

# PRIVACY POLICY PROCEDURES MANUAL

# INTRODUCTION

There are 3 privacy laws/bills you need to know about.

They are as follows:

- ◆ The Federal Personal Information Protection and Electronic Document Act (“PIPEDA”) - Applies to the jurisdictions of Manitoba, Saskatchewan, Northwest Territories, Nunavut and Yukon
- ◆ Alberta Bill 44 - Personal Information Protection Act (“Bill 44”)
- ◆ British Columbia Bill 38 - Personal Information Protection Act (“Bill 38”)

***Implementation date for all 3 laws - January 1, 2004***

Alberta presently has two other privacy laws in place:

**(FOIP) Freedom of Information and Protection of Privacy** - applying to the public sector including government ministries, agency, boards, commissions, educational bodies, health care bodies, local governments, municipalities and police services.

**(HIA) Health Information Act** - applying to the publicly funded health care sector, nursing home operators, pharmacies and pharmacists.

### **Why you need to know about the Privacy Laws of other jurisdictions**

Personal information that crosses provincial borders will be governed by:

- ◆ PIPEDA - (Federal law applies where there is no Provincial Privacy law)
- ◆ Privacy Law of the province from which the information is transferred, and
- ◆ Privacy Law of the province to which the information is transferred

### **Fundamental purpose of Privacy Laws**

- ◆ to balance the right of privacy of individuals with respect to their personal information and the need for organizations to collect, use or disclose personal information
- ◆ for purposes that a reasonable person would consider appropriate in the circumstances

### **Scope of PIPEDA**

#### **The Federal Personal Information Protection and Electronic Document Act**

- ◆ applies to personal information collected, used or disclosed in the course of a “commercial activity”
- ◆ applies to personal information of customers
- ◆ personal information collected before the Bill come into force was collected by “implied consent”

### **Scope of Alberta Bill 44 and British Columbia Bill 38**

- ◆ applies to personal information collected, used or disclosed by all organizations
- ◆ applies to personal information of employees of an organization
- ◆ treatment of personal health information
- ◆ professional regulatory and non-profit organizations
- ◆ personal information collected before Alberta Bill 44 come into force is “grand fathered”
- ◆ personal information collected before BC Bill 38 come into force was collected by “implied consent”

# The 10 Privacy Principles

1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection
5. Limiting Use, Disclosure and Retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance

# GENERAL

The following is a brief account of the Personal Information Protection Act and provides only guidelines to operate within the intent of the Act. Where additional information is required, users should consult the Personal Information Protection Act and your Manager. For referral, a copy of the Act is kept with the company Privacy Officer.

## 1. ACCOUNTABILITY

We are responsible for all the personal information that is in our custody or under our control. We have custody of personal information when it is in our offices, facility (premises), file cabinets, computers, etc.

### Procedures:

We have designated a Privacy Officer for answering questions about the Act and for taking access requests and complaints under the Act. **Our Privacy Officer is: Brenda Simioni.**

Our procedures and practices will cover:

- ◆ why we collect personal information
- ◆ how we obtain consent for collecting, using and disclosing personal information
- ◆ how we limit collection, use and disclosure of personal information
- ◆ how we ensure that the personal information is correct, complete and current
- ◆ how we ensure adequate security measures are in place
- ◆ how to develop or update the timetable for keeping or destroying information
- ◆ how we process access requests
- ◆ how we respond to enquiries and complaints
- ◆ we must do what a reasonable person would in the situation

## 2. IDENTIFYING PURPOSES

We must give notice about why we are collecting the personal information before or at the time the information is collected.

### Procedures:

We will govern the collection, use and disclosure of personal information in a manner that recognizes both the right of an individual to have his or her personal information protected and the need to collect, use or disclose personal information for purposes that are reasonable (what a reasonable person would consider appropriate in the circumstances).

Any new purposes that arise during the course of dealing with personal information you must obtain consent even if the initial purpose has been identified.

### 3. CONSENT

The knowledge and consent of the individual is required for the collection, use, or disclosure of personal information, except where inappropriate.

#### Procedures:

Unless the Act says that you do not need consent, you must get consent to collect personal information; collect personal information from someone who is not the individual, use personal information, or disclose personal information. (Section 7)

There are **three forms of consent**: (Section 8) You should choose the appropriate form, depending upon the transaction or activity. Consider what an individual would reasonably expect, the circumstances, and the sensitivity of the information.

➤ **express (written or verbal)**

1) consent in writing or verbally is express consent (written consent may be given electronically (by fax or e-mail) as long as the organization receiving the consent is able to make a copy of the consent on paper.) If verbal consent is given a note of that consent should be put into the client's file.

➤ **implied**

1) consent happens when an individual does not actually give consent, but supplies the information for a certain purpose or purposes, and a reasonable person would think that it was appropriate in the situation to volunteer that information and consent has been implied by the circumstances.

Or

➤ **opt-out**

1) in some situations an individual can be given the choice to opt out of providing consent - by opting out, he or she has provided consent for the organization to collect, use or disclose personal information for a certain purpose. This form can only be used if the individual knows why the information is being collected, used and disclosed in an easy to understand notice before, or at the time, it collects, uses or discloses the information. The individual must be given a reasonable chance to say no to the collection, use or disclosure and the personal information is not so sensitive that it would be unreasonable to use an opt-out form of consent).

Personal information collected before January 1, 2004 is considered "grand fathered" under Alberta Bill 44.

The Federal Act (PIPEDA) and BC Bill 38 do not recognize "grand fathering", however, we shall consider information given before January 1, 2004 was given with "implied consent".

Outside third parties requesting personal information must submit written consent which may be given electronically (fax or e-mail) as long as we are able to make a paper copy of the consent.

When the individual is a minor, seriously ill, or mentally incapacitated consent must be obtained from a legal guardian or person having a power of attorney or trusteeship order.

## 4. LIMITING COLLECTION

We collect personal information only to the extent that is reasonable for meeting the purposes for which the information is collected.

### Procedures:

We collect only the amount and type reasonably needed to carry out the purposes for collecting the personal information.

We give notice about why we are collecting the personal information before or at the time we collect the information.

We collect directly from the individual, unless he or she agrees to someone else giving the information to us. In some instances, PIPA allows collection without consent.

## 5. LIMITING USE, DISCLOSE AND RETENTION

Personal Information shall not be used or disclosed for purposes other than those for which it is collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

### Procedures:

We use and disclose information only for reasonable purposes and use and disclose the amount and type of information needed to carry out those purposes.

Act permits using and disclosing personal information without consent for limited and specific circumstances.

## 6. ACCURACY

Personal information we collect will be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

### Procedures:

We will take reasonable steps to ensure information is accurate, up-to-date, complete and not misleading.

We will provide recourse to individuals who appear to have legitimate corrections to make to their information on file.

An individual may request we correct an error or omission in the personal information collected.

Corrections must be made as soon as reasonably possible and where the information has been disclosed, send a notification containing the correction, if it is reasonable to do so.

If we determine not to make the correction, we must annotate the personal information with the correction that was requested but not made.

## 7. SAFEGUARDS

We will safeguard the security of personal information under our control in a manner that is appropriate to the sensitivity of the information.

### Procedures:

Our safeguards include the following:

- ◆ use reasonable safeguards to protect personal information from theft, modification, unauthorized access, collection, use, disclosure and destruction. Safeguards should be appropriate to the sensitivity of the information, the amount of information held, the parties to whom information is disclosed, the format in which the information is held and the way in which the information is stored
- ◆ when transferring personal information, only transfer the information strictly needed by the third party
- ◆ our method of protecting personal information shall include physical measures, (office premises have restricted security card access), limiting access on a “need-to-know” basis, technical measures such as the use of passwords and encryption (computers have security password that must be re-entered after 5 minutes of inactivity)
- ◆ clearly communicate our procedures concerning the safeguarding of personal information to staff. Review regularly and revise where appropriate
- ◆ keep information for as long as reasonable to carry out business or legal purposes and use care in disposing of, or destroying information
- ◆ take precautions in the disposal and destruction of personal information to prevent unauthorized parties from gaining access to the information ensuring no one may retrieve personal information after disposal, shredding documents, before recycling them and deleting electronically stored information

## 8. OPENNESS

Individuals will be able to inquire about our policies and procedures without unreasonable effort.

### Procedures:

A brochure explaining our privacy policy and procedures was sent to our clients starting November 15, 2002 and the brochure continues to be attached to new business and is available on our web site.

Our Privacy Policy Procedures Manual is published on our website.

The name or title and address of our Privacy Officer is publicly available.

## 9. INDIVIDUAL ACCESS

Upon request, an individual will be informed of the existence, use and disclosure of his or her personal information which is under our control, and may be given access to, and challenge the accuracy and completeness of that information.

### Procedures:

Our procedures are as follows:

- ◆ an individual may access personal information upon written request
- ◆ an individual is required to supply sufficient information for us to provide an account of the existence, use and disclosure of personal information in an open, complete and accurate manner
- ◆ an individual may request:
  - a copy of the record or examine personal information
  - a list of all parties to whom which the personal information was disclosed
- ◆ every reasonable effort to respond to requests must be made **within 45 days**
- ◆ response to request will be kept in both written and electronic format (in Master Privacy Act binder and on the u:drive)
- ◆ an extra 30 days is allowed to respond in certain circumstances but the individual making the request must be notified in writing as to why you are taking more time, when you will respond to the request, and that he or she may make a complaint to the Privacy Commissioner in their jurisdiction
- ◆ a fee may be charged for access of personal information but not for correcting personal information. At this time we are not charging a fee

Access is not granted under the following circumstances:

- ◆ The information is protected by legal privilege
- ◆ The information was collected for an investigation of legal proceeding
- ◆ Disclosure of the information would reveal confidential information of a commercial nature
- ◆ The disclosure could reasonably threaten the life or security of another person
- ◆ The information reveals personal data about another person
- ◆ The information would reveal the identity of a person who has provided an opinion about another person who has not given consent to disclose

## 10. CHALLENGING COMPLIANCE

An individual may address a challenge concerning compliance with the Privacy Officer.

### Procedures:

Our procedures are as follows:

- ◆ an individual who wishes to file a complaint must do so in writing
- ◆ we will acknowledge a complaint right away and document the complaint
- ◆ all complaints will be directed to the Privacy Officer who will direct to the vice-president of the appropriate area for handling (ex: V. P. Claims, Underwriting, Finance or Calgary)
- ◆ the Vice-President will investigate complaint right away and reply in writing

# DEFINITIONS

**“Access” (Sections 23-24)** means that on making a written request by an individual to an organization for access to his/her personal information, the organization must provide the individual with access to:

- i) the personal information where that information is in a record in the custody or under the control of the organization
- ii) the purposes for which the information has been and is being used by the organization
- iii) the names of the person to whom and circumstances in which the information has been and is being disclosed
- iv) an organization may refuse to provide access in limited circumstances including:
  - a. the information is protected by legal privilege
  - b. the disclosure would reveal confidential information that is of a commercial nature and it is not unreasonable to withhold that information
  - c. the information was collected for an investigation or legal proceeding
  - d. the disclosure might result in that type of information no longer being provided to the organization when it is reasonable that that type of information would be provided
  - e. the information was collected by a mediator or arbitrator who was appointed to act under an agreement, under an enactment or by a court
- v) an organization shall not provide access if
  - a. the disclosure could reasonably be expected to threaten the life or security of another individual
  - b. the information would reveal personal information about another individual
  - c. the information would reveal the identity of an individual who has in confidence provided an opinion about another individual and the individual providing the opinion does not consent to the disclosure of his or her identity
- vi) if an organization can sever the information to provide access to the individual, it must do so

**“Business contact information” (Section 1)** means an individual's name and position or title, business telephone number, business address, business e-mail, business fax number and other business contact information.

**“Care of Personal Information” (Sections 33-35)**

1. An organization must make a reasonable effort to ensure that any personal information collected, used or disclosed is accurate and complete.
2. An organization must protect personal information in its custody or under its control by making reasonable security arrangements against listed risks.
3. An organization may retain information as long as reasonable for legal or business purposes even after consent has been withdrawn or varied.

**“Collection” (Sections 11-15)** means that before or at the time of collecting personal information about an individual from the individual, the organization must notify that individual in writing or orally:

- ◆ the purposes for the collection
- ◆ the name of the person who is able to answer on behalf of the organization the individual’s questions about the collection

If the individual has consented to the collection of information from other organizations, the organization must notify the other organization of the individual’s consent. If the collection is without the individual’s consent, the organization must provide the other organization with sufficient information about the purpose for collection so that the other organization can make a determination whether the disclosure would be in accordance with PIPA.

**“Collection, use and disclosure of personal information without consent” (Sections 14, 17, 20)**

These circumstances are not identical, however, in some situations overlap and must be carefully reviewed. The circumstances relevant to Property & Casualty insurers are as follows:

- ◆ a reasonable person would conclude that the collection/use/disclosure of the information is clearly in the interests of the individual and consent of the individual cannot be obtained in a timely way, or the individual would not reasonably be expected to withhold consent
- ◆ the collection/use/disclosure of the information is pursuant to a statute or regulation of Alberta or Canada that authorizes or requires the collection/use/disclosure
- ◆ the collection is from a public body/information was collected from a public “body/disclosure is to a public body and the public body is authorized or required to disclose or collect the information
- ◆ the collection/use/disclosure is reasonable for the purposes of an investigation or legal proceeding
- ◆ the information is publicly available
- ◆ the collection/use/disclosure is for the purposes of a debt owed to the organization
- ◆ disclosure is necessary to respond to an emergency that threatens life, health, or security of an individual or the public
- ◆ disclosure is necessary for the purpose of protecting against or for the prevention, detection or suppression of fraud

**“Commercial Activity”** means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.

**“Compliance” (Sections 5-6)** means that an organization is responsible for personal information that is in its custody or under its control. An organization is responsible for the compliance of its agents, but the agent is not relieved of his responsibilities or obligations under PIPA (Alberta Law).

**“Consent” (Sections 7-10)** an organization is required to obtain the consent of the individual

- i) to collect that person’s personal information
- ii) to collect that person’s personal information from a source other than that person
- iii) to use that person’s personal information
- iv) to disclose that person’s personal information
- v) to not collect personal information from an individual beyond that which is necessary to provide the product or service
- vi) to obtain consent either in writing or orally

**Exceptions:**

1. an individual is deemed to give consent to an organization for a particular purpose for which the information was collected if:
  - i) the individual, without actually giving a consent, voluntarily provides information to the organization for that purpose
  - ii) it is reasonable that a person would reasonably provide that information
2. an organization may collect, use or disclose personal information about an individual for particular purposes if:
  - i) the organization provides the individual with a notice in a form that can reasonably be understood and gives the individual a reasonable opportunity to decline or object to having his/her personal information collected, used or disclosed for those purposes
  - ii) the individual does not within a reasonable time respond to the notice
  - iii) having regard to the sensitivity, if any, of the information, it is reasonable to collect, use or disclose the information as provided above
3. an individual may, subject to and on giving reasonable notice to the organization withdraw or vary consent if doing so would frustrate the performance of a legal obligation unless otherwise agreed to by the parties who are subject to the legal obligations to the insured, such as settling and adjusting claims and defending the insured against legal actions. Upon receiving the individual’s notice of intention to withdraw or vary consent, the organization must inform the individual of the likely consequences of the withdrawal or varying consent, must stop collecting, using or disclosing the personal information unless the collection, use or disclosure is permitted without consent under the Act. PIPEDA (Federal Law) provides that an individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. **It requires organizations to inform the individual of the implications of such withdrawal.**
4. consent obtained through false or misleading information or by using deceptive or misleading practices is negated. (PIPEDA (Federal Law) contains similar prohibition - Limiting Collection)

**“Limiting Collection” (Section 5(3))** PIPEDA (Federal Law) restricts the collection of information to that which is necessary for the purposes identified by the organization and adds the **reasonable person** test to the collection of information.

**“Correction” (Section 2-32)** means that an individual may request in writing that an organization correct an error or omission in the personal information in the organization’s control.

- i) if there is an error or omission, the organization must correct the information and if it is reasonable to do so, advise other organizations to which it had disclosed the information.
- ii) the organization must note in the information if there is an unresolved request for correction.
- iii) an organization shall not correct or otherwise alter an opinion, including a professional or expert opinion.
- iv) **an individual must send a written request for access or correction to the organization**
- v) an organization has a duty to assist an individual in making a request for access or correction
- vi) an organization must respond to a written request within 45 days of receipt or by the end of any extended period – the Act sets out what an organization must include in its response to a written request
- vii) an organization may charge a reasonable fee to an applicant for access, but not to an applicant for correction of information. If an organization intends to charge a fee, it must give the applicant a written estimate and may require the applicant to pay a deposit.

**“Disclosure of Personal Information” (Sections 19-21)** means the making of personal information available to others outside the organization over which the organization has no control.

**“Employee” (Section 1)** means an individual employed by an organization and includes an individual who performs a service for or in relation to or in connection with an organization

- i) as an apprentice, volunteer, participant or student
- ii) under a contract or an agency relationship with the organization

**“Grandfathering” (Section 4)** means that if an organization acquired personal information prior to January 1, 2004, for the purposes of PIPA (Alberta Law) that information is:

- i) deemed to have been collected pursuant to consent given by the individual
- ii) may be used and disclosed by the organization for the purposes for which the information was collected
- iii) after January 1, 2004 is to be treated in the same manner as information collected under PIPA (Alberta Law)

**There are two definitions insurers can use for fraud investigation, namely “investigation” and “legal proceeding”, both of which an organization may collect, use or disclose personal information without the individual’s consent.**

**“Investigation” (Section 1)** means an investigation related to:

- i) a breach of an agreement
- ii) a contravention of an enactment of Alberta or Canada or another province of Canada
- iii) circumstances or conduct that may result in a remedy or relief being available at law, if the breach, contravention, circumstances or conduct in question has or may have occurred or is likely to occur and it is reasonable to conduct an investigation.

**“Legal proceeding” (Section 1)** means a civil, criminal or administrative proceeding that is related to:

- i) a breach of an agreement
- ii) a contravention of an enactment of Alberta or Canada or another province of Canada
- iii) a remedy available at law.

**“Organization” (Section 1)** includes:

- i) a corporation
- ii) an unincorporated association
- iii) a trade union (defined in Labour Relations Code)
- iv) a partnership (defined in the Partnership Act)
- v) an individual acting in a commercial capacity
- vi) any person acting on behalf of a corporation, unincorporated association, trade union or partnership

This definition in Bill 44 (Alberta Law) includes an individual acting as agent for a corporation (an organization is responsible for its agent’s compliance with PIPA (Alberta Law)).

**“Personal employee information” (Section 1)** means, in respect of an individual who is an employee or a potential employee, personal information reasonably required by an organization that is collected, used or disclosed solely for the purposes of establishing, managing (managing includes administering) or terminating:

- i) an employment relationship
- ii) a volunteer relationship

between the organization and the individual but does not include personal information about the individual that is unrelated to that relationship.

PIPEDA (Federal Law) which does apply to the employee information of banks, airlines and other federal works, undertakings and businesses does not define employee information.

**“Personal Health Information”** with respect to an individual, whether living or deceased means:

- i) information concerning the physical or mental health of the individual
- ii) information concerning any health service provided to the individual
- iii) information concerning the donation by the individual of any part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual
- iv) information that is collected in the course of providing health services to the individual
- v) information that is collected incidentally to the provision of health services to the individual

**“Personal information” (Section 1)** means information about an “identifiable individual” but does not include business contact information. This may include:

- ◆ name
- ◆ birth date
- ◆ gender
- ◆ address
- ◆ phone numbers
- ◆ education
- ◆ employment
- ◆ income
- ◆ medical history

**“Purpose” (Section 3-4)** “to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of an individual to have his or her personal information protected and the need of organizations to collect, use or disclose personal information for purposes that are reasonable”. PIPA (Alberta Law) and PIPEDA (Federal Law) purpose and reasonable person are very similar.

**PIPA (Alberta Law) has broader scope of application than PIPEDA (Federal Law).**

PIPA (Alberta Law) applies to every organization and in respect to all personal information. PIPA (Alberta Law) applies to the collection, use and disclosure of “personal information”, which includes “personal employee information” by “organizations”. PIPEDA (Federal Law) only applies to “employee information” of “organizations” over which the federal government has exclusive jurisdiction i.e. banks, airlines, telecommunication companies and other federal works (not employees of insurance companies) - other employment matters are within provincial jurisdiction.

PIPA (Alberta Law) does not apply to a public body or any personal information in the custody of or under control of a public body. The Act does not apply to

- i) collection, use or disclosure of personal information for personal or domestic purposes
- ii) for artistic or literary purposes
- iii) for journalistic purposes

- iv) to business contact information if the collection, use or disclosure is for the purposes of contacting the individual in that person's capacity as an employee or official of the organization
- v) to personal information if the provincial public privacy law FOIP (Freedom of Information and Protection of Privacy Act) applies
- vi) to health information if the provincial law applies (HIA)
- vii) to personal information collected, used or disclosed by an officer of the legislature
- viii) to personal information if the individual has been dead for at least twenty years
- ix) to personal information in a record in existence for at least one hundred years
- x) to personal information transferred to an archival institution
- xi) to personal information in a court file
- xii) to personal information in records created for or by an elected or appointed member of a public body
- xiii) to personal information in a personal note, communication or draft decision created by a judicial, quasi-judicial or adjudicative body

**“Reasonableness” (Section 2)** The standard for determining whether something is “reasonable” or “unreasonable”, or has been carried out “reasonably” or “in a reasonable manner” means what a reasonable person would consider appropriate in the circumstances. The reasonable person test is an objective legal test. Reasonable judgment is not what you or I may think is reasonable – it is the judgment of an objective third party.

**“Record” (Section 1)** includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine-readable record and any other documentary material, regardless of physical form or characteristics and any copy of any of those things.

**“Use of Personal Information” (Sections 16-18)** means the treatment and handling of personal information within the organization.

# CLAIMS

## 1. ACCOUNTABILITY

### Procedures:

Refer to General Section  
Privacy Principle # 1 – Accountability

## 2. IDENTIFYING PURPOSES

The purpose of these guidelines is to establish acceptable claims etiquette based on various Privacy Laws.

## 3. CONSENT

### Procedures:

Every new claim requires recorded or written consent in order to proceed. This applies to all claims representatives, along with contract employees and independent adjusters.

Consent should be obtained on:

- ◆ Direct damage claims - via recorded statement
  - Property – may also obtain on schedule of loss
  - Auto
- ◆ Section B – via recorded statement & Medical Authorization
- ◆ Bodily Injury – via recorded statement & Medical Authorization

If consent is not obtained:

- ◆ Direct damage claims can not be considered.
  - Personal information is necessary for appraisals, rentals, contractors, replacement vendors, body shops, emergency personnel, independent adjusters or other vendors of this type.
  - Lack of consent to collect, use and disclose personal information will result in underwriting notification.
- ◆ Third Party or Liability claims may be compromised.
  - Lack of information may prejudice a position of liability in whole or part.
  - Personal information cannot be used or disclosed during the normal investigation to determine liability.

## 4. LIMITING COLLECTION

### Procedures:

Refer to General Section

Privacy Principle #4 – Limiting Collection

## 5. LIMITING USE, DISCLOSE AND RETENTION

### Procedures:

#### Limiting Use

All personal information collected is used for the purposes of delivering insurance claims service. All uses of personal information will be for the purpose of reasonable claims practices and will include but not be limited to the following:

- ◆ Claims Investigation
- ◆ Quantification
- ◆ Determining Liability
- ◆ Rehabilitation Co-ordination
- ◆ Indemnifying Policy Holders
- ◆ Fraud Detection

#### Disclosure of Personal Information

All service providers who may be in receipt of personal information provided by Peace Hills have been asked to provide a signature of compliance with the Act, and a copy of their guidelines.

#### Retention of Personal Information

##### Personal Info in paper format

- ◆ *On Site*
  - Edmonton Claims Dept. – 9 months; relocated offsite storage
  - Calgary Claims Dept. – 2 years; relocated offsite storage
- ◆ *Off Site*
  - Edmonton Claims Dept. – 5 years
  - Calgary Claims Dept. – 5 years
  - Off site storage facility in Edmonton is Trust Document Disposal and in Calgary is SPF Files.
  - Both shred on their site

Specific types of claims containing personal information that may never be destroyed are stored either on premise or in storage sites:

- ◆ Structured settlements
- ◆ Claims involving injured minors
- ◆ Claims involving incapacitated persons

#### Electronic Files

- ◆ Retained on system for both Edmonton and Calgary offices since 1995

## 6. ACCURACY

### Procedures:

Take reasonable steps to ensure information is accurate, up-to-date, complete and not misleading.

To provide recourse to individuals who confirm legitimate corrections are required to their personal information.

When data is entered on-line validity edits are in place.

Processing errors that are identified are corrected on a timely basis.

## 7. SAFEGUARDS

### Procedures:

Claims files off premises

- ◆ All personal information off premise in adjusters care is kept in a locked or secured location. This includes both contract and independent adjusters.

## 8. OPENNESS

### Procedures:

Refer to General Section  
Privacy Principle #8 – Openness

## 9. INDIVIDUAL ACCESS

### Procedures:

Refer to General Section  
Privacy Principle #9 – Individual Access

## 10. CHALLENGING COMPLIANCE

### Procedures:

Refer to General Section  
Privacy Principle #10 – Challenging Compliance

# UNDERWRITING

(Personal Lines, Farm and Commercial)

## 1. ACCOUNTABILITY

### Procedures:

Refer to General Section  
Privacy Principle # 1 – Accountability

## 2. IDENTIFYING PURPOSES

### Procedures:

This is done by way of the consent clause on applications, questionnaires and quote sheets which basically states personal information is being gathered for the purpose of obtaining insurance coverage.

## 3. CONSENT

### Procedures:

ALL applications/questionnaires/quote sheets must contain consent clause for collecting personal information with the purpose clearly defined (See note below on current status of this issue.)

**Commercial auto underwriters must obtain consent from all drivers under a commercial auto policy. This applies to new business and endorsements.**

**Personal Lines underwriters must obtain consent from policyholder on behalf of all drivers under a personal auto policy. This applies to new business and endorsements.**

Underwriters must ensure applications for ALL business lines are fully completed and the consent clause signed. (Note: this also applies to brokers issuing policies on our behalf – Falkins, etc.)

Peace Hills will review the consent clause being used by brokers issuing policies on our behalf and program brokers to ensure it meets with our requirements.

Underwriters to ensure personal information is in accordance with the Personal Information Protection Act in the jurisdiction to which the personal information applies (ex: Alberta Bill 44 (PIPA), BC Bill 38 or Federal (PIPEDA)).

New personal information, or any information resulting in a change to the applicant's policy, must have written consent. (Ex: addition of operator or location, experience letters, etc.)

An individual can change or withdraw consent in some situations, but not if it interferes with a legal obligation. (Section 9). When individuals exercise this choice we must advise them their decision may prevent us from providing them with insurance. This advice can be either written or verbal, in the latter case, file documentation is a must.

Regular updating of information on renewals, such as underwriting questionnaires or cost calculators, is not considered a new purpose and new consent is not required.

Cancellation requests will require the signature of all named insured's.

Experience letters will be mailed to the insured's address. No information is to be given via telephone. Facsimile or email requests must have the consent of all insureds. Experience letters may be directed to a third party (i.e. broker) via mail, facsimile or email provided we have the consent of all insureds.

#### Applications/questionnaires/quote sheets

##### Property

Personal Lines – application contains approved CSIO consent clause. Available on web site.

Questionnaires/quote sheets – reviewed web site. Majority of forms contain consent clause,

**Corporate Underwriting will add to remainder of forms. (June 2004)**

Farm – application contains approved CSIO consent clause. Available on web site.

Commercial apps/questionnaires/quote sheets – **Corporate Underwriting will add consent clause to these forms. (June 2004)**

##### Umbrella

Personal Lines – contains approved CSIO consent clause. Available on web site.

Farm – contains approved CSIO consent clause. Available on web site.

Commercial – **Corporate Underwriting will add consent clause. (June 2004)**

##### Automobile – Personal/Farm/Commercial

All auto forms are approved by the Government. The Alberta Superintendent of Insurance has not approved the consent clause for the SPF No. 1 yet thus we are not able to update any auto forms at all. **We will accept all existing automobile forms until further notice.**

#### SPECIAL NOTES:

Transfer and Consent - New application should be signed and completed as opposed to using Transfer and Consent form

Brokerage Letters - Underwriters to ensure the broker has a consent signed by their client

## 4. LIMITING COLLECTION

### Procedures:

Refer to General Section  
Privacy Principle #4 – Limiting Collection

## 5. LIMITING USE, DISCLOSE AND RETENTION

### Disclosure of Personal Information

We submit data, which does include some personal information, to industry related associations for the purposes of statistical data.

### Retention of Personal Information

#### Personal Info in paper file

- ◆ *On Site*
  - Calgary Commercial Dept. – 1 year; relocated offsite storage
  - Edmonton Commercial Dept. – 2 years; relocated offsite storage
  - Calgary Personal Lines – 1 year; relocated offsite storage
  - Northern AB Personal Lines – no files – paperless environment
  - ROC Personal Lines – no files – paperless environment
- ◆ *Off Site*
  - Calgary Commercial Dept. – commercial auto 3 years; all others indefinitely
  - Edmonton Commercial Dept. – commercial auto 3 years; all others indefinitely
  - Calgary Personal Lines – 3 years
  - Northern AB Personal Lines – cancelled files only destroyed after 3 years; all others kept indefinitely
  - ROC Personal Lines – cancelled files only destroyed after 3 years; all others kept indefinitely
  - Off site storage facility in Calgary is SPF Files and in Edmonton is Trust Documents Disposal
  - Both shred on their site

#### Transactional Filing on site

- ◆ Calgary Commercial Dept. - 90 days; recycled
- ◆ Edmonton Commercial Dept. – auto kept 90 days; farm kept 30 days, recycle bin; shredded weekly offsite. Commercial property does not have transactional filing.
- ◆ Calgary Personal Lines – 90 days; recycled
- ◆ Northern AB Personal Lines – 30 days; recycle bin; shredded weekly offsite
- ◆ ROC Personal Lines -30 days; recycle bin; shredded weekly offsite

#### Drop filing on site

- ◆ Calgary Commercial Dept. – kept indefinitely
- ◆ Edmonton Commercial Dept. – farm property only kept indefinitely

- ◆ Calgary Personal Lines – 3 years
- ◆ Northern AB Personal Lines – kept indefinitely
- ◆ ROC Personal Lines – kept indefinitely
- ◆ **We still have to determine when to destroy Commercial files and when to archive data on computer system.**

#### Electronic Files

- ◆ Retained on system for both Edmonton and Calgary offices since 1995

## 6. ACCURACY

#### Procedures:

Refer to General Section  
Privacy Principle #6 – Accuracy

## 7. SAFEGUARDS

#### Procedures:

Refer to General Section  
Privacy Principle #7 – Safeguards

## 8. OPENNESS

#### Procedures:

Refer to General Section  
Privacy Principle #8 – Openness

## 9. INDIVIDUAL ACCESS

#### Procedures:

Refer to General Section  
Privacy Principle #9 – Individual Access

## 10. CHALLENGING COMPLIANCE

#### Procedures:

Refer to General Section  
Privacy Principle #10 – Challenging Compliance

# PAYROLL

## 1. ACCOUNTABILITY

### Procedures:

We have one staff member who is responsible for administering our payroll system.

## 2. IDENTIFYING PURPOSES

### Purpose:

The information being collected is being used to set up an employee file, the employee's payroll record and the employee's company benefits.

## 3. CONSENT

### Procedures:

The Payroll Administrator collects the employee's written consent to collect personal information and the employee is made aware of the reason when they are asked to provide the information.

## 4. LIMITING COLLECTION

### Procedures:

Only relevant information is collected.

## 5. LIMITING USE, DISCLOSE AND RETENTION

### Procedures:

#### Disclosure of Personal Information

Who has access to the employees' personal information?

- ◆ the employee
- ◆ Management
- ◆ Canada Customs and Revenue Agency (CCRA) and
- ◆ the employee benefit carriers

The only other time personal information is disclosed is when an employee requests the information be disclosed. The request for disclosure to an individual outside the company must be a written request.

#### Retention of Personal Information

- ◆ Personal information is held on site for as long as the company employs the individual. Once the employee is terminated the file is retained until all documents are filed (ROE, T4, pension etc.). The file is sent to off site storage with limited access under a separate account where the records are kept indefinitely (records need only be retained for 7 years after termination)
- ◆ All computer records for terminated employees' are purged on an annual basis

## 6. ACCURACY

#### Procedures:

Take reasonable steps to ensure information is accurate, up-to-date, complete and not misleading

Amend incorrect information as it is requested

## 7. SAFEGUARDS

#### Procedures:

Personal information is protected as follows:

- ◆ All file cabinets are locked daily. Only the payroll administrator, controller and the financial accountant who acts as payroll back up, have keys.
- ◆ The payroll software is limited to only the payroll administrator's computer.
- ◆ There are 5 different passwords used to access different information.
- ◆ This computer has a screen saver that requires a password as well.
- ◆ All paper documents, (that can be destroyed), are shredded on site by the payroll administrator.

## 8. OPENNESS

#### Procedures:

Refer to General Section  
Privacy Principle # 8 - Openness

## 9. INDIVIDUAL ACCESS

Procedures:

Refer to General Section  
Privacy Principle # 9 – Individual Access

## 10. CHALLENGING COMPLIANCE

Procedures:

Refer to General Section  
Privacy Principle #10 - Challenging Compliance

# ACCOUNTS RECEIVABLE

## 1. ACCOUNTABILITY

### Procedures:

Refer to General Section  
Privacy Principle #1 – Accountability

## 2. IDENTIFYING PURPOSES

This is done by way of the consent clause on payment plan authorizations, which basically states personal information is being gathered for the purposes of making payments for the insured's insurance.

### Procedures:

We may collect any of the following personal information from the insured depending on billing plan selected:

- ◆ Visa or MasterCard - name of account holder, account number and expiry date
- ◆ Personal banking info - VOID cheque indicating:
  - bank, branch, telephone and transit number
  - Account holder's name, address, telephone number and account number

## 3. CONSENT

Each payment authorization should contain a consent clause with the purpose clearly defined.

### Procedures:

#### *Direct Bill*

- ◆ We accept Visa, MasterCard, EFT (electronic fund transfer), Interac payments and post-dated cheques

#### *PAC*

- ◆ We collect VOID cheques

The majority of the time this information is received by mail or fax. In these situations we obtain the insured's written consent on either the visa/master card form, or the PAC authorization form.

When this information is received by a phone call from the broker/insured we are obtaining insured's implied consent.

## 4. LIMITING COLLECTION

### Procedures:

If requested, we may give banking and/or credit card information to the broker. We must receive expressed consent (written or verbal) to follow this request.

Verbal consent will only be accepted in person and not via telephone, as we are not able to confirm it is the insured we are speaking with.

## 5. LIMITING USE, DISCLOSE AND RETENTION

### Procedures:

#### Limiting Use

Billing clerks enter insured's banking or credit card information into the accounting system.

The underwriter's may enter banking or credit card information into the underwriting system on new policies and then information is passed onto the Accounting Department for processing.

The following internal reports include varying degrees of insured's personal banking information:

- ◆ Upload and authorization sheets
- ◆ EFT (electronic funds transfer) payment sheets
- ◆ Refund reports
- ◆ PAC transmission sheets
- ◆ Stop payment requests

#### Retention of Personal Information

##### Personal info in paper format

- ◆ *On Site*
  - VISA and MasterCard - 2 years, then offsite
  - Void cheques - 1 year then shredded on site
- ◆ *Off Site*
  - All other info - kept offsite 7 years, then shredded
  - Off site storage facility is Trust Documents. They shred on site.

##### Personal info in electronic format

- ◆ Refer to Systems Department Privacy Module

## 6. ACCURACY

### Procedures:

Insured submits new banking, VISA or MasterCard information to broker or us to ensure our information is up-to-date.

## 7. SAFEGUARDS

### Procedures:

The following paper documentation is stored within the Accounting Department and is accessible only to individuals on a “need to know” basis:

- ◆ VISA and MasterCard authorizations
- ◆ void and post-dated cheques
- ◆ Reports containing insured's personal banking and/or credit card information

The above banking information is stored electronically on the company computer system and can be viewed by any staff member, however, cannot be altered by all, as there is restricted access to this area.

## 8. OPENNESS

### Procedures:

Refer to General Section  
Privacy Principle # 8 – Openness

## 9. INDIVIDUAL ACCESS

### Procedures:

An Insured may access their personal banking/credit information upon written request.

## 10. CHALLENGING COMPLIANCE

### Procedures:

Refer to General Section  
Privacy Principle #10 - Challenging Compliance

# SYSTEMS DEPARTMENT

## 1. ACCOUNTABILITY

### Procedures:

Refer to General Section  
Privacy Principle #1 - Accountability

## 2. IDENTIFYING PURPOSES

### Procedures:

Refer to General Section  
Privacy Principle #2 - Identifying Purposes

## 3. CONSENT

### Procedures:

Refer to General Section  
Privacy Principle #3 - Consent

## 4. LIMITING COLLECTION

### Procedures:

Refer to General Section  
Privacy Principle #4 - Limiting Collection

## 5. LIMITING USE, DISCLOSE AND RETENTION

### Procedures:

Insured's personal information is retained as long as the policy is effective or since 1995 if there is a claim.

The computer system is designed on a user's "need to know" basis.

Users are classified into different groups (example - Claims, Underwriting, Systems, Accounting, Marketing, etc).

Access rights to information in the system are granted to certain “user groups” depending on job requirement.

Destroy, erase or render anonymous when no longer required - our computer system has a purge function that removes unused information about an insured as long as they have been cancelled and there are no outstanding claims.

Access to data and computer programs is restricted to authorized personnel.

## 6. ACCURACY

### Procedures:

When data is entered on-line validity checks are in place.

Processing errors that are identified are corrected on a timely basis.

## 7. SAFEGUARDS

### Procedures:

The following safeguards are in place:

- ◆ Protect against loss of data with daily backups
- ◆ Authorized access required to enter building and server room
- ◆ Firewall implemented to manage public access to networked resources
- ◆ Access to system and network resources is password protected
- ◆ Individual computers are locked after 5 minutes of non-use
- ◆ Different modes in system allow user to add, edit, delete or inquire information
- ◆ Daily backup of computer data is stored off site
- ◆ Data submissions are sent to third party via courier
- ◆ Cryptography is used to protect confidential or sensitive programs and information when transmitted over communication line
- ◆ Encryption and decryption of data
- ◆ Recovery procedures are in place in the event of theft, loss, intentional or accidental destruction
- ◆ Provision for offsite processing in the event of disaster
- ◆ Restricted access to systems software and documentation to authorized personnel

## 8. OPENNESS

### Procedures:

Ensure staff is familiar with the policies and practices of the management of personal information.

## 9. INDIVIDUAL ACCESS

### Procedures:

Assist the requestor in accessing personal information

Ensure an individual supplies enough information to account for the existence, use and disclosure of their personal information

Update/correct information and notify any third parties that have access to the information

## 10. CHALLENGING COMPLIANCE

### Procedures:

Record the date a complaint is received and the nature of the complaint

Acknowledge receipt of complaint by notifying commissioner