COMPLIANCE PROGRAM FOR PRIVACY

Sure Plan Services Inc
(the practice)

Compliance officer: Harish Jindal (ED)

Revised on: Annually.

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 **2**
2.1 CLIENT REQUESTS TO ACCESS PERSONAL INFORMATION 2
2.2 MISUSE OF PERSONAL INFORMATION: 3
2.3 PRIVACY INCIDENT/BREACH PROCESS 3
2.3.1 Policy *3*
2.3.2 Containment Process *3*
2.3.2.1 Lost, stolen or hacked electronic devices 3
2.3.2.2 Lost or stolen paper documents (e.g., policy contracts, applications, client files) 4
2.3.2.3 Misdirected emails or mail 4
2.3.2.4 Cyber attack 4
2.3.2.5 Ransomware 4
2.4 DOCUMENTATION PROCESS 4
2.5 COMPLETION OF RROSH ASSESSMENT 5
2.6 MANDATORY BREACH REPORTING UNDER PIPEDA 5
2.6.1 Notification to Affected Individual(s) *5*
2.6.2 Notification to Regulators *5*
2.7 ENHANCE CONTROLS 6
3. OBTAINING VALID, INFORMED CLIENT CONSENT **7**
3.1 NEW USES/ACCESS TO CLIENT INFORMATION 7
3.1.1 Supplier contracts *8*
3.2. BUSINESS TRANSACTIONS CONSENT EXCEPTION 9
3.2.1 Buy/sell agreements *9*
3.2.2 Agent of Record (AOR) changes *10*
4. COLLECTION OF PERSONAL INFORMATION **10**
4.1 RECORDING CLIENT TELEPHONE CALLS 10
5. USE, DISCLOSURE AND RETENTION **10**
5.1 SECURE DISPOSAL 11
5.2 RECORD RETENTION 11
6. SAFEGUARDS **11**
6.1 TECHNOLOGICAL SAFEGUARDS 11
6.1.1 Encryption, antivirus and firewalls *11*
6.1.2 Screen savers, user ID and passwords *12*
6.1.3 Secure email *12*
6.2 PHYSICAL SAFEGUARDS 12
6.2.1 Office design *12*
6.2.2 Computers and consumer devices *12*
6.2.3 Desks and files *13*
6.3 COMMUNICATING CONFIDENTIAL INFORMATION WITH OTHERS 14
6.3.1 Voicemail *14*
6.3.2 Caller authentication *14*
6.3.3 Email *14*
6.3.4 Faxes *15*
6.4 ORGANIZATIONAL SAFEGUARDS 15
6.4.1 Authorization and limiting access on a "need-to-know" basis *15*
6.4.2 Confidentiality agreements *15*
7. ADOPTION OF POLICIES AND PROCEDURES **17**

SECTION 3 – TRAINING PROGRAM 18
SECTION 4 – SELF-REVIEW..... ERROR! BOOKMARK NOT DEFINED.
SECTION 5 – REVIEWS AND AMENDMENTS TO THE COMPLIANCE PROGRAM FOR PRIVACY ... 18
DOCUMENT REVISION HISTORY..... **ERROR! BOOKMARK NOT DEFINED.**

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.

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 companies Manulife , Beneva, Assumption, IA, Equitable , Edge , Empire , Truestone , 2visitCAnada , Allianz, Destination, B2B , SSQ, Tugo).

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 regards to the concern with complete documentation of the concern and related activities kept in the client file.

The practice's compliance officer forwards any privacy concerns, general inquiries or requests related to the company's products and services to that company's chief compliance officer.

2.1 Client requests to access personal information

Under privacy laws, clients have the right to request access to their personal information held in client files maintained by either the practice or the 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.

Follow the company's process if a client requests access to his/her personal information held with the company.

2.2 Misuse of personal information:

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

2.3 Privacy incident/breach process

A privacy breach occurs when there is unauthorized access to or unauthorized disclosure of personal information or loss of personal information resulting from a breach of security safeguards. A privacy breach also includes information that is retained in ways which are not in accordance with applicable privacy legislation, such as retaining information that is no longer needed for the identified purpose.

A privacy breach may be intentional, inadvertent or as a result of criminal activity.

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 emailed to an unintended 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
- Keeping inactive customer information for longer than the retention period

2.3.1 Policy

Suspected or actual breaches are reported immediately to the practice's compliance officer. The practice's compliance officer will contain, assess, remediate, and help enhance controls to prevent the breach from reoccurring in the future.

2.3.2 Containment Process

In the event of a privacy breach of client (cyber attack, unauthorized data access), contact: 672 699 1155.

- the practice's compliance officer, and
- Experior Compliance for contacts of impacted carriers
- Other companies impacted

In addition to the steps outlined above follow specific steps outlined below.

2.3.2.1 Lost, stolen or hacked electronic devices

- Engage the practice's IT support
    - Scan computers for malware before accessing systems again
- Immediately contact each impacted company's service desk to have systems passwords changed.
- File a report with the police.
- Change other system passwords (e.g., online banking).

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

- Report stolen materials to the police.

2.3.2.3 Misdirected emails or mail

Email:

- Recall email immediately.
    - If not successful, contact unintended recipient to obtain written confirmation that email has been deleted and not saved or forwarded to another recipient.

Mail:

- Request the unintended recipient of misdirected mail to return the mail or confirm the mail has been securely destroyed (e.g., shredded).

.

2.3.2.4 Cyber attack

A cyber attack involves computers and computer networks that attempt to expose, alter, disable, destroy, steal, or gain information through unauthorized access to or make unauthorized use of an asset.

- Engage the practice's IT support
- Contact the police

2.3.2.5 Ransomware

Ransomware is a type of malicious software (malware) that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a sum of money (ransom) is paid.

- Engage the practice's IT support
- Contact the police

2.4 Documentation *Process*

Begin the documentation process of any privacy breach as soon as the breach has been contained. All privacy breach records must be kept secure.

Keep records of all privacy breaches for 24 months. The practice should be prepared to provide records to the Privacy Commissioner or other organizations upon request.

The record(s) must be kept secure and include:

- Date of breach
- Description of the circumstances of the breach
- # of individuals affected
- Types of personal information involved in the breach
- Sensitivity of information breached
- Probability of misuse
- Indicator as to whether or not:
    - the breach resulted in a Real Risk of Significant Harm and an explanation of determination
    - affected individual(s) notified
    - confirmation and notification date to the Office of Privacy Commissioner

A tracking log containing a list of all privacy breaches in one location can also be .



Breach Record Keeping Template.xl

2.5 Completion of RROSH assessment

All privacy breaches must be assessed to determine if it meets the threshold for Real Risk of Significant Harm (RROSH).

To determine if a Real Risk of Significant Harm significant Harm exists, consider the following:

- Was sensitive personal information involved? Sensitive personal information includes, but is not limited to SIN, banking information and medical information
- Was personal information maliciously obtained? This includes obtaining personal information by theft, fraud or hack of systems
- Were 5 or more people impacted?
- Is the personal information still not recovered?
- Is the personal information still yet to be confirmed as destroyed?
- Is the incident a systemic issue?
- Has it been more than 20 business days between incident and discovery?

If you answered "yes" to any of the above questions, a RROSH may exist for the individual(s) affected by the breach. Considering both the sensitivity of the personal information involved in the breach, and the probability that the personal information has been, is being or will be misused, a determination must be made as to whether the breach does pose a RROSH to the affected individual(s).

If you answered "no" to all questions, proceed to section 2.7 Enhance controls.

2.6 Mandatory breach reporting under PIPEDA

- When the practice considers that a breach creates a RROSH, it must notify the affected individual(s) and report the breach to the Office of the Privacy Commissioner of Canada (the Commissioner) or provincial regulators where required as soon as feasible even if only one individual is affected;
- The practice must notify any other organization/company that may be able to mitigate harm to affected individuals, (e.g., putting flags on client's accounts)

2.6.1 Notification to Affected Individual(s)

A notification provided by the practice to affected individual(s) with respect to a breach of security safeguards must contain:

a. a description of the circumstances of the breach;
b. the day on which, or period during which, the breach occurred or, if neither is known, the approximate period;
c. a description of the personal information that is the subject of the breach to the extent that the information is known;
d. a description of the steps that the practice has taken to reduce the risk of harm that could result from the breach (e.g., credit monitoring, flagging the accounts);
e. a description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and
f. contact information that the affected individual can use to obtain further information about the breach.

2.6.2 Notification to Regulators

- Report to the Office of the Privacy Commissioner (federal) using the PIPEDA breach report form

- British Columbia – legislation recommends notification to the Privacy Commissioner if there is a real risk of significant harm. See BC's privacy breach checklist for the reporting.
- Report to the Office of the Information and Privacy Commissioner of Alberta using their breach report form
- Quebec – notify the Autorité des marchés financiers of any breach of personal information that will jeopardize the interests or rights of consumers and the institution's reputation.

2.7 Enhance controls

Review all processes, systems updates, employee training and enhance where required to help prevent reoccurrence.

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 of their personal information 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. If information is sensitive, written consent should be obtained.

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 external 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
- Individual's ability to withdraw consent at all times

3.1 New uses/access to client information

Policy
The practice will obtain client consent if the purpose for the collection, access, 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 a 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

3.1.1 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 supplier's experience and technical competence 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 there is 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 or do individuals outside Canada have access to the data? 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.

The service provider must not involve any other third parties and/or data sharing, data pooling or access rights to clients' sensitive information, unless this is specifically mentioned in the service supplier's agreement. Ensure that the supplier:

- Limits use of the information to the purpose specified to fulfill the contract
- Limits access to data to individuals who need access 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's 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 and therefore requires the callers consent.

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 will 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 safe keeping 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

The practice's clients, files and records are maintained for at least any minimum 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 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 requiring safeguards can include:

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

6.1.1 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 while stored and in transit 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.

Security program details

Safeguards	Product	Last updated
Encryption	Top Industry Recommended	Annually
Antivirus/Malware protection	Top rated	Annually
Firewall	Active/enabled	Annually

6.1.2 Screen savers, user ID and passwords

Encryption does not eliminate the need for strong passwords.

- Protect user ID and passwords and never share either with anyone.
- Pick strong passwords (use capitals, lowercase, numbers and symbols with a minimum length of eight characters).
    - 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.

6.1.3 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.

Encryption options when sending email and attachments securely:

1. WinZip
2. Microsoft Office 2007 (Word, Excel and PowerPoint)
3. Microsoft Office Outlook 2007, with the use of digital certificates
4. Office 2016 / O365

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 described 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 discreet bag. Use a padded bag, such as a backpack, instead of the normal laptop tote, to securely and safely transport a 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 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 the 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 never 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 absolutely 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 them with any personal information.

To authenticate the caller, the person must successfully answer three of the following questions. Always ask the questions in this 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 that matches name on file in addition to the name of the 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 in writing.

6.3.3 Email

Messages should not contain personal information unless the client is informed of this in advance 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 contents of this communication, including any attachment(s), are confidential and may be privileged. If you are not the intended recipient (or are not receiving this communication on behalf of the intended recipient), please notify the sender immediately and delete or destroy this communication without reading it, and without making, forwarding, or retaining any copy or record of it or its contents. Thank you. Note: We have taken precautions against viruses but take no responsibility for loss or damage caused by any virus present."

Email authentication

Sensitive information should not be communicated by email unless it's at the client's request. 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 communicate via email.
- Encrypt/password protect files when disclosure of identifiable client information is requested via email.

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.
- Contact recipient once the fax is sent to confirm receipt.

6.4 Organizational safeguards

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

- Authorization is only 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's employment is in the process of being terminated, 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 ____01 June 2023__ by Sure Plan services inc.

Section 3 & 4 – 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 use/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.

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

The present program was adopted on the dated : 01-JUNE-2023.

The present program was revised and amended Annually.