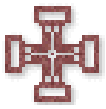
Health Canada Santé Canada

Non-Insured Health Benefits



Privacy Training

Printable version (Text-only)

Canada

Table of Contents

Canada

Non-Insured Health Benefits Privacy Training

Welcome to the on-line privacy training for the Non-Insured Health Benefits (NIHB) program of the First Nations and Inuit Health Branch of Health Canada. This training is for everybody involved in delivering Non-Insured Health Benefits. It is a guided tour to the secure collection, use and disclosure of our clients' personal information.

This training module also includes scenarios (questions) which will test your understanding of what you have learned in the previous section. These scenarios will help you apply protection of privacy to your everyday work environment.

- During the next 20-30 minutes, you will learn:
- What measures exist to protect personal information; and
- What you can do to ensure the protection of clients' personal information.

Narration is provided. To listen, click on the start button in the audio controller at the top of each page. You can also pause, rewind and fast forward.

If you don't see any audio buttons, you will need a media player plug-in for your computer. If your browser does not have a plug-in installed, you may download one free of charge.

- To move through the topics, use the links at the bottom of the page.
- To move to the next topic, choose the 'Next' link,
- To move backwards to review previous topics, choose the 'Previous' link.
- To jump to another topic, choose the 'Table of Contents' link.

To begin:

Choose one of the following links:

- I am a NIHB employee.
- I provide Non-Insured Health Benefits through a contribution agreement.

What is Privacy?

Privacy is the freedom from intrusion into and exposure of personal affairs. It is a basic human right. Everyone has the right to control who has access to his or her personal information and how it will be used.

Privacy is about ensuring client confidentiality through responsible and secure handling of personal information collected for program delivery, administration and management.

Perspectives

It's important to look at privacy from our clients' perspective. You can easily imagine why a client would want to keep their medical information confidential and know the consequences should someone in a position of trust disclose information.

Another way to look at it is from the perspective of the federal and provincial laws and departmental policies that protect privacy:

- The *Privacy Act*
- The *Charter of Rights and Freedoms*
- The *Access to Information Act*
- Treasury Board policies and guidelines, including the Treasury Board of Canada Government Security Policy
- The Health Canada Security Policy
- The *Personal Information Protection and Electronic Documents Act (PIPEDA)*

In the 'Privacy Links' section, you can explore the details of the Acts and policies that apply to you. One of things that you will notice is the standard set of privacy principles that are used in Canada. They are:

- Accountability
- Identifying Purposes
- Consent/Authorization
- Limiting Collection
- Limiting Use, Disclosure and Retention
- Accuracy
- Safeguards
- Openness about Policies and Practices
- Individual Access
- Challenging Compliance

Your official guide is the Non-Insured Health Benefits Privacy Code. It's a set of guidelines to be used regularly on the job to raise awareness of privacy. It is available on the Health Canada Website.

Privacy Starts with You

Everyone involved in handling personal information has a responsibility to keep it secure and confidential. It's about earning and keeping the trust of our clients.

We are all accountable.

- Employees need to follow the Non-insured Health Benefits Privacy procedures.
- Managers are expected to set an example for compliance with the policies and procedures.
- Contractors have to obey standard privacy clauses.
- Health-care professionals must respect the privacy codes of their regulatory or licensing bodies.

Any breach of the privacy procedures may result in disciplinary action. This may include suspension, dismissal or termination of a contract.

 Scenario

You have been talking with a client about their prescription and reason for seeking mental-health counselling. While having lunch in the cafeteria, a co-worker who is not involved with the client's request for benefits, asks you about the client's reason for calling.

What should your response be?

A. Change the topic.
B. Talk about the prescription, but not the reasons for counselling.
C. Point out that personal information cannot be disclosed unless required to provide a benefit/service.
D. Ask your colleague to stop by your cubicle after lunch as personal information cannot be discussed in the cafeteria.

Scenario Answer

The correct answer is C.

Point out that personal information cannot be disclosed unless required to provide a benefit or service. Since your co-worker is not involved with this client's request for benefits, it would be a breach of privacy to disclose any information.

A crowded cafeteria is most definitely not the place to discuss a client's personal information. Even discussing it in a secure location, with this co-worker, is a breach of privacy. This violates both the trust of the client and the *Privacy Act*. It's a very serious offence with consequences to the client, the organization and to you.

Changing the topic is incorrect. It does not help your co-worker understand that he or she is breaching the privacy of the client.

Collecting Personal Information

The collection of personal information is limited to the sole purpose of providing non-insured health benefits to clients. Only collect what is necessary when it is needed.

What personal information is collected?

Only the minimum amount of personal information required to assess the need for a benefit is collected. The three pieces of information required to identify and provide benefits to a client are:

- Name
- Date of birth
- Identification number

Other personal information that might be collected includes:

- Diagnosis, treatment, care and health information directly related to the benefit request.
- Additional health information may be required for prior approvals and exceptions.

Why is personal information collected?

Our clients often want to know why their personal information is required. There are two reasons for collecting personal information in the Non-Insured Health Benefits program:

- To review benefit requests for funding
- To conduct reviews of program benefits and administration

How is the information collected?

Personal information is collected either directly from the client or indirectly from a parent or guardian, or provider that is registered with NIHB. We must inform clients about how their information is collected, used, disclosed and protected by the Program.

We do not require formal permission (express consent) from our clients to collect and use their personal information for the everyday processing of benefit requests and program administration. Express consent is required when we need to share information with appropriate health-care professionals. This would be the case where patient safety or inappropriate use of the Program may be of concern. Express consent can be given verbally or in writing.

Accuracy

The collection of personal information must be accurate to provide benefits. We ensure this by:

- regularly updating client eligibility lists
- requiring client identification by name, date of birth and identification number
- having mandatory information fields in our computer systems that must be fully completed for the claim to be processed.

Inaccurate information may cause delays in processing claims.

Scenario

A client calls your office to find out if she is eligible for benefits. You collect her name, date of birth and identification number, but the client also tells you her social insurance number.

Can you write down her social insurance number and keep it in on file?

Scenario Answer

No.

You would tell the client that a social insurance number is not required for Non-Insured Health Benefits. Collecting it would be a breach in privacy.

Using and Sharing Personal Information

Like collection, the use of personal information is limited to the administration, delivery and management of the Non-Insured Health Benefits program. Restricting access to client information on a need-to-know basis also helps to limit the use and disclosure of personal information.

You may use and share personal information only when required with the following people:

- Non-Insured Health Benefits program staff and contractors;
- Health care professionals and providers. This includes doctors, nurses, pharmacists, optometrists/opticians, dentists, denturists, registered psychologists, social workers, medical supply and equipment and transportation providers;
- First Nations and Inuit organizations administering Non-Insured Health Benefits under contribution agreements; and
- Other third-party health insurers who coordinate or extend benefit coverage.

Before providing anyone with a client's personal information, you should ask yourself:

- What is the need for the information?
- Does this person need to know?

Scenario

A provider calls Non-Insured Health Benefits with the necessary identification for a client. The identifiers match the client record in the database except the date of birth in our system is different from the one given by the provider.

Can you give the provider the correct date of birth to update their records?

Scenario Answer

No.

Giving the provider the correct date of birth is a breach of privacy. The provider can ask the client to confirm their date of birth then submit the claim.

Storage and Disposal of Personal Information

Records must be kept for at least seven years. This includes personal information, whether filed in cabinets or stored in the databases of our computer systems. After seven years, records may be disposed of in a secure manner. However, some records may be kept for more than seven years. To learn more about the storage and disposal of personal information, look in the 'Privacy Links' section.

Protecting Personal Information

Keeping client personal information secure and confidential is the responsibility of all Program employees. Good habits go a long way!

- Do you have passwords in plain view, such as on sticky notes attached to your computer monitor, or on calendars or notepads around your desk?
- Do you lock your workstation before leaving it unattended?
- Do you double check fax numbers and e-mail addresses before pressing 'Send'?
- Do you shred waste paper containing personal information?

Chances are your common sense will guide you. To help you out, there are a number of procedures and standards to safeguard personal information that you need to be aware of.

At Health Canada

Health Canada has a number of procedures and policies to help protect personal information. These include authorizing computer system access and file security measures.

Personal information collected by the Program is classified as "designated information."

- You must mark it PROTECTED.
- You must keep designated WASTE separate from regular waste.
- You must shred, pulp or burn designated WASTE.

Around the office

- You should always use secure computers and fax machines.
- You are responsible for keys, locks and safe combinations.
- You must report loss or theft of personal information.
- You must wear your identification badge at all times.
- When you move to another job, your access to buildings will be withdrawn.
- Random security inspections help to keep everyone aware of security procedures.

In our computer systems

- We provide passwords to computer systems only to those who need to use them.
- We ensure that database fields are available only to those who need to know.
- Only NIHB managers can request passwords for staff and authorize access to specific benefit databases.
- When you move to another job, your access to computer systems will be withdrawn.

Contractors and Consultants

Contractors and consultants have confidentiality clauses in their contracts. Their access to personal information is limited.

Scenario

You are getting ready to attend a meeting. What steps should you take before leaving a workstation unattended?

A. Organize paper on your desk so that you can complete the most urgent client files after the meeting.
B. Secure your computer workstation and remove client files from your desk.
C. Place all client related documents face down on your desk.

Scenario Answer

The correct answer is B.

You need to get all client files off your desk and lock your computer before you go. The files need to be secured in a locked cabinet or drawer. You can secure your computer by logging off the network. You may also use a password-protected screensaver.

Scenario

You have been asked to send 'Designated - PROTECTED' information to another department.

Can you send this information by e-mail?

Scenario Answer

Yes.

You can send 'Designated - PROTECTED' information by e-mail if you follow these steps:

- Include 'Designated - PROTECTED' in the subject line
- Indicate in the message that the information is for the use of the addressee only and unauthorized use or retransmission is prohibited
- Include the sender's full contact information in the message signature
- Verify the correct e-mail address of the recipient
- Use the receipt confirmation option in the e-mail program
- Telephone the recipient before sending the message so that it is expected and after sending to verify that it was received.

Scenario

You have been given 'Designated - PROTECTED' information to photocopy for a meeting the next day. What is the best way for you to do this?

A. Wait until just before the meeting so that copies don't exist any longer than they have to.
B. Immediately rush the file by courier to a print shop.
C. Do not make any copies because it is a breach of privacy to duplicate 'PROTECTED' information.
D. Ensure that both the original and copies are marked 'PROTECTED' and are securely stored until the meeting.

Scenario Answer

The correct answer is D.

You need to make the copies yourself, allowing time to take the following precautions:

- First check that the material is marked 'PROTECTED'.
- Remove personal identifiers if possible.
- Keep the number of copies to a minimum.
- Mark the copies 'PROTECTED'.
- Shred any spoiled copies.
- Store originals and copies in a secure area or in a locked cabinet until the meeting.

Empowering Clients

By being open about our policies and practices, we empower our clients to become aware of privacy.

This has two benefits:

- It strengthens the accountability of our Program staff, and
- It builds trust between our staff and clients who will feel confident that their personal information is being handled securely.

Everyone who provides or receives non-insured health benefits can find out about the privacy policies and procedures. The Health Canada web site provides the latest information.

Clients have the right to ask what personal information exists in program files. They have a right to question if the information is accurate and complete. They also have a right to complain if they feel their privacy has been breached.

Summary

This training has taken a look at how the Program collects, uses, shares, stores and protects the personal information of its clients. The following questions summarize what you need to know.

What personal information do we collect?

Only information required to assess the need for a benefit is collected. Name, date of birth and identification number is the minimum requirement for identification. Other personal information collected by the Program may include names of children and legal dependants, diagnostic, treatment, care and health information directly related to benefit requests.

Why do we collect it?

- To review and approve requests for benefits and to process claims from providers.
- To be accountable for the use of public funds.

How do we collect it?

- Directly from the client.
- Indirectly from the client's parent or guardian or health care provider.
- We make sure the information is accurate for the safety of the client and to prevent delays in processing claims.

How do we protect it?

- With common sense and vigilance.
- By obeying privacy policies and laws.
- By understanding what privacy protection really means.

With whom do we share it?

We share it carefully between Program staff and contractors, health-care professionals, service providers, and First Nations and Inuit groups administering non-insured health benefits under contribution agreements. But only if and when they need to know. Information is shared only when it relates to the benefit being requested by the client.

Privacy Links

Federal Privacy Protection

Privacy Legislation in Canada
http://www.privcom.gc.ca/fs-fi/02_05_d_15_e.asp

An overview of provincial and federal laws regarding privacy in Canada.

Using the *Access to Information Act* and *Privacy Act*
http://canada.justice.gc.ca/en/ps/atip/using.html

An overview on the *Access to Information Act* and *Privacy Act*.

Access to Information and Privacy
http://canada.justice.gc.ca/en/ps/atip/

Canadian laws and policies dealing with access to information and privacy.

NIHB Privacy Code
http://www.hc-sc.gc.ca/fnihb-dgspni/fnihb/nihb/privacy_code.htm

A set of guidelines for Health Canada's Non-Insured Health Benefits (NIHB) employees to ensure the confidentiality of personal information that the NIHB program collects and uses.

Privacy Act
http://laws.justice.gc.ca/en/P-21/

The Privacy Act protects your personal information collected by the federal government and gives you the right to see it.

Access to Information Act
http://laws.justice.gc.ca/en/A-1/

The *Access to Information Act* entitles you to examine or obtain non-personal information contained in federal government records.

Canadian *Charter of Rights and Freedoms*
http://laws.justice.gc.ca/en/charter/

An overview of the Canadian *Charter of Rights and Freedoms* and other Human Rights.

Info Source Publications
http://infosource.gc.ca/index_e.asp

Info Source Publications is a key reference tool to assist members of the public in exercising their rights under the *Access to Information Act* and the *Privacy Act.*

Info Source - Health Canada - Personal Information Bank
http://infosource.gc.ca/inst/shc/fed07_e.asp

Information on Personal Information Banks within Health Canada

Non-Insured Health Benefits
http://www.hc-sc.gc.ca/fnihb-dgspni/fnihb/nihb/index.htm

The Non-Insured Health Benefits Directorate provides medically necessary health-related goods and services, not covered by other federal, provincial, territorial or third-party health insurance plans, to eligible registered Indians and recognized Inuit and Innu.

Privacy and Data Protection
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/CHAP1_1-1_e.asp

Government of Canada Policy on collection, data-matching and data linkage of personal information.

Government Security Policy
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg_e.asp

The Government Security Policy complements other Treasury Board policies for the management of information.

Personal Information Protection and Electronic Documents Act (PIPEDA)

***PIPEDA* for Health Sector Associations and Providers**
http://www.hc-sc.gc.ca/ohih-bsi/theme/priv/privinfo_e.html

A Guide to Privacy under *PIPEDA*
http://www.privcom.gc.ca/information/guide_e.asp

A Guide for Businesses and Organizations - Your Privacy Responsibilities

Frequently Asked Questions about *PIPEDA*
http://privacyforbusiness.ic.gc.ca/epic/internet/inpfb-cee.nsf/en/h_hc00003e.html

***PIPEDA* Awareness Raising Tools (PARTs) Initiative For The Health Sector**
http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00207e.html

Privacy for Businesses
http://privacyforbusiness.ic.gc.ca/epic/internet/inpfb-cee.nsf/en/Home

Gearing up for the *Personal Information Protection and Electronic Documents Act*
http://www.privcom.gc.ca/fs-fi/02_05_d_16_e.asp

Provincial and Territorial Privacy Laws

Provincial and territorial legislation
http://www.hc-sc.gc.ca/ohih-bsi/theme/priv/index_e.html#prov

Ontario's *Personal Health Information Protection Act*
http://www.health.gov.on.ca/english/public/updates/archives/hu_03/priv_legislation.html

Retention and Disposition of Records

The Government Records Disposition Program of the National Archives of Canada
http://www.collectionscanada.ca/information-management/0605_e.html

Retention and Disposal of Personal Information
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/CHAP2_3-1_e.asp

National Archives Act
http://laws.justice.gc.ca/en/N-2.5/

Policy on the Management of Government Information
http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/TB_GIH/mgih-grdg_e.asp

Answers to Questions about Privacy

Who ensures that employees and contractors know there is a Privacy Code and are abiding by it?

Non-Insured Health Benefits (NIHB) managers are responsible to ensure that all employees under their supervision comply with the NIHB Privacy Code.

Contractors must abide by the confidentiality clauses in their contracts. NIHB is responsible for ensuring a comparable level of protection is in place for personal information that has been disclosed or transferred to a third party, such as a contractor responsible for claims processing purposes.

Employees and contractors who are health care professionals are also bound by their licensing organization to ensure the protection of personal information.

What are the consequences if they don't abide by it?

Employees are subject to subsequent investigation which may result in disciplinary action.

Contractors are subject to the termination of their contract and subsequent investigation by Health Canada.

Health care professionals who are employees of Health Canada are subject to the same monitoring as NIHB staff in terms of their responsibility to meet the confidentiality requirements and may also face investigation by their respective professional, regulatory or licensing bodies.

Who is the Privacy Officer for my department?

In all of the NIHB Regions there is a designated Privacy Coordinator and the name of the Privacy Coordinator can be provided when contacting the First Nations and Inuit Health Branch Regional Office.

What are the consequences to organizations or groups involved in contribution agreements if they do not meet confidentiality clauses of their contribution agreement?

The NIHB Privacy Code has been developed to be used by NIHB staff administering and managing the Program. Organizations or Groups administering NIHB benefits through contribution agreements must comply with privacy requirements found in the schedules, and confidentiality clauses that form part of the Terms and Conditions of the agreement. The clauses for the year 2004-2005 read as follows:

> 11.
>
> The Recipient shall ensure that any information of a confidential nature, relating to the affairs of the Minister, to which the Recipient or its officers, servants or agents become privy pursuant to or as a result of this Agreement, shall, unless this Agreement provides otherwise, be treated as confidential and not disclosed to any

person except with consent of the Minister or otherwise in accordance with applicable law.

The Minister shall ensure that any information of a confidential nature, relating to the affairs of the Recipient to which the Minister or his officers, servants or agents become privy pursuant to or as a result of this Agreement, shall, unless this Agreement provides otherwise, be treated as confidential and not disclosed to any person except with the consent of the Recipient or otherwise with applicable law.

12.

The Recipient shall ensure that all information of a personal medical nature to which the Recipient or its officers, servants, or agents become privy pursuant to or as a result of this Agreement, shall be treated as confidential and not disclosed to any person except with the consent of the individual to whom the information relates, or otherwise in accordance with applicable law.

The Minister shall ensure that all information of a personal medical nature to which the Minister or his officers, servants, or agents become privy pursuant to or as a result of this Agreement, shall be treated as confidential and not disclosed to any person except with the consent of the individuals to whom the information relates, or otherwise in accordance with applicable law.

If a group or organization is identified as not meeting the First Nations Inuit Health Branch (FNIHB) contribution agreement privacy requirements, a plan will be developed by FNIHB and the First Nations organization to address the situation. If the problem cannot be resolved the contribution agreement may be terminated.

Organizations are subject to either federal, provincial, or territorial data protection legislation, including the *Personal Information Protection and Electronic Documents Act*, and its provincial counterparts in Quebec, British Columbia, and Alberta. In Ontario, the *Health Information Protection Act* will take effect in November 2004. This Act ensures the privacy, confidentiality and security of personal health information that is collected, used and disclosed by individuals and organizations.

It is recommended that all First Nations and Inuit groups administering Non-Insured Health Benefits put in place their own Privacy Code to ensure that clients are aware of their commitment to privacy and protection of personal information.

If an employee is given access to a system for specific records, is there a check on whether that employee is accessing only that information? Is there a mechanism to prevent the employee from browsing through files within the system?

At this time, there is a mechanism for the tracking of individuals making changes to information but no capacity exists to track viewing and searches on Non-Insured Health Benefits (NIHB) systems. The NIHB Directorate is reviewing current systems capacities and looking at opportunities to enhance systems to fully track user activities.

All employees must have designated security clearances and authorization from their manager in order to have access to the electronic systems and paper files they require to do

their job. There is a specific process involving authorization which is controlled at the NIHB Directorate 'Operational Support and Systems Maintenance' in Ottawa.

How would you send Designated documentation within Health Canada and externally? If a Designated document needs to be faxed, does it have to be faxed to a designated protected fax machine, and who is entitled to pick it up/read it?

Personal information collected by the Non-Insured Health Benefits (NIHB) program for review and claims processing is classified, according to the Government of Canada Security Policy, as "DESIGNATED" information. Originals and copies must be marked PROTECTED in the upper right corner of the front page of the document.

Duplicating or taking extracts of designated information is kept to a minimum and the copies/extracts are marked with the same security marking as the original.

NIHB employees must not remove designated materials from secure areas in the departmental workplaces. In special circumstances, such as tele-work arrangements, an exception may be made in the case of PROTECTED information.

Protected documents may be sent by fax, Telex or e-mail unless greater safeguards, such as encryption are indicated.

Waste materials: Designated waste is kept separate from regular paper waste and is shredded, pulped or burned.

For additional information, consult Health Canada Security Policy under Security - Transporting & Transmitting Sensitive Material.

Should staff use "Protected" or "do not copy" stamps?

Designated information should be marked 'Protected' at the time it is created or collected. However, it must be marked if it is to be disclosed beyond the organizational unit that created or collected it.

For additional information, consult Health Canada Security Policy under Security - Marking and Photocopying Sensitive Information.

Are paper and electronic records destroyed after 7 years? Who does this?

Paper and electronic records must be kept for a minimum of 7 years and are destroyed according to the Records and Retention Disposal Policy of the Government of Canada as set out by the *National Archives Act.*

How do groups involved in contribution agreements deal with documentation of personal information after the minimum 7 year period for retention has passed? Does the information come back to NIHB for disposal?

The contribution agreement recipient maintains ownership of all documents that are collected as part of the administration of a contribution agreement. However, they are required to provide reports as per the terms and conditions of the agreement and to keep and maintain all accounts, financial records and supporting documentation for a period of seven (7) years unless advised otherwise, in case of audit.

Under the confidentiality section of the agreement, recipients are required to handle personal information "in accordance with applicable law". This would include the disposal of confidential documentation. Recipients of agreements are also bound by either the federal, provincial/territorial privacy laws.

Who tracks which employees have received Non-Insured Health Benefits (NIHB) Privacy training?

NIHB Managers across Canada are required to ensure:

- that new and current employees are informed of and receive a copy of the NIHB Privacy Code,
- that all employees review the Privacy Code annually as part of their Performance Review.

In addition, Managers are to ensure that casual employees have read and understand the NIHB Privacy Code.

Is there one database in the regions or headquarters which will note who has had privacy training and when?

There is no single database to track Non-Insured Health Benefits Privacy Code training. However, each area must ensure that every employee is familiar with the most up-to-date copy of the NIHB Privacy Code. The Code can be found on the Health Canada Website at the following location:

http://www.hc-sc.gc.ca/fnihb-dgspni/fnihb/nihb/privacy_code.htm

How can we be sure that other employees that we share client files with have received privacy training?

Non-Insured Health Benefits managers are responsible to ensure that all current and new employees are informed about and understand privacy in the workplace. They are also responsible to ensure that employees are given privacy training.

This On-line Privacy Training Module is one example of a learning tool accessible to all Non-Insured Health Benefits employees.

How do you know when sending a protected document to someone if they have the correct security clearance to view this information?

Managers are also responsible to ensure that employees have the appropriate level of security clearance for their day to day work. Each position has a security designation which must be met at the time they are hired.

A provider calls Non-Insured Health Benefits (NIHB) with the necessary identification for a client. Each identifier matches, except the date of birth which is incorrect. Is the NIHB employee permitted to give the provider the correct date of birth?

No. The employee is not permitted to disclose the date of birth to the provider. The provider should advise the client of the error and to contact their First Nations and Inuit Health Branch regional office which will provide the client with the information on how they can update/correct the information.

Are Privacy Impact Assessment documents available to the public? What about the Threat & Risk Assessment documents?

A Privacy Impact Assessment is a public document. It is available by making a formal request to the Access to Information office. Threat and Risk Assessments are classified as 'Designated' and are not available to the public.

Privacy and Contribution Agreements

Privacy is the freedom from intrusion into and exposure of personal affairs. Everyone has the right to control who has access to his or her personal information and how it will be used.

If you administer Non-Insured Health Benefits under a contribution agreement, you are responsible for protecting the confidentiality of the personal information that you collect and use everyday. To find out what is involved, you should:

- Review the privacy requirements found in the schedules, and confidentiality clauses of your contribution agreement.

The confidentiality clause in contribution agreements is provided in the Frequently Asked Questions below.

- Review federal, provincial, or territorial laws that deal with the protection of personal information.

The federal *Personal Information Protection and Electronic Documents Act (PIPEDA)* applies to all provinces except Quebec, British Columbia and Alberta. These three have developed their own provincial laws that are comparable to *PIPEDA*. In Ontario, the *Health Information Protection Act* will take effect in November 2004. This Act ensures the privacy, confidentiality and security of personal health information that is collected, used and disclosed by individuals and organizations.

You can learn more about federal, provincial and territorial laws in the 'Privacy Links' section.

Frequently Asked Questions about Privacy and Contribution Agreements

Are organizations or groups involved in contribution agreements required to meet Non-Insured Health Benefits (NIHB) Privacy Code requirements?

The NIHB Privacy Code has been developed for the use of NIHB staff administering and managing the Program.

Organizations or groups administering NIHB benefits through contribution agreements must comply with the privacy requirements found in the schedules, and confidentiality clauses that form part of the Terms and Conditions of the agreement.

The standard clauses in Health Canada's contribution agreements for the year 2004-2005 read as follows:

> 11.
>
> The Recipient shall ensure that any information of a confidential nature, relating to the affairs of the Minister, to which the Recipient or its officers, servants or agents become privy pursuant to or as a result of this Agreement, shall, unless this Agreement provides otherwise, be treated as confidential and not disclosed to any person except with consent of the Minister or otherwise in accordance with applicable law.
>
> The Minister shall ensure that any information of a confidential nature, relating to the affairs of the Recipient to which the Minister or his officers, servants or agents become privy pursuant to or as a result of this Agreement, shall, unless this Agreement provides otherwise, be treated as confidential and not disclosed to any person except with the consent of the Recipient or otherwise with applicable law.
>
> 12.
>
> The Recipient shall ensure that all information of a personal medical nature to which the Recipient or its officers, servants, or agents become privy pursuant to or as a result of this Agreement, shall be treated as confidential and not disclosed to any person except with the consent of the individual to whom the information relates, or otherwise in accordance with applicable law.
>
> The Minister shall ensure that all information of a personal medical nature to which the Minister or his officers, servants, or agents become privy pursuant to or as a result of this Agreement, shall be treated as confidential and not disclosed to any person except with the consent of the individuals to whom the information relates, or otherwise in accordance with applicable law.

What happens if a group or organization does not meet the First Nations Inuit Health Branch (FNIHB) contribution agreement confidentiality requirements?

A plan will be developed by FNIHB and the First Nations organization to address the situation. If the problem cannot be resolved, the contribution agreement may be terminated.

Organizations are subject to either federal, provincial, or territorial laws regarding data protection. These include the *Personal Information Protection and Electronic Documents Act* and its provincial counterparts in Quebec, British Columbia, and Alberta. In Ontario, the *Health Information Protection Act* will take effect in November 2004. This Act ensures the privacy, confidentiality and security of personal health information that is collected, used and disclosed by individuals and organizations.

I have a contribution agreement for medical transportation and receive log sheets from drivers. Once we pay them, what are we supposed to do with the paper files?

As a recipient of a contribution agreement, you maintain ownership of all documents that you collect as part of the administration of the agreement. However you are required to provide reports as per the terms and conditions of the agreement and to keep all accounts, financial records and supporting documentation for a period of seven years unless you are advised otherwise, in case of audit. Under the confidentiality section of the agreement, you are required to handle personal information "in accordance with applicable law". This would include the disposal of confidential documentation. You are also bound by either federal, provincial or territorial privacy legislation.

My neighbour doesn't want to obtain health services for fear of personal information becoming known to everyone in the community. What should I tell my neighbour?

You should explain that employees must follow laws and policies that protect personal information they collect and use to provide benefits. Encourage your neighbour to talk with the staff processing the benefit requests to find out what privacy safeguards are in place and what options exist if they are not satisfied.