PRIVACY POLICY

Objective
To ensure that:

(a) Myself is in compliance with regulatory and self-regulatory requirements regarding Privacy ("Regulations");
(b) client's Privacy is handled in a professional manner, in a secure environment and appropriately monitored;

Policies
Person(s) Responsible:

(1) Myself is hereby designated as responsible for the application of this policy;

There are 10 principles that we must follow to be in compliance with PIPEDA
(Personal Information Protection and Electronic Documents Act) ***https://www.priv.gc.ca/resource/fs-fi/02_05_d_16_e.asp***

1. Accountability: An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. Identifying Purposes: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. Consent: The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except when inappropriate.

4. Limiting Collection: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. Limiting Use, Disclosure, and Retention: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law. Personal information shall be retained only as long as necessary for fulfillment of those purposes.

6. Accuracy: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. Safeguards: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. Openness: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. Individual Access: Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Challenging Compliance: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals for the organization's compliance.

Applicability
The Act is applicable to personal information only. However, it has been suggested that in keeping with the spirit of the law, PIPEDA should also be applied to information obtained on closely-held corporations which would be most, if not, all of our corporate clients.

The Privacy Officer
Myself is the Privacy Officer and all inquiries / complaints shall be directed to me.

Information Collection and Use
We collect the information required for us to complete the task for which we are engaged, whether that is insurance, money products or financial plans.

This information may include:

Name
Date of Birth/Date of Death
Social Insurance Number
Home Address (s)
Work Address (s)
Telephone Number (s)
Fax Number (s)
Email Address (s)
Marital Status
Financial Income/Expense Info
Lawyer (s)
Banker (s)
Bank information
Investment advisor and account information
Financial Statements

Consent
The consent for us to establish a file and collect and maintain personal information is included in the completed applications from our supplier companies.

Protection of Personal Information
I have the only access to client information and must understand the need to keep the information protected and confidential.

Retention of Personal Information
We will retain our completed client files for a minimum period of seven years. Any files where there were complaints or legal issues will be kept indefinitely.

Privacy Choices
Clients may request copies of our privacy policies and procedures at any time.

Clients may request access to their information. We must respond to this request as quickly as possible as but no later than 30 days after the receipt of the request.

Clients may withdraw their consent at any time by contacting our Privacy Officer. However, they will be made aware that failure to provide adequate information may prevent us from completing the task for which we were engaged.

Clients may file complaints about our privacy procedures. Complaints should be received in writing and forwarded to the Privacy Officer. The Privacy Officer will then deal with the complaint which must include contacting the individual making the complaint.

Exception to client access
Organizations must refuse an individual access to personal information:

- if it would reveal personal information about another individual* unless there is consent or a life-threatening situation
- If the organization has disclosed information to a government institution for law enforcement or national security reasons. Upon request, the government institution may instruct the organization to refuse access or not to reveal that the information has been released. The organization must refuse the request and notify the Privacy Commissioner. The organization cannot inform the individual of the disclosure to the government institution, or that the institution was notified of the request, or that the Privacy Commissioner was notified of the refusal.

Organizations may refuse access to personal information if the information falls under one of the following:

- solicitor-client privilege
- confidential commercial information
- disclosure could harm an individual's life or security
- it was collected without the individual's knowledge or consent to ensure its availability and accuracy, and the collection was required to investigate a breach of an agreement or contravention of a federal or provincial law (the Privacy Commissioner must be notified)

- It was generated in the course of a formal dispute resolution process.

Privacy Breach

Should we become aware of a privacy breach, we will review our privacy policy and amend as required.

If necessary, the affected client/s will be notified as well as the insurance carrier.

If necessary, we will notify our E&O insurance carrier.

SCHEDULE A
(Office Safeguards)

- Disclaimer on all e-mail, faxes etc.
- Clean desk policy
- All confidential materials to be removed from view at end of day, lunch, break time etc
- No information in view of public, on desks
- No discussion of client files outside the office
- Empty shredding file daily
- Lock shredding bin
- Password protected screensavers on all computers
- Any inquiry should be directed to the Privacy Officer
- All file cabinets to be locked
- All waste paper containing personal information to be shredded
- Any person, client or broker, must identify themselves by a broker code, SIN #, DOB, etc to confirm identity
- Employees must be furnished with a copy of the privacy policy and sign off acknowledging that they have read it
- Staff are required to sign a confidentiality agreement
- Fax is set up to keep faxes in memory when office is closed
- Office is locked and alarmed and professionally monitored
- Complaint logs are maintained
- Certificates of Destruction are received for shredded material

Our Privacy Practices

Personal information is information that refers to you, specifically.

For *any* financial product or service you obtain, we will tell you the purposes for which we need the personal information we collect.

We will use fair and lawful means to collect your personal information. We will only collect information that is pertinent and consistent with the purposes of the collection. Whenever practical, we will collect the required Information directly from *you,* or from *your* authorized representative(s), in completed applications and forms, through other means of correspondence, such as the telephone, mail or the Internet, and through *your* business dealings with us.

In some cases, and with your consent, we may need to ask an independent source to verify or provide supplemental information these sources could include service providers we retain, other insurance companies or financial Institutions, *your* employer or credit reporting agencies In the case of your medical or health-related information, additional sources could include healthcare providers or facilities.

If your information is being collected by telephone,
The call *may* be recorded or monitored for the following reasons:

- to establish a record of the information *you* provide,
  To take or verify instructions from *you,* to maintain quality service levels,
- to assist in staff training

If you are not comfortable with having your telephone calls recorded, you have the option of communicating
with us in writing, instead Where *you* have chosen to only communicate with us in writing, your written communications should request that *any* response to you be in writing, as well. We collect information from you and about you, only with *your* consent, or as required or permitted by law. In general, we will collect personal information such as your name, address, telephone number(s) or other identifying information, such as *your* Social Insurance Number (SIN) or date of birth.

The type of additional information we gather will depend on the type of product or service involved. For example, it would depend on whether the product or service is banking, insurance or investment related. The information gathered may be financial, which would include such information as place of employment,
annual income, assets and liabilities. It may be investment or advice related, requiring information on such things as *your* financial goals and retirement plans. If *you* are applying for insurance or group insurance benefits, it *may* also include health information or lifestyle related information, such as *your* occupation, travel history and plans, driving record or criminal record.

Generally, we collect, use and disclose *your* personal information to:

- Confirm your identity, and to protect both *you* and us against errors, fraud or other misrepresentations,
- Evaluate *your* financial needs and determine the suitability of our products and services for you,

Determine your eligibility for products and services,

Properly administer the products and services we provide, including the assessment of claims,

Comply with a variety of legal requirements, including any tax reporting obligations under the Quebec Ad respecting the Minister du Revenue

- Assist us to understand the current and future needs of our customers. for example, to conduct customer surveys and other forms of market research and analysis

we will only keep your personal information in our records for as long as it is needed to fulfill the identified purposes. or as required or permitted by law.

Personal information that is no longer required will be destroyed. erased or made anonymous.

- When \Ye destroy personal information, \Ye will use safeguards to prevent unauthorized access to the information during the destruction process.

Your SIN

There are a number of reasons why we may ask for your Social Insurance Number (SIN)

Where there may be interest income or other income to be reported, your SIN is required by law in order to meet tax reporting requirements under the federal Income Tax Ad, or the Quebec Ad respecting the Minister du
Revenue.

With your consent, we may also use your SIN as a unique identifier, to keep your personal information separate from that of other customers. or individuals with similar names, and to help maintain the integrity and accuracy of your personal information. For example, where it is appropriate to verify your audit history, we may use your SIN to ensure that the audit information \Ye are asking for - and receiving - is about you. rather than someone else with the same or similar name.

You may not to have your SIN used for purposes other than as required by law, however, as explained earlier, this may affected our ability to fully ensure the accuracy and integrity of your personal information. We coiled. use and share your personal information only for disclosed purposes related to the product and services \Ye offer, and only with your consent, or as permitted or required by law. Your consent may be expressed in writing. or it may be given verbally, electronically, or through our, or your authorized representative {s), such as your financial services advisor.

If you present your benefit identification card to your healthcare provider. instead of paying for the prescription or procedure directly, it is understood that you are giving your consent for the healthcare provider to provide your personal information to us, in order for us to process the claim payment.

You may withhold or withdraw your consent for us to coil. use and disclose your personal information, as long as there are no legal or contra dual reasons preventing you from doing so. Depending on the circumstances, however, withdrawal of your consent may impact our ability to continue to provide you with the products and services you have requested, or, in the case of insurance and group insurance benefits. it may prevent us from keeping your coverage in force, or properly evaluating and processing any claims.

Generally, the discourse of your personal information will be restricted to those who have a need for, and the right to. the information.

Your personal information will only be provided to, or be accessible by:

- Our employees. agents and representatives. who need the information in the performance of their duties for us.
- Our affiliates, to

- resolve your concerns about any related products and services with us
- assist in other required investigations Service providers, which need the information in the performance of their duties for us, and to satisfy their obligations to us,

- Any person or organization to whom you gave consent, and,
- Anyone who is otherwise authorized by law

In some cases, your personal information may be provided to these people, organizations and service providers in other provinces or jurisdictions outside Canada, and would therefore be subject to the Jaws of those provinces or jurisdictions.

Service Providers

We may use service providers to provide us with various services such as, printing, mail distribution, information technology, data storage, administration, marketing, (which would include mar1<et research and promotional services), paramedical, claims adjudication, Investigation and reinsurance. Where personal information is provided to our service providers, we will require them to protect the information in a manner that is consistent with our privacy policies and practices.

Accessing and amending your information

We will make all reasonable efforts to ensure that any personal information we collect and keep is as accurate, complete and as up-to-date as required for the identified purposes. To do so, we will rely to a large extent on you to provide us with accurate information and to inform us of changes, such as changes in your contact information. You have the right to access and verify your personal information maintained in our files, and to request that any factually inaccurate personal information be corrected, if appropriate. Depending on the circumstances, we may not always be able to give you access to all information, or there may be a charge for personal information that you request. Should this happen, we will let you know.

We are committed to protecting your information

We are committed to protecting your personal information from unauthorized access or use, by ensuring that the necessary physical, organizational and technological safeguards are in place, that are appropriate to the sensitivity of the information Essentially, this means that personal information is pro. tested:

- Physically, by building security measures and physical barriers,
- Organizationally, by our policies, procedures and access levels, and,
- Technologically by, for example, where appropriate, the use of passwords, firewalls, anti-virus and anonymzing software

All of our employees, representatives, agents and service providers, who act on our behalf, are required to abide by our privacy policies and practices.

If we receive a request to release your personal information, we will only do so upon satisfactory identification and proof of entitlement of the requestor, or as required or permitted by law.

If you have any questions or concerns about our privacy policies and practices, or you want to know more about the process for accessing and *I* or correcting your personal information, or opting-out of marketing offers, please contact us: