services
- Involvement with us
- Letters written to us by the person
- Letters written to us about the person
- Views, evaluations, opinions by us about the person

Our authority to collect personal information about patients for these primary purposes is one or more of implied consent, verbal consent (documented), written consent, or where collection is in the interests of the person and timely consent is not possible. We will attempt to have written consent from all patients.

Personal Information About Members of the General Public
For members of the general public, our primary purposes for collecting personal information is to make them aware of optometry services in general or our practice in particular, or to provide notice of special events. While we try to use work contact information, we might collect home addresses, fax numbers and e-mail addresses.

On our website we only collect, with the exception of cookies, the personal information provided and only use that information for the purpose for which it was provided. Cookies are used only to assist navigation of the website and are not used to monitor users.

Our authority to collect personal information about the general public for this primary purpose is implied consent.

Personal Information About Staff, Volunteers and Students
For people who work, volunteer or observe us, our primary purpose for collecting personal information is to ensure that we can contact them in the future and for necessary work-related communication. It is rare for us to collect such information without prior consent, but it might happen in the case of a health emergency or to investigate a possible breach of law. We disclose information about the work related performance of staff, volunteers or students only as authorized by them if they wish a letter of reference or an evaluation.

The personal information we collect about staff, volunteers, and students for this primary purpose may include:

- Name, home contact information, date of Birth
- Identification numbers such as social insurance number
- Gender
- Education, occupation
- Work hours
- IncomeTransaction history
- Intentions Involvement with us
- Views, evaluations or opinions by us about the person

Our authority to collect personal information about staff, volunteers, and students for this primary purposes is one or more of implied consent, verbal consent (documented)and written consent.

We Collect Personal Information: Related and Secondary Purposes

We also collect, use and disclose information for purposes related to or secondary to our primary purposes. Some of the information used for related and secondary purposes will have been collected for our primary purposes; other, additional information, may be collected for related or secondary purposes. Our secondary purposes are detailed in Table 1.

Related Purposes
Optometrists are regulated by the College of Optometrists of Ontario who may inspect our records and interview our staff as a part of their regulatory activities in the public interest. As professionals, we report serious misconduct, incompetence or incapacity of other practitioners, whether they belong to other organizations or our own. Also, our practice believes that it should report information suggesting serious illegal behavior to the authorities. External regulators have their own strict privacy obligations. Sometimes these reports include personal information about our patients or other individuals to support the concern.

Various government agencies (e.g., Canada Customs and Revenue Agency, Information and Privacy Commissioner, Human Rights Commission, etc.) have the authority to review our files and interview our staff as a part of their mandates. In these circumstances, we may consult with professionals (e.g., lawyers, accountants) who will investigate the matter and report back to us.

If Brisson, Leis and Associates or its assets were to be sold, the prospective purchaser would want to conduct a due diligence review of the practice records to ensure that it is a viable business that has been honestly portrayed to the prospective purchaser. This due diligence may involve some review that may include releasing personal information. The prospective purchaser would not be allowed to remove or record personal information and, before being provided a review of the clinical files and records, the prospective purchaser must provide a written promise to keep all personal information confidential. Only reputable purchasers who have already agreed to purchase the practice or its assets would be provided, at closing, complete access to personal information. The purchaser would be required to maintain the same principles of privacy as established under the present privacy legislation.

Our authority to collect and use personal information for these related purposes is one or more of implied consent, verbal consent, written consent or investigation of breach of law/contract where consent would compromise the investigation.

Patients can choose not to be part of some of the secondary purposes by declining in writing to receive notices and by paying for services in cash in advance. Patients cannot opt out of the related purposes.

A patient may ask us, in writing, to restrict our use and disclosure of personal information at any time. We will discontinue the use or disclosure of a patient's personal information after a written revocation of the patient's implied or informed consent is received. We cannot, however, restrict our use and disclosure of personal information for some related or secondary purposes.

Protecting Personal Information

Brisson, Leis and Associates understands the importance of protecting personal information. For that reason, we have established the following policies:

Employee Training
Employees, including temporary staff, are trained to collect, use and disclose personal information only as necessary to fulfill their duties and in accordance with our privacy policy. Employees will be retrained at least annually

Paper Information
Paper information is either under supervision or secured in a locked or restricted area. In areas restricted to staff, no non staff will be permitted entry without continuous supervision. All non staff who require access must sign confidentiality agreements. In areas open to non staff, the area will be supervised at all times. Every effort will be made to avoid having paper information visible to non staff. Where practical, information will be locked away after hours.

When transporting paper information, the information must be in the personal custody of staff at all times during transit. The information must be locked away out of sight while unattended. If paper information is used in a home office, it must be locked away in a desk, filing cabinet or separate room while unattended and no one, other than staff, may have the key.

Electronic Information
Electronic information is either under supervision or secured in a locked or restricted area at all times. Passwords and screen savers are used on computers and computer monitors are shielded so that information on the screen is not visible to non staff. In areas restricted to staff, no non staff will be permitted entry without continuous supervision. All non staff who require access must sign confidentiality agreements. In areas open to non staff, the area will be supervised at all times. Every effort will be made to avoid having electronic information visible to non staff and personal information is not left on unattended screens. Our fax machine is in a secure location.

When transporting electronic information, the information must be in the personal custody of staff at all times during transit. The information must be locked away out of sight while unattended. If electronic information is used in a home office, it must be locked away in a desk, filing cabinet or separate room while unattended and no one, other than staff, may have the key.

Transfer of Information
Paper information will be transferred in sealed envelopes marked private and confidential, sent by Canada Post, reputable courier, delivered by staff or picked up by a person who asks for it by name of the recipient. Sealed envelopes will be kept out of sight until picked up.

Newsletters and other general information will be sent in sealed, addressed envelopes. Post cards will be used only with written consent of recipients for information collected prior to January 1, 2004 or with implied consent for information collected prior to January 1, 2004.

We control mailings and notices sent to patients and do not share mailing lists with other organizations, health professionals or agencies.

Electronic information is transferred through a direct line or is through a disk, CD or other storage medium transferred in sealed box or envelope marked private and confidential, sent by Canada Post, reputable courier, by staff or picked up in person by a person who asks for it by name of the recipient. Email or other internet communication is with the consent of the person to whom the personal information relates or is anonymized or encrypted.

Fax transmissions have one of the following safeguards:

- the fax number has been approved by the person to whom the information applies
- the fax is to another health professional, agency, organization or laboratory that is expected to keep information private
- the recipient has a Privacy Policy
- the recipient has advised that the fax machine is securely located and there is no basis to doubt the assurance

General Safeguards

Staff (including temporary workers, volunteers and students) are trained

- to know the importance of the privacy of personal information
- to provide access to personal information is on a need to know basis
- to collect verbal personal information in such a manner that the information is not overheard by persons other than the patient or practice members
- to recognize and avoid being pumped for information
- to ensure that discarded personal information is not placed in the regular garbage system, but is shredded or destroyed
- to avoid discussing personal information in public places
- to know that breach of the Privacy Policy will result in discipline
- annually, included review and update of the Privacy Policy
- to minimize the amount of personal information sent with orders when ordering materials or products for specific patients
- to notify individuals if their personal information has been improperly used or disclosed

External consultants, contract workers, maintenance workers and others with access to personal information must enter into privacy agreements with us.

The Information Officer or delegate regularly monitors compliance with the Privacy Policy.

The physical layout of the office and operating procedures are reviewed and modified to enhance privacy.

Retention and Destruction of Personal Information

Patients or other individuals we deal with may have questions about our products or services after they have been received.. We also provide ongoing vision care services for many of our patients over a period of months or years for which our previous records are helpful. We need to retain personal information for some time to ensure that we can answer these questions and provide those services. Our regulatory College requires us to retain our patient records for a minimum of 10 years after the last contact or for ten years after the year in which the patient turned 18.

For the protection of the optometrist and patient under malpractice law, records will be kept indefinitely. We will destroy patient records ten years after the patient's date of death, if we are aware of the date of death.

We minimize the volume of personal information retained by periodically destroying duplicate or working copies of information when the main record containing the information is retained. We destroy paper files containing personal information by shredding. As an alternative to shredding, we may send the entire patient file to the patient. We destroy electronic information by deleting it when the hardware or storage vehicle is retained and by physical destruction when the hardware or storage vehicle is discarded.

A patient may ask us, in writing, to restrict our use and disclosure of personal information at any time. We will discontinue the use or disclosure of a patient's personal information after a written revocation of the patient's implied or informed consent is received. We cannot, however, restrict our use and disclosure of personal information for some related or secondary purposes.

Patient Access to and Correction of Personal Information

Patients have the right to see what personal information we hold about them. We may ask the patient to request access to their records in writing an we may need to confirm the patient's identity before providing them with access to their records. If we cannot give the patient access, we will notify the patient within 30 days of the request and provide the reason, as best we can, as to why we cannot provide access.

We will assist patients in identifying what records we have that contain their personal information and we will assist the patient in understanding the information (e.g., short forms, technical language, etc.). We may charge a nominal fee for such requests and we will schedule access to a time convenient for both the patient and Brisson, Leis and Associates.

Patients have the right to ask for incorrect factual information to be corrected. Patients do not have the right to ask for correction of any professional opinions we may have formed. We may ask patients to provide documentation that our files are incorrect. Where a mistake has been made, we will make the correction without obliterating the original entry and, when possible, notify anyone to whom we sent the incorrect information. If we do not agree that a mistake has been made, we will include in our file a brief statement from the patient on the point and, when possible, we will forward that statement to anyone else who received the earlier information.

Complaints System

A patient may make a formal complaint about our privacy practices in writing to our Information Officer, who will acknowledge receipt of the complaint, ensure that it is investigated promptly and are provide the complainant with a formal decision and reasons in writing. The Information Officer may delegate investigation to another person. Investigation will be timely, with a decision expected within 30 days of receiving the complaint.

The Information Officer will ensure compliance with Brisson, Leis and Associates' policies in respect of the complaint and may, in consultation with staff, change the way we handle information and our policy. In some cases, the Information Officer may award a refund, credit or financial compensation to the complainant.

The complainant will be informed that, if not satisfied with the decision, that further complaints can be made to the Federal Information and Privacy Commissioner or to the College of Optometrists of Ontario. The complainant will be provided with contact information for those two bodies.

Monitoring Compliance with the Privacy Policy

The Information Officer will ensure that an Privacy Policy Compliance Report is produced annually, that the Policy is reviewed and updated annually and that refresher privacy training is provided to all staff annually.

Records of the annual Policy review and update and of the annual Compliance Report will be kept.

Table 1, Secondary Purposes

Purpose	Additional Information	Limitations in Collection	Authority to Collect (one of)
Invoicing and Collection To invoice patients for services, products or treatments that were not paid for at the time the service was provided, to process credit card payments or to collect unpaid accounts	Credit or loan data Banking information Credit Card Numbers Cheque verification information Alternate billing/delivery address or information	Only for patients who have not paid at the time of service or delivery of goods, who pay by personal cheque or who use post dated credit card payment	Implied consent for information obtained prior to January 1, 2004 Verbal consent (documented) Written consent Investigation of breach of law/contract and consent would compromise
Recall Visits To advise patients that their vision and eye care needs or treatment should be reviewed	N/A	Only for patients who have consented to receive recall notices	Implied consent for information obtained prior to January 1, 2004 Verbal consent (documented Written consent
Special Offers and Promotions To advise patients, prospective patients, and others of special events , products or opportunities that we have available	N/A	Only for patients who have consented to receive offers	Implied consent for information obtained prior to January 1, 2004 Verbal consent (documented Written consent
Third Party Billing The cost of services we provide is paid by third parties. Third-party payers usually have the patient's consent or legislative authority to direct us to collect and disclose the personal information needed to demonstrate patient entitlement to funding.	Identification numbers including OHIP, UHIP and other insurance numbers Identification numbers such as Veteran Affairs , WCSB, Status Indian Band	Only for patients receiving goods or services paid for by third parties	Implied consent Verbal consent (documented) Written consent Investigation of breach of law/contract and consent would compromise
Quality Control and Risk Management to reviews patient and other files to ensure that we provide high quality services, including assessing the performance of staff. In addition, external consultants may, on our behalf, do audits and continuing quality improvement reviews of our practice, including reviewing patient files and interviewing our staff.	Usually no information is collected. In rare cases, our practice or our consultants may make inquiries to verify that the information we have about patients is accurate.	No limitations	Implied consent for information obtained prior to January 1, 2004 Verbal consent (documented) Written consent