

COMPLIANCE PROGRAM FOR PRIVACY

Nadavot Financial Services
(10169536 Canada Inc.)

Compliance officer: David Emmanuel Kakon

Effective: September 1, 2018
Revised on: November 2, 2018

SECTION 1 – APPOINTMENT OF A COMPLIANCE OFFICER	1
SECTION 2 – POLICIES AND PROCEDURES	2
1. PRIVACY AND OUR BUSINESS	2
2. CONCERNS AND GENERAL INQUIRIES OR REQUESTS	3
2.1 CLIENT REQUESTS TO ACCESS PERSONAL INFORMATION	3
2.2 MISUSE OF PERSONAL INFORMATION:	3
2.3 PRIVACY INCIDENT/BREACH PROCESS	3
3. OBTAINING VALID, INFORMED CLIENT CONSENT	5
3.1 NEW ACCESS TO CLIENT INFORMATION	5
3.1.2 SUPPLIER CONTRACTS	6
3.2. BUSINESS TRANSACTIONS CONSENT EXCEPTION	7
3.2.1 <i>Buy/sell agreements</i>	7
3.2.2 <i>Agent of Record (AOR) changes</i>	7
4. COLLECTION OF PERSONAL INFORMATION	8
4.1 RECORDING CLIENT TELEPHONE CALLS	8
5. USE, DISCLOSURE AND RETENTION	9
5.1 SECURE DISPOSAL	9
5.2 RECORD RETENTION	9
6. SAFEGUARDS	10
6.1 TECHNOLOGICAL SAFEGUARDS	10
6.1.2 ENCRYPTION, ANTIVIRUS AND FIREWALLS	10
6.1.3 SCREEN SAVERS, USER ID AND PASSWORDS	10
6.1.4 SECURE EMAIL	11
6.2 PHYSICAL SAFEGUARDS	11
6.2.1 OFFICE DESIGN	11
6.2.2 <i>Computers and consumer devices</i>	11
6.2.3 <i>Desks and files</i>	12
6.3 <i>Communicating confidential information with others</i>	12
6.3.1 <i>Voicemail</i>	12
6.3.2 <i>Caller authentication</i>	12
6.3.3 <i>Email</i>	13
6.3.4 <i>Faxes</i>	13
6.4 <i>Organizational safeguards</i>	14
6.4.1 <i>Authorization and limiting access on a “need-to-know” basis</i>	14
6.4.2 <i>Confidentiality agreements</i>	14
7. ADOPTION OF POLICIES AND PROCEDURES	15
SECTION 3 – TRAINING PROGRAM	16
SECTION 4 – SELF-REVIEW	17
SECTION 5- REVIEWS AND AMENDMENTS TO THE COMPLIANCE PROGRAM FOR PRIVACY	20
DOCUMENT REVISION HISTORY	20
ADDITIONAL INFORMATION	20

Section 1 – Appointment of a compliance officer

The compliance officer (CO) is responsible for:

- The implementation, monitoring, updating and carrying out the compliance program which includes:
 - Policies and procedures
 - Training and awareness
 - Program self-review/assessment
- The privacy breach process, and client inquiries and complaints
- Reporting new risks, existing risks, monitoring and any legislative/regulatory changes that will impact the compliance program on a regular basis to senior decision makers within the practice

The CO should have the authority and the resources necessary to discharge his or her responsibilities effectively. The CO should hold a senior position within the practice that enables them to have direct access to senior decision makers. The CO may delegate certain duties to other employees however the compliance officer retains responsibility for the implementation of the compliance program.

The person below has been appointed to the position of compliance officer:

NAME: DAVID EMMANUEL KAKON

EMAIL: admin@nadavot.com

PHONE: (514) 613-3145 #3

POSITION: MANAGER

DAVID EMMANUEL KAKON
Compliance officer

SEPT 1 2018

ELIZABETH LIPKOWITZ
Principal/Senior decision maker

SEPT 1 2018

Section 2 – Policies and procedures

1. Privacy and our business

Clients provide personal information that is essential to the practice's business. Protecting this information is important to maintaining client trust and confidence. The federal privacy law, the *Personal Information Protection and Electronic Documents Act (PIPEDA)*, and Alberta, British Columbia and Quebec provincial privacy laws govern the collection, use and disclosure of personal information. Personal information is defined as any information about an identifiable individual, including health and financial information, as well as business information unless it's classified as "business contact information." This includes business title, business telephone

number and email, and information that's used in relation to the individual's employment, business or profession.

The practice is responsible for personal information under its control and for taking appropriate steps to safeguard the personal and confidential information in its possession. In some situations, this will mean adopting new business practices to safeguard personal information.

Policy

The practice makes information regarding its policies and procedures available to the public and abides by the privacy guidelines of the insurance companies it represents.

2. Concerns and general inquiries or requests

Procedure

Any concerns, general inquiries or requests related to privacy and the practice are forwarded to the practice's compliance officer. The compliance officer will review and acknowledge requests within 24 hours or if away, redirect appropriately for handling. The client will be updated on the compliance officer's progress with regard to the concern with complete documentation of the concern and related activities kept in the client file.

2.1 Client requests to access personal information

Under privacy laws, clients have the right to request access to their personal information held in files maintained by either the practice or insurance company and to challenge its accuracy, if need be.

Procedure

Any client access requests for personal information held in the practice's client files are forwarded to the practice's compliance officer to accommodate the client request as quickly as possible and no later than 30 days after receipt of the request.

Correct or amend any personal information if its accuracy and completeness is challenged and found to be deficient. Note any disagreement on the file and advise third parties where appropriate.

Immediately contact carrier ombudsman if a client requests access to his/her personal information held with Carrier.

2.2 Misuse of personal information:

Procedure

Any misuse of personal information or potential breach of security safeguards relating to Carrier products and services are reported immediately to Carrier's chief compliance officer by the firm's compliance officer.

2.3 Privacy incident/breach process

A privacy breach occurs when there is the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of security safeguards.

Examples of privacy breaches:

- Copies of client personal information statements are stolen from a vehicle
- Advisor laptop is lost/stolen and it contains client personal information
- Client information on an advisor's computer hard drive is compromised/hacked
- Client information not emailed to the intended recipient either internal or external
- Client information going to the wrong address (someone else opening the mail)
- Release of personal information without proper authorization or use of personal information without proper consent

Policy

Suspected breaches, complaints or any concern relating to a privacy issue, whether through an individual or a supplier, are reported immediately to the practice's compliance officer and/or the insurance company. Where Carrier client personal information is involved, Carrier will provide support to assess, contain, remediate and help enhance controls to prevent the breach from reoccurring in the future.

Procedure

Carrier client personal information:

Lost, stolen or hacked electronic devices:

- Immediately contact the Carrier service desk
- LAN, Advisor portal, Investment Centre passwords will be changed by the service desk
- File a report with the police.
- Change other system passwords (e.g., online banking).
- Scan computers for malware before accessing systems again
- Engage the practice's IT support when required.

Lost or stolen paper documents (e.g., policy contracts, applications, client files):

- Notify the practice's compliance officer, Carrier's chief compliance officer and the practice's regional director/business services manager.
- Additionally, report stolen materials to the police.

Misdirected emails:

- Recall email immediately.
- Notify the practice's compliance officer, Carrier's chief compliance officer and the practice's regional director/business services manager.

Carrier Distribution Compliance will be notified by the chief compliance officer and will contact the practice's compliance officer to help determine if clients' personal information was

compromised and to discuss containment, remediation and required client and regulator notification.

3. Obtaining valid, informed client consent

Consent is considered valid only if it is reasonable to expect that individuals understand the nature, purpose and consequences of the collection, use or disclosure to which they are consenting.

Policy

At the beginning of a relationship with a client, the practice will obtain client consent for the collection, use and disclosure of their personal information and notify them of potential out-of-country storage.

When collecting information from clients and prospects, explain the purposes behind the collection of this information and provide information about the practice's privacy policies.

Only disclose personal information about clients to another person or company if verbal or written consent from the client has been obtained or if otherwise allowed or required to do so by law.

The practice will recommend other professionals or advisors to clients if the client asks or if the client may benefit from such services. The practice never provides any client names or other information to third parties to market their services unless the client has first been informed and consented.

Procedure

Review the *Privacy commitment and your client file* form with the client, keeping the signed copy in the client file for future reference. Cover the:

- Purposes for the collection,
- Who has access - staff access, other advisors
 - This covers a short-term or temporary absence from the practice. At times when the practice is unable to provide service to clients for an extended period of time and help from another advisor or new administrative support person is required
- Use of suppliers (e.g., information processors which includes; client relationship managers and cloud-based storage services)
 - Likelihood that information will be stored outside Canada and is subject to regulation, including public authority access laws in that country
- Sharing spousal information consent; joint files and access to that information
- Individuals ability to withdraw consent

3.1 New access to client information

Policy

The practice will obtain client consent if the purpose for the collection, use and disclosure of the client's personal information changes.

Procedure

Review the new purpose, access, use and disclosure with the client and keep a copy of the new consent in the client file.

If a client objects to this transfer or new access, the client has the right to:

- Request that his/her information not be disclosed
- Request a new advisor
- Receive the names of other advisors to contact or be provided with the name and number of the regional director where they can request another advisor

3.1.2 Supplier contracts

Policy

The practice requires client consent prior to transferring client information to a supplier and retains control of the information when transferring personal information to a supplier for processing.

Information transfers to suppliers for processing, including cloud computing, is done for a variety of reasons including information storage, processing or manipulating client personal information.

Procedure

Before entering into, substantially amending or renewing a contractual arrangement with a supplier, the practice assesses whether or not the supplier has appropriate safeguards in place to protect client information.

The practice will check with its legal counsel before agreeing to the terms of the supplier and keep a printed copy of the agreement for the practice's records.

Assessment considerations:

Business experience: Evaluate the experience and technical competence of the supplier to implement and support the planned activities.

- How long has the supplier been in business? A new supplier may not have a sufficient track record to allow the practice to judge its processes and procedures as they relate to the safeguarding of information.

Reputation: Assess how long the supplier has been in the market and their market share.

- Obtain references to assess reputation? References from current users can help gauge the supplier's reputation.

Information security:

- What is their experience in handling sensitive personal and financial information?
- Does the supplier have a documented privacy policy in accordance with privacy legislation?
- Do they have a documented and current physical security policy or information security policy?

- Confirm with the supplier that the data they store, as well as data in transmission, is encrypted.

Incident reporting: Review the supplier's incident reporting and management programs to ensure they have clearly documented processes for identifying, reporting, investigating and escalating incidents. Ensure the supplier's escalation and notification process meet the practice's expectations.

- Does the supplier agree to notify the practice within 48 hours or less if they incur a data security breach that may involve client information?
- If a security breach is suspected, is there support from the supplier for an investigation? Are access logs maintained and provided on demand?

Contingency planning:

- Does the supplier have backup and recovery processes? Will the practice be able to access files if the supplier shuts down? What will the practice do if the supplier loses the client files? Does the practice have a backup?

Out-of-country notification:

- Does the supplier hold data outside of Canada? Information held in other countries may not have the same safeguards as in Canada and may not be in compliance with privacy requirements. Attempt to use a supplier that stores information in Canada or the practice will notify clients that their information will be stored outside of Canada.

Review the supplier's licensing agreement carefully: It is a contract, and by clicking "I agree" or by downloading any software, you may inadvertently expose information stored at the site to undue risk if the proper safeguards of information are not adhered to.

There must not be any involvement of any other third parties and/or data sharing, data pooling or access rights to clients' sensitive information being granted by the service supplier. This must be explicitly mentioned in the service supplier's agreement. Ensure the supplier:

- Limits use of the information to the purpose specified to fulfill the contract
- Limits disclosure of the information to what is authorized by the practice or required by law
- Refers any access requests or complaints relating to the information transferred to the practice
- Returns or securely disposes of the transferred information upon completion of the contract
- Reports on the adequacy of its personal information security/control measures and allows your organization to audit the third party's compliance with the contract as necessary

Understand:

- How to terminate the agreement with the supplier and ensure data is purged or returned. A supplier that does not remove or return information may present a risk to a client's information and therefore to the practice.
- The limitations of the service supplier's liability

3.2. Business transactions consent exception

Business transactions include, for example, the sale of a business, a merger or amalgamation of two or more organizations or any other prescribed arrangement between two or more organizations to conduct a business activity.

Policy

The practice transfers personal information where necessary to determine whether to proceed with a transaction, or in order to complete a transaction. The information must be used or disclosed solely for purposes related to the transaction, safeguarded appropriately, returned or destroyed when no longer needed for that purpose and the affected clients must be notified that their personal information has been transferred to another organization.

Procedure

When receiving personal information the practice will enter into an agreement to use or disclose the information for the sole purpose of the transaction, to protect it and to return or destroy the information if the transaction does not proceed. If the transaction proceeds, the practice will notify affected clients that their personal information has been transferred to another organization.

3.2.1 Buy/sell agreements

Policy

The practice will use, disclose and protect client information during the valuation process and when seeking a buyer for the book of business or looking to purchase a book of business.

Procedure

The practice limits identifying client information on documents shared with third parties and contacts legal counsel to draft a suitable confidentiality agreement that should be signed by third parties involved in the process of valuing the book for potential sale or purchase.

3.2.2 Agent of Record (AOR) changes

Policy

For client initiated AORs, the practice assumes consent to transfer access to the client's information and files, if applicable to the new advisor.

4. Collection of personal information

Policy

When collecting personal information:

- Limit the amount and type of the information gathered to only what is necessary, for the identified purposes.
- Take reasonable efforts to ensure client and prospect information held in client files is accurate and is updated or corrected as needed.
- Take appropriate measures to ensure that information collected is used for the purposes identified and that it is not used for another purpose or disclosed to a third party without the client's or prospect's consent, except as may otherwise be allowed by law.

4.1 Recording client telephone calls

Policy

Any recording of client calls involves the collection of personal information, therefore the practice must meet fair information practices. The same rules apply to calls initiated by the client and to calls initiated by the advisor.

Procedure

- Recording may only take place with the individual's consent. If the caller objects to the recording, provide the caller with meaningful alternatives and if the caller continues to refuse, cease recording the conversation immediately and destroy any recordings that may have been created.
- Only record calls for specified purposes.
- The individual must be informed that the conversation is being recorded at the beginning of the call and make a reasonable effort to ensure the individual is advised as to the purposes for which the information will be used.
- Ensure compliance with applicable privacy legislation.
- If a copy of the client file is requested, provide the recording or transcription of the recording of calls with the client.

5. Use, disclosure and retention

Policy

Personal information is not, without consent, used or disclosed to a third party for any purpose other than that for which it was collected, unless such use or disclosure is required or allowed by law.

The practice retains personal information only as long as necessary to fulfill the identified purpose or as otherwise required or allowed by law and is solely responsible for the safekeeping of this material and for maintaining its confidentiality.

Personal information that is no longer required to fulfill the purpose(s) identified when collected is securely destroyed or erased.

5.1 Secure disposal

Policy

- When paper materials containing any client or prospect personal information are to be destroyed, this is done by shredding, not recycling.
- Information is deleted from all business technology before the technology is destroyed. Storage devices must be destroyed when being disposed of to ensure the information is not retrievable.
 - When disposing of or destroying personal information, take appropriate measures to prevent unauthorized parties from gaining access.

- When disposing of equipment or devices used for storing personal information (such as filing cabinets, computers, diskettes, and audio tapes), take appropriate measures to remove or delete any stored information or otherwise to prevent access by unauthorized parties.

5.2 Record retention

Policy

For any Carrier product or services purchased by the practice's clients, files and records are scanned and shredded within period required by law.

6. Safeguards

Policy

Appropriate safeguards must be taken in the storage and disposal of client information. Anyone working for or contracted with the practice is required to follow the procedures outlined in this section.

Procedure

The practice uses a mix of technology, physical and organizational safeguards to protect client personal information from theft or misuse, as well as unauthorized access, disclosure, copying, use or modification.

6.1 Technological safeguards

Technology examples include:

- Computers – desktops, laptops, servers and personal digital assistants (tablets/smartphones)
- Hardware and software
- Mobile devices
- Portable media – encrypted/password protected USB/thumb drives, CDs and DVDs
- Printers, scanners, fax machines and photocopiers with secure print options
- Email and internet services (e.g., cloud computing)

6.1.2 Encryption, antivirus and firewalls

Policy

- Encryption and antivirus software and firewalls are installed and kept up-to-date on all business technology as means to ensure client data remains secure. This includes encryption of sensitive data for storage and transmission including transmission to backup servers.
- Business technology safeguards are reviewed on an annual basis and upgraded as necessary.
- When technology is unattended or is being transported, all devices are shut down (powered off). Logging off, locking or leaving the device in standby or sleep mode could render additional security measures ineffective.

6.1.3 Screen savers, user ID and passwords

Encryption does not eliminate the needs for strong passwords.

- Protect user ID and passwords and never share either with anyone.
- Pick strong passwords.
 - Avoid using proper names and words found in dictionaries (e.g., insurance, password) and personal information, like family and pet names, birthdays, government ID numbers or words associated with hobbies and interests.
- Use password-protected screensavers to prevent unauthorized access to unattended computers.
- Lock computers by clicking on “lock computer” when away from your computer temporarily.

6.1.4 Secure email

Password protection

When dealing with sensitive information, emails containing personal information need to be secured by a file/document password, or where possible, be encrypted. File passwords should be provided by telephone or by SMS.

Encryption options when sending email and attachments securely:

1. PDF password protected
2. FTP URL to password protected file

6.2 Physical safeguards

Consideration is given to the following safeguards:

6.2.1 Office design

- Desks/workspaces are arranged out of the traffic flow within the office.
- Fax machines, photocopiers, printers, etc. are located in areas where access is reasonably limited.
- Associates/staff dealing with sensitive client information are located, where possible, in an area where conversations will not be easily overheard.
- Personal client information files are located out of the traffic flow within the area.
- Locked file cabinets are used for files containing personal information.

6.2.2 Computers and consumer devices

Always take steps to protect against the theft of laptop computers and mobile devices by using an anti-theft security device (e.g., locking cable), whether at the office, at home, in a meeting room or hotel room, etc.

- Lock your device away in a secure place when not using it.

- To prevent theft, avoid leaving laptops in vehicles. If you must, keep your laptop in your trunk or another out-of-sight area.
- Shut down and power off your laptop – this will ensure that all applications have been properly closed.
- Log out of any websites or programs when you are finished using them. And remember, don't "save" your information so that you can automatically log in the next time – if your mobile device is lost or stolen, someone may be able to access your accounts or files.
- Computers and consumer devices (and if applicable associate/staff computers) are stored securely to prevent access during all absences (evenings, weekends, illnesses and vacations).

Securing laptops

In the office during the day – Laptops are locked using a locking cable and securely anchored to an immovable piece of furniture or a secure docking station. The lock key is stored in a safe place away from the laptop.

When leaving work at the end of the business day – Laptops are stored in a locked cabinet or drawer, and the lock key is stored in a safe place away from the laptop.

Laptop security rules above still apply when office doors are locked.

On the road:

- Be cautious of public Wi-Fi hotspots as someone may be eavesdropping on them. Avoid banking, shopping online or accessing corporate resources from such connections. It's best to save sensitive transactions for when you're on a network that you trust. Also be wary of using your mobile device outside your home country. Eavesdropping and traffic analysis maybe more prevalent on a foreign network. While working, position laptops so only the user can see the personal information on the screen.
- Record laptop serial and model numbers and keep them in a separate location.
- Carry laptops in a discrete bag. Use a padded bag, such as a backpack, instead of the normal laptop tote, to securely and safely transport disguised laptop.
- Keep laptops out of sight by storing in car's locked compartment during travel to prevent theft.
- Never place laptops in a taxi or limousine trunk since most hired drivers do not lock their trunks.
- Never check laptops with hotels or airlines.
- After placing laptop a on an airport's x-ray conveyer belt, watch the bag and don't let anyone cut ahead of you in line.
- At home or in a hotel room, secure laptops as you would at work. Have you locking cable on hand, lock the laptop down and store it out of sight.
- Card-access hotel rooms produce an accurate audit trail of who has visited the room and when. Metal keys can be lost and copied. If the hotel room uses metal keys, consider not leaving the laptop in the hotel room.

6.2.3 Desks and files

- Sensitive personal information or other client documentation should not be left unattended. When personal information needs to be accessible in paper format for active business purposes, all files and file contents should be placed so the contents are protected from the view of those who are unauthorized to see them.
- Ensure all sensitive personal information is secured in locked rooms, cabinets and/or desk drawers when not actively in use and that access is appropriately restricted.

Documents outside of business premises

Client information must be safeguarded whether in the office, car or other location. Paper files containing personal information should be removed from the office only when necessary or required to appropriately service clients.

For tracking purposes, all files/documents are recorded before being removed from the premises for reference if lost or stolen. All associates/staff must be made aware of and comply with this requirement.

6.3 Communicating confidential information with others

- Never discuss clients in public places such as elevators, cafeterias or restaurants.
- When sharing client or employee personal information on cellular phones, take precautions to avoid being overheard.
- When reading a client's personal information on public transit such as trains, planes or buses, position documents so as to prevent anyone else from reading them.

6.3.1 Voicemail

Messages left for clients should not contain personal information unless the client is informed in advance that the message may contain personal information. The client must also confirm that he/she wants this information to be provided on his/her voice message service.

6.3.2 Caller authentication

If a request is made by phone, it is necessary to authenticate that person before providing personal information.

To authenticate the caller, the person must successfully answer three of the following questions. Always ask the questions in order.

- Full name of owner(s)
- For person calling on behalf of the estate, ask for full name of the deceased owner
- For owner - in-trust for, ensure the caller's name matches the trustee name on the system
- For power of attorney, caller must provide name of power of attorney in addition to name of policyowner
- Policy number
- Apartment number, street number, street name and city
- Date of birth of the life insured/annuitant
- Full name of life insured/annuitant

If the validation is not successful inform, the caller that the practice is responsible for protecting the privacy and confidentiality of personal client information and therefore cannot disclose any details without first validating that the caller is the person who should be receiving this information. Ask them to submit their request by mail.

6.3.3 Email

Messages should not contain personal information unless the client is informed in advance that the message may contain personal information and has confirmed that he/she wants this information to be provided by email.

The following disclaimer is added to all email containing client personal information:

"The content of this email is confidential and intended for the recipients specified in the message only, do not distribute. "

Email authentication

Matters of a sensitive nature should not be communicated by email unless the client asks to use it. If a request is made by email, it's necessary to authenticate that person before providing personal information through email.

- Call the client and confirm they requested the information.
- Ensure the email is being sent to the correct recipient as names on address listings may be similar.
- Authenticate the client and obtain and document consent to correspond via email.
- Encrypt/password protect files when disclosure of identifiable client information is requested via an email account.

6.3.4 Faxes

Faxes should not contain personal information unless the client is informed in advance that the fax may contain personal information and has confirmed that he/she wants this information to be provided by fax.

The following disclaimer is added to the cover sheet of all faxes containing client personal information:

"The contents of this fax, including any attachment(s), are confidential and may be privileged. If you are not the intended recipient (or are not receiving this fax on behalf of the intended recipient), please notify the sender immediately and delete or destroy this fax without reading it, and without making, forwarding, or retaining any copy or record of it or its contents. Thank you."

Confirm fax number before sending client personal information

- Pay careful attention to the different long distance prefixes (i.e., 1-866, 1-888, 1-800) and take time to confirm the fax number before hitting send. Personal or confidential information can easily be misdirected by using the incorrect long distance prefix.

- For commonly used fax numbers, consider preprogramming your fax machine to avoid errors.
- Reconfirm the fax number before you hit send.

6.4 Organizational safeguards

6.4.1 Authorization and limiting access on a “need-to-know” basis

- Authorization is granted for access to personal information on a “need-to-know basis” (i.e., information required to perform defined job functions). Access to files (physical, system and electronic) is reviewed when associates/staff are hired or moved to a different job function.
- When an associate/staff member is terminating his/her employ, access to client information, including electronic information from computers and all other material from work areas is suspended.

6.4.2 Confidentiality agreements

Employees are made aware of the importance of maintaining security and privacy of personal information. Where personal information is sensitive or where the potential consequences of improper disclosures are significant, the practice:

- Uses confidentiality agreements with employees
- Takes appropriate precautions to safeguard client information from third parties who may have access to the premises (i.e., security, cleaning services and suppliers).
- Obtains, if appropriate, a non-disclosure agreement from the individual or corporation servicing the device if confidential information cannot be removed from a device before releasing it for repairs.

7. Adoption of policies and procedures

Policies and procedures adopted on SEPT 12 2018 by ELIZABETH LIPKOWITZ

Section 3 – Training program

All advisors and staff, permanent and temporary, are trained as outlined in this training program.

- Training is mandatory prior to the individual being given access to personal information.
- Training is an ongoing process with refresher training conducted annually or more frequently if needed based on changes to legislation, technology, service providers as well as new access to personal information, etc.
- The compliance officer facilitates and tracks completion of all training. Training is completed through circulation and review of the policies and procedures section of this compliance program which are reviewed as part of the program self-review to ensure materials are accurate and up-to-date.

- Completion of training is tracked and signed by each advisor and staff acknowledging completion. Records of completed training are retained in this section of the compliance program.
- Optional/additional training may include modules provided by insurers, circulation of insurer privacy communications and updates, news articles, industry communications and training modules etc.
- Staff not able to attend refresher training on the originally scheduled date(s) will need to have alternate arrangements made to meet this requirement.

Training completion tracking

Name	Type of training and content (initial training, ongoing, review of policies procedures and background information, module provided by insurer, etc.)	Date	Employee signature
<i>E Lipkowitz</i>	<i>Initial training, review of policies procedures and background information</i>	<i>09/04/2018</i>	E LIPKOWITZ
<i>D Kakon</i>	<i>Initial training, review of policies procedures and background information</i>	<i>09/04/2018</i>	D KAKON

Section 4 – Self-review

Date completed: SEPT 4 2018

Review completed by: DAVID EMMANUEL KAKON

Signature of principal/advisor: ELIZABETH LIPKOWITZ

Accountability	Yes	No	Comments
Has the practice designated a person to oversee compliance with privacy legislation and is the name of the designated person available to a client on request?	X		
Has the practice implemented procedures to protect personal information?	X		
Has the practice communicated and trained staff about policies and practices?	X		
Does the practice understand that personal information should not be collected that is not needed to fulfill the purpose identified?	X		
Does the practice understand that when providing third parties (e.g., computer consultants, cleaning staff, accountants, etc.) access to personal information, it must have contractual or other means to provide a comparable level of protection?	X		
For Canadian clients - Is the practice aware of and follow Carrier's privacy guidelines and strong business practices.	X		
Is the practice aware of and follow the privacy guidelines and strong business practices of other insurance companies it represents?	X		
Does the practice understand insurer processes regarding privacy complaints and inquiries?	X		
Consent	Yes	No	Comments
Does the practice understand that it's responsible for obtaining consent for the collection, use and disclosure of personal information?	X		
Does the practice have a process in place to obtain consent from clients for the collection, use and disclosure of their personal information?	X		

Does the practice make a reasonable effort to tell the client how his/her information will be used or disclosed?	X		
--	---	--	--

Consent	Yes	No	Comments
Does the practice understand that consent must be given by the client or by an authorized representative (e.g., legal guardian, general power of attorney)?	X		
Does the practice have a process in place to manage opt-out and withdrawal of consent (e.g., can track and respect the wishes of clients who have opted out)?	X		
Limiting collection	Yes	No	Comments
The practice only collects information that is necessary to fulfill the purpose(s) disclosed to the client.	X		
The information is collected by fair and lawful means.			
Limiting use, disclosure and retention	Yes	No	Comments
Does the practice understand that if personal information is intended to be used for a new purpose I must disclose that purpose to the client and obtain his/her consent?	X		
Does the practice have guidelines and procedures for the retention of personal information?	X		
Has the practice taken steps to ensure that when disposing of or destroying personal information, unauthorized parties will not access it?	X		
Accuracy	Yes	No	Comments
Does the practice have a process in place to ensure that the personal information collected and used is as accurate, complete, and up-to-date as is necessary for the purpose(s) for which it is to be used?	X		
Safeguards	Yes	No	Comments
Does the practice have security safeguards in place to protect against loss or theft, as well as unauthorized access, disclosure, copying, use or modification of personal information?	X		

Does the practice use a higher level of protection for sensitive information? Examples: <ul style="list-style-type: none"> Physical measures (e.g., locking filing cabinets, restricted access to office, etc.) Organization measures (e.g., limiting access on a “need-to-know” basis) Technological measures (e.g., use of passwords and encryption) 	X		
The practice has made advisors and staff aware of the importance of maintaining the confidentiality of personal information	X		
Openness	Yes	No	Comments
Clients can easily obtain information about my privacy policies and practices.	X		
Individual access	Yes	No	Comments
The practice understands that clients have a right to request information about them held in files I maintain.	X		
The practice has a process in place if a client requests access to/her personal information.	X		
The practice understands that clients have a right to request information about them held in files maintained by Carrier.	X		
The practice knows the process if a client requests access to his/her personal information held at Carrier.	X		
Actions required:			

Section 5- Reviews and amendments to the compliance program for privacy

The present program was adopted on September 01 2018

The present program was revised and amended on September 01 2018

Below is a summary of these amendments:

Document revision history

Date	What changed?	Reason for the change
01/09/18	Generated	Required