

Manulife's Commitment to Privacy

Advisor Q&A on **Privacy Legislation**

Introduction

Protecting customers' private information is a top priority at Manulife Financial. Our employees understand the importance of maintaining customer privacy and confidentiality including the personal information in our care. We've been working to safeguard clients' personal information for decades – and during that time, our approach has evolved to support new legislative requirements.

Canada's federal privacy legislation takes full effect January 1, 2004. Plan advisors and plan sponsors have asked Manulife to explain what effect this legislation will have on group benefits plans and on the service process.

This question and answer series responds to issues raised by clients and advisors about the effect PIPEDA is likely to have.

If you have a question about privacy practices in use with your organization, please consult your legal advisor.

Q What is PIPEDA?

PIPEDA – the Personal Information Protection and Electronic Documents Act – will apply to all businesses operating in Canada effective January 1, 2004. Personal information of an identifiable individual cannot be collected, used or disclosed without the individual's knowledge and consent (except in limited circumstances). All private sector companies in Canada, including insurance companies and financial advisors, are governed by this Act or by a substantially similar provincial law.

The Act recognizes the distinctions between types of information and specifies appropriate rules or handling measures. For example, a request to use an individual's medical information, credit card numbers or other financial information requires the owner to provide more clear and detailed consent than a request for an individual's name and mailing address required to process some magazine subscriptions.

Federally regulated institutions (banks and national transportation companies, for instance) have been governed by PIPEDA requirements since January 1, 2001.

Q What is 'personal information'?

Personal information includes any detail – whether it's a fact or subjective detail -- about an identifiable individual. This includes age and name, along with any sort of identification number from an obvious identifier like a social insurance number to a library card number.

This broad category also includes details about any individual's:

- income
- ethnic origin
- blood type
- opinions
- evaluations (report cards or employer evaluations)
- comments
- social status
- disciplinary actions
- employee records
- credit records

- loan records
- medical records
- existence of a dispute between a consumer and a merchant and/or
- intentions (to acquire goods or services or change jobs).

Personal information **does not** include the name, title, business address or business telephone number of an employee.

Q Does Manulife have established practices regarding privacy legislation?

Manulife has long-standing privacy protection practices. More recently, in 1993, Manulife's Canadian Division introduced formal policies and practices in compliance with Quebec's privacy legislation. Quebec's private sector Privacy Act is much like PIPEDA. Manulife's practices have evolved during this decade. The strong knowledge base and clear handling guidelines we established early on have been helping to protect our customers' privacy effectively – and we will continue to enhance our programs.

In conjunction with the Canadian Life and Health Insurance Association (CLHIA), Manulife's Group Benefits team regularly monitors privacy legislation developments for collecting, using and disclosing customers' personal information. This helps to ensure we're protecting confidential customer details effectively. We monitor privacy legislation and adapt administrative procedures as necessary. Manulife's Canadian Division's privacy policy appears on our public web site so any customer can review it in detail at any time.

Q When is member consent required?

Consent is required whenever personal information is collected, used or disclosed – with limited exceptions described below.

Member consent should be obtained before or at the time of collection of personal information. For example:

- when an employee enrolls for benefits or submits a claim form;
- when a transaction or a relationship is initiated (when a member dependant accepts a drug card to use for direct transactions).

Some exceptions are identified in the new federal legislation. Consent is not required when disclosure is required by law or a potential breach of an agreement is under investigation. In addition, solicitor-client privilege does not require explicit consent.

Q What form should consent take?

Generally, consent should be expressed and informed. Expressed consent means direct verbal or documented permission. For example, express consent should be obtained from a member before sensitive information such as medical, financial or credit information can be obtained. There is, however, considerable flexibility in the form of consent (either written or oral) but it must be appropriate to the specific circumstances. The designation of a beneficiary or consent to release medical information must be documented in writing.

Q Can consent be implied?

Consent should be expressed in most circumstances, especially when a member (an individual) is consenting to the release or use of sensitive information. In some circumstances, consent can be implied from certain actions when the individual clearly understands the meaning of his or her actions.

Specifically where benefits are concerned, these examples detail circumstances under which implied consent can be seen as being given:

- When a plan member presents a pay-direct drug card to a pharmacist instead of paying for a prescription, the pharmacist provides relevant information to the insurer

to obtain payment for the service rendered. This allows the insurer to process the claim. By presenting the card for service, the member consents to allowing the pharmacist and insurer to make use of the personal information required to process the claim.

- When a spouse or dependant provides a receipt to the plan member for submission to the insurer, or uses a pay-direct drug card to fill a prescription, the insurer has implied consent to collect, use and disclose the personal information necessary to process the individual's claim.
- Personal information provided to an insurer for establishing and administering a member's benefits prior to the effective date of the legislation is deemed as being given with the participating member's consent.

Privacy legislation in British Columbia provides specific rules with respect to implied consent as the notion relates to group benefits plans. This legislation specifically says an individual is deemed to consent to the collection, use or disclosure of personal information for the purpose of enrolment and coverage under an insurance, pension, benefit or similar plan if he or she is a beneficiary of a plan member or has an interest as an insured member covered under the plan.

Q Whose consent is required?

Ideally, consent to use any information should be provided by the individual to whom the information relates. In the case of a group benefits plan, an insurer usually communicates only with the plan member, and not directly with that member's dependants (who may be eligible for benefits). In some situations, the insurer will require a dependant's expressed consent. If, for instance, an insurer requires additional medical information from a third party (such as a physician) before the insurer can agree to provide benefits for that dependant, the dependant's expressed consent must be given to the insurer before that additional information can be collected.

Q Does consent allow for unlimited collection, use and disclosure of personal information?

No. There are other principles that govern appropriate collection, use and disclosure of personal information. Before an individual or company can collect information, the purpose for which the details will be used must be identified.

Identification of purpose – A firm or individual collecting information must explain why the information is required. For example, asking for a dependant's birth date and address is appropriate, as an insurance carrier needs these details to satisfy eligibility criteria.

Limitation of collection – Only information related to the purpose in question can be requested. For instance, an individual applying for a mortgage can't be asked about family medical history.

Limitation of use – Details collected for one purpose can't be shared and used for any other.

Plan members shouldn't be asked to give a blanket consent for personal information without purpose and limitations being disclosed.

To be valid, consent must:

- be informed and voluntary
- relate to an identified and legitimate purpose
- relate only to information necessary for a specified purpose, and
- be used in conjunction with the other principles.

Q Can a plan sponsor or administrator collect personal enrolment information from a plan member?

Yes. Some employee information needed to manage a benefit program may flow through the plan sponsor; however, the plan member may choose to submit additional personal information to the insurer directly.

Q Can a plan sponsor or administrator certify eligibility for a claim?

Yes, but the plan member can choose to provide the plan sponsor or administrator only with the information required for the certification process. A plan member is not obliged to provide any claim details. The member can submit all other information directly to the insurer, in a sealed envelope or other secure form that protects confidentiality.

Q Can a plan sponsor audit enrolment or claim files?

Audits of enrolment or claim files can be conducted provided all principles governing the protection of personal information are respected. Before Manulife agrees to any audit, the auditor will be required to complete a confidentiality agreement and Manulife will monitor the auditor's use of information. To protect members' confidentiality, Manulife recommends that plan sponsors contract a third party to conduct plan audits.

Q When can personal information be collected or disclosed to another insurer or administrator?

Personal information can be collected, used or disclosed to accomplish the purpose(s) for which consent has been provided even though the member hasn't provided expressed consent (to co-ordinate benefits; to move member data when an insurer or administrator changes; to transfer business when a company is involved in a merger; or to transfer member files when a company has sold a block of business). All other principles governing the protection of personal information must apply, and the information should be transferred directly between the parties involved, not through the plan sponsor. In the event that the new administrator is also the plan sponsor, a confidentiality agreement indicating

that information will be used solely for the purpose of ongoing plan administration should be in force.

In any instance where information is used or disclosed for a different purpose, the individual member must provide consent.

Q What restrictions does Manulife put on plan sponsor reporting?

Personal information, including claims experience for plan members, dependants, or any other identifiable individual must not be disclosed routinely to the plan sponsor or to any other party. Any information provided to the plan sponsor must protect member anonymity. Identifiers such as names and certificate numbers must be removed.

Detailed claims listings without identifiers are considered personal information. Therefore, Manulife places restrictions on the amount of detail that can be provided to plan sponsors in an effort to ensure that personal information protected by PIPEDA cannot be linked to an identifiable individual.

To protect member confidentiality:

- Detailed claims listings, usually sent at renewal, exclude names and certificate numbers that can identify specific individuals.
- There are some reporting restrictions for groups with fewer than 50 employees to ensure the privacy of employees' personal claims information.
- Plan sponsors do not have access to plan members' personal information on health and dental claim statements distributed to plan members.

All drug claim submissions reports are reviewed to ensure information protected under PIPEDA cannot be linked to specific identifiable individuals.

Q Is there going to be an effect on the quote process?

Based on our practices and interpretation of PIPEDA, we do not anticipate changing the quotation process.

Q What are the risks in faxing personal information?

Faxing personal information may increase the risk that highly sensitive details will fall into the hands of people who should not receive them. Risks in faxing include dialing a wrong fax number that could accidentally send sensitive personal information to the wrong person, or placing a fax machine out in the open where personal information received may be visible to passers-by.

If you must fax personal information, consider buying a machine that encrypts transmissions. For more information and tips on reducing the risks of faxing, visit the Privacy Commissioner of Canada's web site at www.privcom.gc.ca

Q How does Manulife protect employee information on the Internet?

Manulife Financial provides layers of protection for all information on its secure sites based on a combination of the latest information security technology and existing trustworthy practices. We use Secure Socket Layer (SSL) technology and either 128-bit or 40-bit encryption to provide a very high level of confidentiality. All major changes to Manulife's e-commerce environment over the Internet are subject to independent external review including Attack and Penetration Studies. Professional information security practitioners are responsible for overseeing the security of our Internet connection, including active participation in the information security community to learn of new exposures and measures to combat them.

Q Can an employee's Social Insurance Number (SIN) be used as the employee certificate number?

Many plan sponsors use employees' social insurance numbers (SIN) as certificate numbers for their group benefits plans. Currently, no legislation prohibits organizations from collecting and using SIN for identification purposes **providing those organizations have the employee's consent**. Sponsors considering this should be advised that the Office of the Federal Privacy Commissioner has recently advised against this practice, and should seriously consider alternative certificate numbering.

Q What other resources are available?

Manulife's Canadian Division's privacy policy appears on our public web site at www.manulife.ca.

The Privacy Commissioner of Canada has published an information guide for businesses and other organizations. Their web site, www.privcom.gc.ca, also contains links to provincial privacy commissions. Similar sites are available in provinces that already have legislation, such as Quebec, Alberta and British Columbia.

We will provide updates on any new developments related to PIPEDA or other privacy legislation.

The data contained in this article is for informational purposes only. Specific questions about the collection, use or disclosure of personal information in any organization should be directed to that firm's legal advisor.