Health Canada Santé Canada

Non-Insured Health Benefits Program

Privacy Code

First Nations and Inuit Health Branch

Health Canada

Version 5: February 2005

Canada

NON-INSURED HEALTH BENEFITS (NIHB) PROGRAM

First Nations and Inuit Health Branch

Health Canada

PRIVACY CODE

Version 5 – February 2005

Ce document est aussi offert en français sous le titre :

CODE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS
Version 5 – février 2005

TABLE OF CONTENTS

INTRODUCTION

Health Canada's Non-Insured Health Benefits (NIHB) Program funds registered Indians and recognized Inuit with medically necessary health-related goods and services which supplement those provided by other provincial/territorial or private programs. These benefits include drugs, medical transportation, dental care, vision care, medical supplies and equipment, crisis intervention mental health counselling and provincial health care premiums, where applicable.

In order to process these benefits, the NIHB Program collects, uses, discloses and retains clients' personal information, and does so in accordance with the applicable federal laws and policies.

These include:

- the *Privacy Act*;
- "The *Privacy Act* gives Canadian citizens and people present in Canada the right to have access to information that is held about them by the federal government. The Act also protects against unauthorized disclosure of personal information. In addition, it strictly controls how the government will collect, use, store, disclose and dispose of any personal information"[1];
- the *Canadian Charter of Rights and Freedoms*;
- the *Access to Information Act*;
- the *Library and Archives of Canada Act*;
- Treasury Board Secretariat' (TBS) Privacy and Data Protection Policies;
- TBS' Government Security Policy; and
- the Health Canada Security Policy.

The NIHB Privacy Code reflects these *Acts* and policies and uses, as a guideline, the 10 principles set out in the Canadian Standards Association, *Model for the Protection of Personal Information* (*The CSA Model Code*). The *CSA Model Code*, which incorporates a higher benchmark of privacy protection, has been formally approved by the Standards Council of Canada as a National Standard of Canada.

[1]Info Source - Sources of Federal Government Information 2003-2004. Section F-*Privacy Act*.

The objectives of the NIHB Privacy Code are:

- to set out the NIHB Program's commitments that will ensure responsible and secure handling of personal information collected, used, disclosed and retained for program delivery, administration and management; and
- to foster transparency, accountability and increased awareness of the NIHB Program's privacy procedures and practices.

The NIHB Program is committed to protecting privacy and safeguarding the personal information in its possession. The NIHB Privacy Code represents a consistent approach to privacy and data protection for personal information collected, used, disclosed and retained by the Program. It ensures the Program's compliance with the *Privacy Act.*

Since the first version of the NIHB Privacy Code was released in May 2003, significant enhancements have been made to it. First Nations and Inuit and privacy experts have all made valuable suggestions for improvement. Some of the important changes made so far include providing more detailed information on NIHB privacy procedures and simplifying the definitions of terms.

The Non-Insured Health Benefits Privacy Code will be reviewed and revised on an ongoing basis as Federal Government privacy policies, legislation and/or program changes require. The Program would be pleased to receive stakeholder advice on the Code at any time. Comments received will be reviewed for possible incorporation into a later version of the Privacy Code. Summaries of the comments received will be posted on the NIHB Website at: www.hc-sc.gc.ca/fnihb/nihb

Suggestions and comments may be sent to:

E-mail: nihbprivacycode_comments@hc-sc.gc.ca

Mail: Attn: NIHB Privacy Code
First Nations and Inuit Health Branch
Non-Insured Health Benefits Directorate
Postal Locator 1919A, Room 1926B
Jeanne Mance Building, Tunney's Pasture
Ottawa, ON K1A 0K9

SCOPE OF THE NIHB PRIVACY CODE

The NIHB Privacy Code applies to all Health Canada employees administering and managing the NIHB Program. Organizations or groups administering NIHB benefits through contribution agreements must comply with privacy requirements found in the schedules and the confidentiality clauses that form part of the Terms and Condition of the agreement. Health care professionals must respect the privacy codes of their regulatory or licensing bodies.

The NIHB Privacy Code applies to all NIHB Program activities in order to provide eligible clients with non-insured health benefits including:

- prescription drugs (prescription and over-the-counter);
- dental services;
- vision care;
- medical supplies and equipment;
- medical transportation;
- short-term crisis intervention mental health counselling; and
- funding for provincial health care premiums, where applicable.

The NIHB Privacy Code:

- recognizes that the NIHB Program collects, uses, discloses, retains and disposes personal information to process benefit claims and to conduct program reviews. The objectives of the NIHB Program reviews are to improve accessibility of benefits, limit health risks, ensure responsible fiscal management and to contribute to improving the health status of First Nations and Inuit clients. This Code recognizes the need for compliance with privacy laws such as the *Privacy Act* and contains policies and procedures that ensure this through clearly defined terms and conditions;
- has been established with the view that privacy and good health are mutually supportive goals and that the individual right to privacy does not need to be compromised in order to achieve better health outcomes; and
- has been developed by the NIHB Program, with input from clients and stakeholders (providers and prescribers) to protect the privacy of NIHB clients and to ensure the confidentiality and security of their personal information.

1. NIHB PRIVACY CODE PRINCIPLES

1.1 Principle 1 – Accountability

Deputy Ministers and Heads of Agencies are responsible for ensuring that their organizations comply with *Access to Information* and *Privacy Acts*. In addition, the President of the Treasury Board co-ordinates the administration of the Acts by preparing and distributing policies and guidelines to help institutions interpret the laws.

Health Canada employees administering and managing the NIHB Program will be held responsible for ensuring the private and secure handling of personal information collected, used, disclosed, retained and disposed by the Program.

Criteria for the uses of personal information are to be respected; any breach of these criteria by staff may result in disciplinary action, which may include suspension or dismissal.

In the case of contractors or those organizations administering NIHB, a breach may result in terminating the contract or the contribution agreement.

1.1.1 Health Canada

1.1.1.1 Responsibilities of Managers and Employees

Managers of the NIHB Program have a duty to uphold Health Canada's reputation for integrity, honesty and ethical and legal conduct according to privacy legislation and the Treasury Board of Canada's Government Security Policy.

This means:

- to create and maintain a work environment that encourages the respect of privacy and ethical behaviour;
- to set an example by complying with the NIHB Privacy Code and Health Canada policies and guidelines at all times;
- to ensure their employees review the NIHB Privacy Code annually or more frequently should changes occur;
- to ensure that all employees comply with procedures that are already in place for the private and secure handling of client personal information;

- to ensure that all employees know, understand and comply with the NIHB Privacy Code at all times;
- to foster an environment of open communication in which issues may be raised and discussed without fear of reprisal; and
- to report to their immediate supervisor, any apparent violation of the Privacy Principles or breach of government policies.

Should managers have concerns with the conduct of their staff in relations to the Privacy Code, it is their responsibility to address these concerns using appropriate action such as providing the individual with training or by restricting access to personal information.

Health Canada employees with the NIHB Program are responsible for the confidential and secure handling of the personal information collected, used, disclosed, retained and disposed of while administering the Program.

This means:

- to comply with procedures that are already in place for the confidentiality and secure handling of client personal information;
- to know, understand and comply with the NIHB Privacy Code at all times; and
- to review the NIHB Privacy Code annually or more frequently should changes occur.

1.1.2 Contracts or Contribution Agreements

The NIHB Program is responsible for ensuring that a level of privacy protection comparable to the *Privacy Act* and policies to which the Program is subject, is in place for personal information disclosed or transferred to a third party such as a contract for claims processing or a First Nations or Inuit organization that provides NIHB benefits under the terms and conditions of a signed contribution agreement.

Contracts and Contribution agreements contain standard clauses dealing with the confidentiality and privacy of personal information, which are to form part of the Terms and Conditions.

Private claims processors are also subject to industry standards for transmitting data between themselves and the providers to ensure the security and privacy of personal information. Most of these organizations are also subject to federal, provincial or territorial data protection legislation, including the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). PIPEDA applies to all provinces and territories except where the Governor in Council has issued exemption orders (i.e., Quebec, British Columbia and Alberta). Business organizations in all provinces and territories must ensure their compliance with the applicable federal or provincial law that deals with protecting the collection, use and disclosure of personal information within that province.

1.1.3 Health Care Professionals

Health care professionals who are employed by Health Canada must meet the confidentiality requirements of the NIHB Program, in addition to their professional ethical obligations. Their professional code of ethics which is established by their respective regulatory bodies encompasses privacy and confidentiality. Any breach of these ethics may result in the regulatory body requiring the health care professional to take training, suspending or withdrawing his or her licence.

1.2 Principle 2 – Identifying Purposes

The NIHB Program collects, uses, discloses, retains and disposes of personal information for the following purposes:

- to provide funding for non-insured health benefits for eligible clients; and
- to conduct Program reviews aimed at improving health care benefits, services, therapy or delivery, and ensuring the long-term sustainability of the NIHB Program.

1.2.1 Provide Funding for Non-Insured Health Benefits

The process to provide funding for non-insured health benefits requires reviewing personal information in order to:

- approve benefit funding requests;
- process payment of claims received from providers; and
- audit and verify claims and payments.

1.2.1.1 Approve Benefit Requests

Personal information is collected, used, retained and disclosed for assessing criteria that need to be met before benefit claims can be approved and to allow health care providers to deliver benefits or services to clients.

The criteria are:

- *Client eligibility for the NIHB Program:* This is verified either online or by telephone using Health Canada's Status Verification System, or by calling a NIHB regional office and providing the required client information for the Program to verify.
- *Benefit eligibility:* Benefit lists and policies have been established for each benefit area to ensure that those benefits which the Program is mandated to provide are funded consistently. Assessing benefit eligibility begins with comparing the benefit/claim request against the relevant benefit policies and lists. In some cases, benefits require prior approval, as in the case of a limited use drug benefit that has established criteria that must be met before funding is approved. Prior approval is also required for most benefits that are not on the NIHB benefit lists, which may be considered on an exception basis. In cases where a benefit request has been denied, clients can appeal the Program's decision. This appeal process is considered part of the benefit eligibility approval process.
- *Absence of other-third party coverage:* The NIHB Program has been set up to fund non-insured health benefits to clients when other federal, provincial, territorial or private coverage does not exist. Where other third-party coverage does exist, the NIHB Program will fund any outstanding balances for eligible benefits.

1.2.1.2 Processing Payment Claims from Providers

Generally, clients of the NIHB Program are not required to pay up front for benefits received. Once the provider has confirmed that the benefit approval criteria have been satisfied, he or she may provide the benefit or service to the client and then bill the Program directly.

Claim-specific details, including the personal information of the client involved, must be submitted by the provider to the NIHB Program within one year from the date of service to facilitate payment. In the case of drug benefits, the process for submitting the claim data electronically for approval and for payment are often completed simultaneously. Dental benefits may be claimed electronically also for those using CDAnet. In the case of other benefits, such as medical supplies and equipment, the provider must submit benefit requests to the claims processor or regional office in paper format for processing.

1.2.1.3 Auditing and Verifying Claims and/or Payments

First Canadian Health Management Corporation Inc. (FCH) is the claims processor for drugs, medical supplies and equipment (MS&E) and dental benefits on behalf of the NIHB Program. FCH is required to conduct on-site audit and claims verification activities by reviewing claims submitted under the NIHB Program.

First Nations and Inuit Health Branch (FNIHB) regional offices are responsible for the adjudication, audit and claims verification of medical transportation, vision and mental health crisis intervention benefits provided within their region.

These activities are conducted in compliance with:

- accountability requirements for using public funds in accordance with the *Financial Administration Act, Part VI-Public Accounts*;
- the *Privacy Act*; and
- the NIHB Program's terms and conditions outlined in the provider agreements, provider information kits, Program newsletters and benefit frameworks.

The audit activities are based on generally accepted industry practices and accounting principles. Audits are carried out to identify potential billing irregularities; to ensure that claims are paid in accordance with Program billing requirements; to ensure that services paid for were received by eligible NIHB clients; and to ensure that providers have retained appropriate documentation that supports each claim.

As part of the audit process, the auditor may contact the prescriber to verify clients and prescriptions or contact clients to substantiate receipt of the benefit or service and the specific claim information.

In order to complete the audit, the auditor must conduct an assessment of the claims paid by the NIHB Program to ensure adequate data are available by scanning all the relevant information or the paid claims which are under review.

All personal information obtained for claims verification is maintained in accordance with the *Privacy Act*.

1.2.2 Conducting Program Reviews

As outlined in the Scope of the NIHB Privacy Code, the NIHB Program collects, uses and discloses personal information to conduct Program reviews. These review activities are critical for:

- improving health care benefits;
- limiting health risks;
- ensuring responsible fiscal management; and
- contributing to improving the health status of First Nations and Inuit clients.

Program reviews include:

- statistical reporting; and
- Drug Utilization Evaluations (DUEs).

Program reviews, such as statistical reporting, use anonymized or non-identifiable aggregate data. The DUEs use identifiable data. However, it is important to clarify that identifiable personal information is not required for the actual review activity, but rather it may be required in very limited circumstances when client or provider-level interventions are required when a client may be at risk. More details are provided in the NIHB Policy section entitled "The Use of Personal Information in Program Reviews" (section 2.1)

1.3 Principle 3 – Consent

1.3.1 Individual Privacy - Consent

1.3.1.1 Collection of personal information - Consent

Under the *Privacy Act*, there is no consent requirement for the collection of personal information. However there is an obligation to inform concerned individuals of the reasons for the collection of their personal information (section 5) of the *Privacy Act*.

1.3.1.2 Use and Disclosure of personal information - Consent

Express (written or verbal) consent for the use and disclosure of the personal information is required:

- as described in sections 7 and 8(1) of the *Privacy Act*. However, if the use or disclosure of the personal information is for the purpose for which it was collected, for a consistent purpose, or for any of the purposes set out under section 8(2), consent is not required.

1.3.2 Informing Clients

As mentioned previously, under the *Privacy Act*, institutions must inform the concerned individuals about the reasons for collecting and using their personal information. The NIHB Program communicates this information to clients and stakeholders through a number of mechanisms including:

- the Government of Canada's Info Source;
- the NIHB Personal Information Banks SCan PPU 016 and SCan PPU 017;
- the NIHB Privacy Code;
- the NIHB Privacy Impact Assessment;
- the NIHB Program and privacy information found on the Health Canada Web site;
- regional office staff who are available to respond to questions and provide information to clients; and
- the NIHB toll-free number: 1-800-259-5611.

The NIHB Program has also committed to undertake a communication campaign every five years to remind clients about the collection, use and disclosure of personal information under the Program.

1.4 Principle 4 – Limiting Collection

Personal information is primarily collected indirectly for the NIHB Program by physicians, nurses, pharmacists, optometrists/opticians, dentists/denturists, registered psychologists/social workers, medical supply and equipment and medical transportation providers in accordance with section 5(1) of the *Privacy Act*.

The NIHB Program must limit its collection of personal information for the purpose described in Principle 2 of this Code (i.e., to provide funding for non-insured health benefits and to conduct program reviews). The collection is limited to the individual claims submitted by the provider (transaction-based). Only the minimum amount of information required to assess the need for a benefit is collected. This limited collection complies with section 4 of the *Privacy Act* in that the information being collected is directly related to NIHB Program activity.

In cases where benefit exceptions are being considered for funding, additional client information may be collected and shared between the treating health care professional and NIHB's health care professionals, as required, to verify client need.[2]

[2]The NIHB Program employs or contracts health care professionals who are responsible for reviewing and approving exceptions and prior approvals. Information plays a critical role in providing evidence to support a specific need and ensuring the request is assessed according to evidence-based standards of care. These health care professionals have to comply with the NIHB Privacy Code as well as privacy requirements set out by their regulatory body.

The table below outlines situations with the type of information that is collected by the NIHB Program.

TABLE 1

Information that is collected for NIHB benefit requests that <u>do not</u> require Prior Approval	**Information that is collected for NIHB benefit requests that require Prior Approval or when a benefit is considered an exception**
• Client's Name • Date of Birth • Identification Number • Prescription/Benefit Request Details	• Client's Name • Date of Birth • Identification Number • Address ✣ • Phone Number ✣ • Prescription or Benefit Request Details The following additional information may also be required to approve the benefit: • Past and current treatment • Laboratory results • X-rays (dental) • Information on a client's medical and/or dental condition • Existing information when needed to support the benefit request • Other personal information when needed to support the benefit request

✣ Not always required; used only if information is missing.

1.5 Principle 5 – Limiting Use, Disclosure and Retention

The NIHB Program must use and disclose personal information only for the purposes outlined in Principle 2 of this Privacy Code, unless it is otherwise required or authorized by law. This is in compliance with sections 7 and 8 of the *Privacy Act*.

The NIHB Program limits the use, disclosure and retention of personal information by restricting access to client information on a need-to-know basis. It is worth noting that, in the majority of cases, a client's personal information is received from providers/professionals rather than the Program disclosing to providers/professionals. The Program limits the disclosure of information back to the provider to only what is required to process the benefit request.

TABLE 2

Who Accesses	For what purpose(s) and under what conditions
NIHB • Staff • Contractors • Consultants	As outlined in Principle 2: Use and disclose personal information: • to process claims; • to review benefit requests; and • to conduct Program reviews. NIHB staff or its contractors (i.e., claims processor). Use and disclose anonymized data: • to improve health care benefits, services, therapy or delivery for clients; and • to ensure the long-term sustainability of the NIHB Program.
Program Health Care Professionals/Providers	Eligible health care professionals and providers share personal information with the NIHB Program: • to support a benefit request in its day-to-day operation. When clients at risk or inappropriate use are identified, personal information is disclosed to the client's provider only when express consent has been provided to supplement the provider's professional judgement.
Professional Regulatory and Licensing Bodies	Client's personal information may be disclosed by the NIHB Program to professional regulatory and licensing bodies as evidence to support an investigation of health care providers who have been seen by the client.
First Nations and Inuit organizations under contribution agreements to administer non-insured health benefits	As outlined in Principle 2, First Nations and Inuit organizations administering benefits under Contribution Agreements will use and disclose personal information: • to provide funding of benefits; and • to conduct benefit reviews to monitor the delivery of those benefits, provided the body requesting the information does so pursuant to lawful authority.
Federal/Provincial/ Territorial or other third-party health insurance plans	Where clients have coverage either through provincial or territorial governments or private health plans that provide only partial coverage of a particular benefit, the NIHB Program may use and disclose a client's personal information to coordinate benefit coverage in order to provide further coverage.

1.5.1 New Purposes and Uses of Personal Information

If personal information needs to be used for a new purpose, the NIHB Program will amend the NIHB Privacy Code, the Privacy Impact Assessment and required policies. The Program will undertake a communication strategy to inform clients as required. For more information, see NIHB's Privacy Change Management section, section 3.1, of this document.

If the Program requires personal information for a new purpose as mentioned above, express consent will be required. The Program will specify to the client what information is needed and the purpose for which it will be used.

1.5.2 Retention and Disposal of Personal Information

Information shall be retained and disposed of according to the Records Retention and Disposal of Personal Information policy of the Government of Canada, section 6(1) of the *Privacy Act*, section 12 of the Regulations and *the Library and Archives of Canada Act*. Health Canada has guidelines and procedures in place concerning the retention and disposal of personal information. Health Canada employees can access a policy icon through an internal database on their Lotus Notes workspace. This icon links to Health Canada policies on Information Management.

The Acts and policies mentioned above pertain to all personal information stored by the NIHB Program in the following systems:

- Status Verification System (SVS) electronic records;
- Health Information and Claims Processing System (HICPS) electronic records;
- Medical Transportation Records System (MTRS) electronic records; and
- Vision Care Systems (Regional) electronic records.

1.6 Principle 6 – Accuracy

According to the *Privacy Act*, section 6(2), all reasonable steps will be taken to ensure that personal information collected by the NIHB Program is accurate and complete. Personal information collected for processing benefit requests is not routinely updated, unless required to ensure ongoing delivery of a specific benefit or service for claims processing.

Updating the client eligibility lists on the SVS is completed when Indian and Northern Affairs Canada, the Governments of Nunavut and Northwest Territories and the Labrador Inuit Association regularly provide the NIHB Program with updated information. The NIHB Program does not provide these groups with any personal information. The personal information flows only into the NIHB Program.

In order to ensure the accuracy of client information collected, the NIHB Program requires clients to identify themselves by providing three pieces of information before accessing benefits. This information includes: name, date of birth and identification number.

Each of the databases that store NIHB claims information contains mandatory information fields that must be completed before a claim can be processed and/or approved. If the fields are not completed properly, the claim will not be processed. This is to ensure the accuracy of the information that is being collected for each client.

1.7 Principle 7 – Safeguards

In accordance with the *Privacy Act* and Regulations, the Government Security Policy, the Privacy and Data Protection Policy, the Operational Security Standard and the *Library and Archives of Canada Act*, the NIHB Program will take every reasonable precaution to protect the security and confidentiality of personal information it collects, uses, discloses, retains and disposes and by ensuring that organizational, physical and technological safeguards and controls have been put in place and are maintained.

1.7.1 Sensitivity of the Information

Personal information collected by NIHB for claims processing is classified as "Designated Information" and must be marked as "Protected" (upper right corner) according to the Government Security Policy.

Documents containing medical information pertaining to individuals indicate "Medical - Confidential" and are handled only on a "need-to-know" basis.

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

Health Canada employees administering and managing the NIHB Program must not remove protected materials from secure areas.

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

1.7.2 Organizational Safeguards

Employee Security: All employees and contractors must hold an enhanced reliability status security clearance as a minimum requirement for handling personal information in the day-to-day processing of benefits and administration of the NIHB Program. An enhanced reliability status security clearance will allow them access to designated information.

Authority for system access: The Program manager is responsible for identifying and authorizing those who require access to NIHB Program data systems. They are also responsible for maintaining control records for sensitive material and items such as keys, codes, combinations, identification badges and individual system passwords.

Withdrawal of access: This takes place when employees conclude their employment, when their duties no longer require them to have access, or when inappropriate use and disclosure is identified. When access to the NIHB Program data system is withdrawn, the employee's user number to enter a data system is no longer valid.

Staff training: Health Canada employees administering and managing the NIHB Program and contractors are given training on the secure handling of personal information. Employees receive training for their specific responsibilities, a critical part of which are the procedures that are used in NIHB units (regional or headquarters). For further information, please refer to NIHB's Privacy Training Policy section, section 2.4, of this document.

1.7.3 Physical Safeguards

Several steps have been taken to secure the physical work environment in which personal information is stored. These include:

Identification Cards: Health Canada employees administering and managing the NIHB Program are given identification cards which must be displayed at all times. These cards act as an effective access control, to avoid admitting unauthorized personnel into FNIHB, NIHB or Health Canada buildings. Security signs are posted, as required, in Health Canada work locations.

Keys, lock and safe combinations and entry code numbers: These are issued only to authorized persons with an established need for access in order to avoid inappropriate access to any personal information.

Office security: All FNIHB and NIHB offices are required to ensure confidentiality of personal information by using enclosed offices and secure data-sharing equipment, to avoid exposure of personal information to unauthorized individuals.

Withdrawal of access: All employees must return their identification card when their employment is terminated. Consequently, they no longer have access to Health Canada offices. All system access is withdrawn at the same time.

Random inspections: Random, unannounced inspections of offices and work-sites may be carried out to ensure Departmental information and assets are adequately protected. Breaches of security detected during an inspection are brought to the attention of the director or manager responsible for the area and the Branch Security Coordinator.

Loss or theft: The loss or theft of personal information must be reported to the manager or designated custodian of the affected information and to the Health, Safety and Security Division or the Branch Security Coordinator. A Report of Loss or Theft Form (NHW-518 1-91) must be completed, including the police occurrence report number. When the investigation is completed, the police will contact the responsible manager to identify any recovered information.

For additional information, refer to the Treasury Board Index - Physical Security Standards, Organization and Administration Standards, Information Technology Security Standards at: www.tbs-sct.gc.ca/index_e.asp

1.7.4 Technological Safeguards

Password protection: Access to a system (HICPS, SVS, MTRS, Vision System) is protected by an individual password. Access is limited only to those health professionals, authorized employees and/or administrators who require access.

Central coordination of access: The NIHB manager is responsible for authorizing staff access to only those benefit databases relevant to their work assignment. All passwords for HICPS, MTRS and SVS are assigned centrally from the NIHB Directorate, Operational Support, managers must request access for staff in writing using prescribed forms.

Regional access controls: Vision systems are regionally managed, with the respective regional manager responsible for determining who requires access and assigning individual passwords relevant to assigned work. This ensures that only those who require access are given passwords.

For further information regarding the NIHB Procedure for Authorizing Access to HICPS, MTRS, SVS and Vision systems, please refer to the Privacy Procedure section, section 3, of this document.

For further information on the standards that define baseline security requirements that federal departments must fulfill to ensure the security of information and information technology (IT) assets under their control (e.g., laptops), please refer to the Management of Information Technology Security (MITS) section of the Operational Security Standard Policy.

Encryption: According to the Health Canada Government Security Policy, Protected Information may be sent by fax or e-email, unless a Threat Risk Assessment (TRA) indicates the requirements for greater safeguards such as encryption. Information designated as Protected A and Protected B information does not require encryption when transmitted internally on the Health Canada Network. (For a definition of Protected A, Protected B and Protected C information, refer to Appendix I, under "Designated Information").

The Management of Information Technology Security (Section 16.4.4 Cryptography) states: "Departments must use encryption or other safeguards endorsed or approved by the Communications Security Establishment (CSE) to protect the electronic communication of classified and Protected C information. Departments should encrypt Protected A and Protected B information, when supported by a Threat and Risk Assessment. However, departments must encrypt protected B information before transmitting it across the Internet or a wireless network."

Information designated as Protected A and Protected B transmitted externally (Internet) must be encrypted.

All Protected C information must be encrypted for both internal and external (Internet) transmission. Due to the high sensitivity requirements, the strength of the encryption system, in unison with other safeguards, is important.

1.7.5 Contractors and Consultants

All contracts with health professionals and providers include clauses stating they are subject to the same procedures and standards as Health Canada employees. According to the Personnel Security Standards in the Government Security Policy, contractors must obtain an enhanced reliability status before their involvement with the NIHB Program. This will allow them to access designated information.

Contractors/Consultants/Providers to the Program are provided only with the information they require to complete contracted responsibilities; e.g., reviewing a vision request. Should the consultant require further information, Health Canada employees administering and managing the NIHB Program would provide only that information. They are bound by the confidentiality clause in their contract.

An example of a standard clause is:

"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."

1.8 Principle 8 – Openness about Policies and Practices

The NIHB Program will make the NIHB Privacy Code and its related policies and procedures available to First Nations and Inuit clients, providers, health care professionals and stakeholders. This also includes, but is not limited to: privacy impact assessments, employee privacy training manuals and privacy provisions in third-party contracts.

The NIHB Privacy Code and NIHB Program information are available at the following Internet address: www.hc-sc.gc.ca/fnihb/nihb or on request from FNIHB regional offices.

1.9 Principle 9 – Individual Access

Under the Privacy Act section 12(1) every individual who is a Canadian citizen or a permanent resident within the meaning of the *Immigration and Refugee Protection Act* has a right of access to personal information about themselves that is under the control of a government institution.

According to sections 12-17 of the Act and the completed request section of the TBS Privacy and Data Protection Policy on right to access, the NIHB Program will inform an individual about the existence of his or her personal information and will give an individual the right to access personal information about himself or herself included in the NIHB Personal Information Banks HCan PPU 016 and HCan PPU 017. An individual also has a right to challenge the accuracy and completeness of the information and to have it amended under appropriate circumstances.

Health Canada's Access to Information and Privacy (ATIP) office is mandated to coordinate, review and evaluate privacy requests for Health Canada including the Non-Insured Health Benefits Program. This is in accordance with the Department of Health *Privacy Act* Designation Order. Each federal government department or agency has an Access to Information and Privacy Coordinator. The Coordinators' offices are staffed by people who can answer questions and help clients access their personal information under the *Privacy Act* using a Personal Information Request Form. Additional information on this issue can be found in section 3.4 entitled Individual Access and Correction of Personal Information, later in this document

According to TBS Privacy and Data Protection policies, namely Assistance to Individuals in Exercising Their Rights and Right of Access to Personal Information, government institutions should also provide individuals with informal access to their personal information whenever possible.

1.10 Principle 10 – Challenging Compliance

According to the TBS, Deputy Ministers and Heads of Agencies are responsible for ensuring that their organizations comply with *Access to Information* and *Privacy Acts*. In addition, the President of the Treasury Board co-ordinates the administration of the Acts by preparing and distributing policies and guidelines to help institutions interpret the laws.

Clients should address their concerns on the NIHB Program's compliance with the Privacy Code by contacting Health Canada's Access to Information and Privacy (ATIP) office. Additional information on this issue can be found in section 3.5 entitled Privacy Complaints and Inquiries, later in this document.

The Minister of Health has designated Health Canada's Privacy Coordinator as having the power to make representations on behalf of an individual or head of the government institution to the Privacy Commissioner relevant to an investigation on a privacy complaint. Please refer to section 33 of the *Privacy Act*.

The *Privacy Act,* sections 29-35 outlines the scope, powers and procedures to be followed by the Privacy Commissioner in receiving and investigating complaints by individuals regarding the access, collection, use, disclosure, retention and disposal of their personal information held by a government institution.

2. PRIVACY POLICIES

2.1 The Use of Personal Information in Program Reviews

Program reviews, such as statistical reporting and promotional/educational strategies, will only review:

- anonymized information, which has been stripped of identifiable details (name, date of birth, identification number, any geographical information); and
- non-identifiable aggregate data, which are summarized at a level where it can be reasonably assured that the information will not identify an individual.

Program reviews, such as prospective and retrospective DUE, involve the review of:

- non-identifiable aggregate data, which are summarized at a level where it can be reasonably assured that the information will not identify an individual;
- identifiable information such as individual drug benefit history. This component identifies clients that may be at risk based on medication quantities and the clinical review by an NIHB pharmacist; and
- identifiable information is not shared outside the day to day claims processing and administration activities without the consent of the client, or as required by law.

2.2 NIHB Drug Utilization Evaluation (DUE)

Optimal drug use means the right drug to the right client in the right dose at the right time. FNIHB recognizes that, in order to address medication issues, and improve health outcomes, the branch must work with First Nations and Inuit communities, organizations and stakeholders to develop and implement strategies around awareness, promotion, prevention and treatment.

This includes:

- sharing of aggregate FNIHB information to identify trends, and issues;
- engaging FN/I communities, organizations and stakeholders in working together on approaches and materials (toolkit); and
- working with prescribers, pharmacists and clients to address specific clients at risk.

Of urgency are a small number of clients who may be at risk as a result of their medication use. This section sets out the approach NIHB will use to ensure that client's prescriber(s) and pharmacist(s) have the information they require to support their professional judgement in ensuring optimal medication use.

The NIHB Program is not a regulatory body or a health care provider, but a program which funds drug benefits based on the professional judgement of health care providers who prescribe and dispense medications. NIHB possesses important information that prescribers and pharmacists may not have.

2.2.1 Identification of At-Risk Clients

NIHB, like other drug benefit programs, identifies trends in medication use on both a population and client level, using established clinical review processes. NIHB performs prospective DUE which involves sending electronic messages to pharmacists, at the time of dispensing, to alert to such potential incidences as drug to drug interaction or duplicate therapy. These messages supplement the professional judgement of the pharmacist.

The program also undertakes retrospective DUE, which is a quarterly review of client level drug utilization. As a first step in retrospective DUE appropriate medication use quantities are established using expert physician, pharmacist and DUE Advisory Committee advice. Every three months a copy of the HICPS database is generated with all identifiable information removed. This database is then queried using the established medication quantities to produce anonymized files of client medication histories. These files are then reviewed by an NIHB pharmacist to determine if the client's medication use is placing them at risk. The file identified as being at risk is then relinked to the HICPS database and the client identified. The NIHB pharmacist will then contact the client's pharmacist(s) and request that the client contact the NIHB Program at the time of the next dispense. No drug benefit information will be provided until client consent is obtained.

2.2.2 Assisting Clients, Prescribers and Pharmacists

In order to assist at risk clients, the NIHB Program must share information with the client's prescriber(s)/pharmacist(s). Only then can the prescriber and the dispensing pharmacist review the relevant client medication history and make a decision based on professional judgment, to continue to prescribe or dispense such medication.

2.2.3 Limiting Client Consent

NIHB is committed to protecting client privacy. This means that the sharing of the client's information with the prescriber(s) and pharmacist(s) cannot occur until the client has provided consent. While the number of clients at risk is small, the consequences of inappropriate drug therapy can be serious.

Those clients who have already signed a consent form will not need to provide any further consent. Those clients who have not provided consent will be asked, by the dispensing pharmacist, to telephone the NIHB toll-free number to talk with an NIHB pharmacist who will explain that:

- The NIHB Program will not share information without client consent.
- The consent limits the NIHB Program to share only relevant drug benefit history with their pharmacist(s) or prescriber(s).
- This will result in the pharmacist's decision to dispense the drug or not based on this information.
- The client drug benefit history is critical in assisting the pharmacist to safely provide medications and identify possible interactions or duplicate prescriptions.
- The types of information that may be shared are: names of drugs, quantities, dates of prescriptions, names of prescribers and other pharmacies.
- The client has a right to refuse to provide consent.

The client can then ask questions, and make a decision to provide consent or not. If the client does not provide consent to share their information, no information can be provided to their pharmacist. It will then be up to the pharmacist to dispense the medication or not.

2.2.4 Implementing Patient Safety Plans, and Treatment Interventions

If consent has been provided, the NIHB pharmacist will contact the dispensing pharmacist and share only the relevant drug use history for the medication being requested. It will then be up to the pharmacist to decide whether or not to dispense the medication.

Once the information is shared, the client, physician and/or pharmacist can address the client's medication and treatment needs, which may range from putting in place a medication management plan to addictions and mental health treatment as part of a larger set of issues.

2.2.5 Reviewing Procedures

NIHB will review the effectiveness of these procedures on a regular basis. The NIHB Program anticipates claims processing systems changes will be put in place which will further streamline the process for both the client and pharmacists. As changes are identified updates and advice will be sought through mechanisms such as the DUE Advisory Committee, discussions with First Nations and Inuit organizations and prescriber and pharmacist organizations.

2.3 NIHB Consent Policy

NIHB will not require express consent for day-to-day processing activities and administration of the Program. The NIHB Program requires express consent only when a patient is identified as being at-risk or if inappropriate use of the system is a concern and requires the Program to disclose personal information to a service provider.

2.3.1 Informing Clients and Stakeholders

The NIHB Program communicates information on the collection, use, disclosure, retention and disposal of personal information, to clients and stakeholders through a number of mechanisms including: the NIHB Personal Information Banks HCan PPU 016 and HCan PPU 017; the NIHB Privacy Code; the NIHB Privacy Impact Assessment; the Health Canada Website with NIHB Program and privacy information; regional office staff who are available to respond to questions and provide information to clients; and through the NIHB toll-free contact number at 1-800-259-5611. The NIHB Program has also committed to undertake a communication campaign every five years to remind clients about the collection, use and disclosure of personal information.

2.3.2 Withdrawal of Written Consent

If a client wishes to withdraw his or her written consent, he or she must clearly state this in a letter to Health Canada, addressed to the NIHB Program.

This letter must include:

- client's legal name;
- date of birth;
- identification number;
- address;

- telephone number (optional);
- signature of client;
- date of the letter; and
- Statement of the client's request to withdraw his or her written express consent.

The client will receive written confirmation from the NIHB Program that their written express consent has been withdrawn. The consent form will be retained by Health Canada and will be disposed of according to the records and retention schedules of the federal government.

The mailing address for the NIHB Program is:

First Nations and Inuit Health Branch
Non-Insured Health Benefits Directorate
Postal Locator 1919A, Room 1917A
Jeanne Mance Building, Tunney's Pasture
Ottawa, ON K1A OK9

If a client has withdrawn his or her written consent, he or she will continue to receive benefits for which he or she is eligible subject to Program policy.

2.4 NIHB Privacy Training Policy

2.4.1 The NIHB Privacy Code

All Health Canada employees administering and managing the NIHB Program are required to review and acknowledge their compliance with the NIHB Privacy Code before assuming their duties.

Managers will review the NIHB Privacy Code with new employees immediately upon appointment. Privacy training will be arranged as soon as possible.

Employees shall be required to review the NIHB Privacy Code annually or more frequently, if changes occur.

2.4.2 The NIHB On-Line Privacy Training Module

The NIHB Program has developed the NIHB On-Line Privacy Training Module.

This training module includes:

- privacy training for all Health Canada employees administering and managing the NIHB Program; and
- privacy information for communities administering NIHB under contribution agreements.

This module is available on the Internet or on a CD-ROM. A copy of the CD-ROM has been made available to NIHB managers and First Nations and Inuit communities.

The on-line version is available on the NIHB Website at:
www.hc-sc.gc.ca/fnihb/nihb

2.5 Uses of Personal Information in Research Policy

There may be instances where Health Canada uses anonymized data for research purposes. In such cases Health Canada's Research Ethics Board (REB) reviews and approves any proposed research or study. It is in place to ensure that "all research involving human subjects carried out by Health Canada, or by investigators associated with Health Canada, meets the highest scientific and ethical standards" and that "safeguards are developed which provide the greatest protection to participants who serve as research subjects."

The REB is an independent, decision-making board that reports to the Chief Scientist of Health Canada. The REB is guided by the ethical principles found in the Tri-Council Policy Statement, Ethical Conduct for Research Involving Humans. The Board is concerned solely with protecting human research subjects. It will provide the Department with an independent review mechanism and fulfil an educational function for Health Canada managers and researchers. The REB also has to comply with relevant privacy legislation.

3. PRIVACY PROCEDURES

3.1 Privacy Change Management

The NIHB Program's commitment to privacy involves the ongoing monitoring of Program activities to ensure that any changes are in accordance with the NIHB Privacy Code and are clearly reflected in the NIHB Privacy Impact Assessment (PIA). It is understood that both these documents are based on the *Privacy Act*, the *Canadian Charter of Rights and Freedoms*, the *Access to Information Act*, as well as TBS policies and guidelines including, the Privacy and Data Protection Policy, the Government Security Policy and the Health Canada Security Policy. The NIHB Privacy Code addresses the requirements of these Acts and policies.

The NIHB Privacy Code and PIA form the basis of the privacy documents for the NIHB Program. Any changes to the NIHB Program will be reviewed in terms of their impact on privacy requirements as outlined in the NIHB Privacy Code. Once this impact is determined, the PIA will be revised to include the changes as well as any relevant Program policy documents.

The NIHB Program is committed to ensuring that clients continue to be aware of NIHB privacy commitments. As part of this commitment, every five years, specific communication activities will be undertaken to remind clients about the collection, use, disclosure retention and disposal of personal information as well as any changes to the NIHB Program that may have occurred.

If the Program requires personal information for uses other than what is described in Principle 2 of this Code, express consent will be required from the client, which will specify what personal information is needed and the purpose for which the information will be used.

3.2 Authorizing Access to HICPS, MTRS, SVS and Vision Systems

- Access to the system (HICPS and SVS) is protected by individual passwords and the access is limited to health professionals and/or administrators.
- NIHB managers are responsible for approving staff access to only those benefit databases relevant to their work assignment.
- The HICPS system maintains the drug, medical supplies and equipment and dental benefit history. Individual passwords are assigned and/or coordinated by the Director of Operational Support at the NIHB Directorate. Passwords must be requested by the individual's manager, and only for those systems needed to perform his or her duties.

- The medical transportation data is tracked by the regions through the Medical Transportation Record System (MTRS). Access is controlled by assigning individual passwords for access through the Director of Operational Support at the NIHB Directorate.
- Vision benefits are tracked in regional systems where individual passwords assigned by managers restrict access to information.

3.3 Protecting Privacy of NIHB Reports and Public-use Tables

NIHB protects against the possibility of any form of identification or disclosure by carefully reviewing statistical material intended for use external to the NIHB Program, and modifying the information as necessary to prevent any identification.

This could include:

- deleting table data that contain information on fewer than five people (and other tables as necessary to prevent identification based on row and column totals);
- combining categories;
- random rounding of numbers, or replacing numbers with ranges;
- suppressing statistical measures (means, variances, etc.) based on small numbers of people, if required to prevent identification;
- reviewing charts and graphs to ensure that they do not display information on identifiable individuals;
- attention to combinations of "indirect identifiers" - such as community and age group - that might permit either identity or attribute disclosure; and
- attention to the possibility that tables might allow identification of communities and providers, not just individuals.

3.4 Individual Access and Correction of Personal Information

3.4.1 Requesting Access to personal information

The NIHB employee who receives a request from an individual wishing to access his or her personal information held by the NIHB Program, will inform the individual that Health Canada's Access to Information and Privacy Coordinator is mandated to coordinate, review and evaluate privacy requests on the NIHB Program.

Employees with the NIHB Program will explain the procedure on how to apply for information under the *Privacy Act* described in the Government of Canada's Info-Source as follows:

Should an individual wish to make a formal request under the *Privacy Act*, they must:

- obtain a form entitled "Personal Information Request Form" (Refer to Appendix III or Internet site www.tbs-sct.gc.ca/tbsf-fsct_e.html);
- fill out the form and identify themselves in such a way that the government can verify who they are to ensure that it is the individual themself, and not someone else, asking for their information. The more precise the information provided, the faster the request can be answered; and
- send the form to Health Canada's Privacy Coordinator at the following address:

  Health Canada
  Access to Information and Privacy Coordinator
  Postal Locator 1912C1, 12th Floor
  Jeanne Mance Building, Tunney's Pasture
  Ottawa, ON K1A 0K9

There is no charge to apply for information under the *Privacy Act.* The requested information, in compliance with section 14 of the *Privacy Act*, will be provided within 30 days after the request is received with an explanation of any abbreviations or codes. As soon as the information is available, the individual will be contacted in writing.

Employees may provide assistance to clients by listing the type of information that will assist Health Canada's Access to Information and Privacy Coordinator in the processing of the request. They may also provide assistance to clients in filling out the form. These steps will ensure that information specific to the NIHB Program will be properly identified hence facilitate the processing of the request.

3.4.2 Requesting a correction to personal information

If a client believes his or her personal information held by a federal institution is inaccurate or misleading, the client can ask to have it corrected. Even if the department or agency does not agree to change this information, it must make a note that the client has asked for the change and attach it to the file.

3.5 Privacy Complaints and Inquiries

When an inquiry or complaint is received at any office of the FNIHB regarding complaints on privacy compliance concerning the NIHB Program, the individual will be referred to Health Canada's Access to Information and Privacy (ATIP) Office. Health Canada's ATIP Office remains accessible at all times for information on the process to submit a complaint and other privacy issues. Individuals may contact the ATIP office by calling (613) 954-8744 or by mailing their request to the Access to Information and Privacy Coordinator (see section 3.4.1 for their mailing address).

APPENDIX I

Acronyms

ATIP: Access to Information and Privacy

DUE: Drug Utilization Evaluation

FCH: First Canadian Health

FNIHB: First Nations and Inuit Health Branch

HICPS: Health Information and Claims Processing System

MS&E: Medical Supply and Equipment

MTRS: Medical Transportation Record System

NIHB: Non-Insured Health Benefit

OPCC: Office of the Privacy Commissioner of Canada

PIA: Privacy Impact Assessment

PIPEDA: *Personal Information Protection and Electronic Documents Act*

REB: Research Ethics Board

SVS: Status Verification System

TBS: Treasury Board Secretariat

TRA: Threat Risk Assessment

APPENDIX II

Definitions

These definitions have been adapted for the specific use of the NIHB Privacy Code.

Accountability means having clearly defined and understood responsibilities in connection with personal information, agreeing to accept those responsibilities and being subject to consequences for failing to fulfill accepted responsibilities.

Administrative purposes, in relation to using personal information about an individual, means using that information in a decision-making process that directly affects that individual.

Aggregate information means information that has been rolled up or combined to summarize a population trend or statistic.

Anonymized information means personal health information that has been altered, so that the risk is small that the information could be used alone or in combination with other reasonably available information using a reasonably foreseeable method to identify an individual who is the subject of the information.

Audit of claims refers to verifying claims submitted by a provider against the NIHB Program's billing requirements, as stated in the Provider Agreement, Pharmacy Provider Information Kit, Dental Practitioner Information Kit, Medical Supplies and Equipment Provider Information Kit, NIHB Newsletters and NIHB Drug Bulletins (for additional information, please refer to section 1. 2.1.3 of the NIHB Privacy Code).

Authorization means a client's agreement to provide or permit access to or the collection, use or disclosure of his or her personal information for specific and appropriate purposes.

Client (beneficiary, recipient) means the person whose personal information is collected and, for the purposes of this Code, may also mean a surrogate or guardian, including a parent or person having a legally recognized authority to act on behalf of the individual. Client means an eligible recipient of benefits under the NIHB Program of the First Nations and Inuit Health Branch (FNIHB).

Collection means the act of accessing, receiving, compiling, gathering, acquiring or obtaining personal information. It includes information collected from the client, as well as collecting personal information on behalf of the client from the client's health care, service professionals or providers.

Confidentiality, confidential means personal information that is collected from NIHB clients is to be kept private and not disclosed or made accessible to others unless authorized by consent where required of the client.

Consent means a client's agreement to provide or permit access to or the collection, use or disclosure of his or her personal information for specific, appropriate purposes. Consent, for the purpose of this document, can be defined as explicit/formal (express consent).

Contractor/consultant means any individual or party authorized to conduct elements of the NIHB Program – contractors hired to complete audits, provide professional expertise in reviewing and approving claims, etc. As contractors fall under the auspice of Health Canada, they are, therefore, subject to the same information handling policies and procedures as is Health Canada.

Designated information is information not concerning the national interest, but which must still must be protected, as its release because if it was compromised, it could cause injury to a specific government department, corporate interests or individuals. Examples of designated information are personal information, self-identification data and medical records. Treasury Board recommends the use of three levels of designation:

1. **Protected A - *Low Sensitivity***: applies to information that, if compromised, could reasonably be expected to cause *injury* or embarrassment outside the national interest; e.g., disclosure of an exact salary figure.
2. **Protected B - *Particularly Sensitive***: applies to information that, if compromised, could reasonably be expected to cause *serious injury* outside the national interest; e.g., loss of reputation or competitive advantage.
3. **Protected C - *Extremely Sensitive***: applies to the very limited amount of information that, if compromised, could reasonably be expected to cause *extremely grave injury* outside the national interest; e.g., bankruptcy or loss of life (e.g., the disclosure of the identity of a RCMP informant).

Disclosure means providing personal information to a third party for any reason. It includes any transfer or migration of personal information from the NIHB Program to a provider.

Encrypted information means information that has been processed by mathematically converting the information, in order to make it unintelligible (written in code), and that can only be deciphered by someone with the appropriate encryption key to decode it.

Express consent is given explicitly and clearly either verbally or in writing.

Health care professional is any person who is registered and entitled by provincial or territorial law to practise or provide health care in that province or territory, including: doctors, pharmacists, optometrists, nurses, dentists, registered psychologists and registered social workers.

Health service provider includes pharmacists, dentists, transportation providers, vision care, mental health and medical supply and equipment specialists.

Identification number can be the status or treaty number for registered First Nations, "N" or "B" number issued by NIHB for Inuit clients, or other health care number for clients from the Northwest Territories.

Identifiable personal information means any client data that could be linked back to a specific individual.

Integrity of personal information means protecting personal information throughout storage, use, transfer and retrieval so that there is confidence that the information has not been tampered with or modified other than as authorized. All database systems for the Program require passwords that allow the system to track each time a record is modified and also identifies who modified the record by the password used to access the system.

Personal information Personal information includes any information about an identifiable individual. This includes information in any form, such as:

- age, name, ID numbers, income, ethnic origin or blood type; and
- medical history.

The complete definition of personal information can be found in section 3 of the *Privacy Act.*

Personal information custodian means any organization, institution authorized to have custody, care or control of personal information and, for the purpose of the NIHB Program, includes NIHB staff nationally, First Nations and Inuit authorities delivering NIHB under Contribution Agreements and claims administrators or processors.

Personal Information Banks provide a summary of the type of information about individuals that is held by federal departments and agencies. The *Privacy Act* requires that Personal Information Banks include all personal information that is organized and retrievable by a person's name or by an identifying number, symbol or other particular assigned only to that person. Personal Information Banks must also include personal information that has been or is being used, or is available for use for an administrative purpose. Information holdings with the NIHB Program are contained in the following: Bank number: HCan PPU 016 and HCan PPU 017.

Privacy Impact Assessment (PIA) refers to a Treasury Board policy resulting in a comprehensive process recommended by the Treasury Board of Canada to help institutions determine the effects of program and service delivery initiatives on individual privacy.

Program review refers to using anonymized or identifiable information aimed at improving health care benefits, services, therapy or delivery and ensuring the long-term sustainability of the NIHB Program. NIHB Program reviews include: statistical reporting (anonymized) and Drug Utilization Evaluations (anonymized and identifiable).

Protected information is information related to other than the national interest that may qualify for an exemption or exclusion under the *Access to Information Act* or *Privacy Act*, and the compromise of which would reasonably be expected to cause injury to a non-national interest. There are three levels of protected information - Protected A, B and C. Refer to the definition of "Designated information" for details.

Privacy is the right of an individual to control the circulation of information about himself or herself and the right to protect personal information against misuse or unauthorised disclosure.

Provider means a health professional or institution that delivers health care services or products in the therapeutic context or individuals who provide transportation benefits that help clients access health benefits and services.

Purpose means a reason or aim for which personal information is collected, used, disclosed or accessed. Purposes for collecting personal information from clients must facilitate the funding of benefits and services, or delivery and ensures the long-term sustainability of the NIHB Program.

Research means a systematic investigation designed to develop or establish principles, facts or general knowledge, or any combination of them, and includes its development, testing and evaluation.

Right of privacy means that a client has the right to determine with whom he or she will share his or her information and to know about and exercise control over use, disclosure and access concerning any information collected about him or her.

Security means reasonable precautions, including physical and technical protocols, to protect personal information from unauthorized collection, use, disclosure and access, and to ensure that the integrity of the information is properly safeguarded. A breach of security would occur whenever personal information is collected, used, disclosed or accessed other than as authorized, or its integrity compromised.

Sensitivity of personal information refers to the client's interest in keeping the information private. It varies according to the nature of the information, its form, and the potential repercussions on the client's interests from its collection, use or disclosure.

Transparency and openness are the characteristics of policies, procedures and practices that seek to ensure that clients know what will happen with the personal information they confide or permit to be collected, used, accessed or disclosed.

APPENDIX III

Reference Documentation

Privacy Act

laws.justice.gc.ca/en/P-21/index.html

Access to Information Act

laws.justice.gc.ca/en/A-1/8.html

Canadian Charter of Rights and Freedom

laws.justice.gc.ca/en/charter/

Library and Archives of Canada Act

laws.justice.gc.ca/en/L-7.7/index.html

Financial Administration Act

laws.justice.gc.ca/en/F-11/

***Financial Administration Act* - Part V1 - Public Accounts**

laws.justice.gc.ca/en/F-11/58861.html#rid-58902

Privacy Legislation in Canada

www.privcom.gc.ca/legislation/index_e.asp

Access to Information and Privacy

www.canada.justice.gc.ca/en/ps/atip/

Using the *Access to Information Act* and *Privacy Act*

www.canada.justice.gc.ca/en/ps/atip/using.html

Canadian Standards Association (CSA) Standards - Privacy Code

www.csa.ca/standards/privacy/code/Default.asp?language=English

Treasury Board Secretariat (TBS) - Government Security Policy

www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg_e.asp

TBS - Privacy and Data Protection Policies

www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_128/siglist_e.asp

TBS - Retention and Disposal of Personal Information

www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/CHAP2_3_e.asp

TBS - Policy on the Management of Government Information

www.tbs-sct.gc.ca/pubs_pol/ciopubs/TB_GIH/mgih-grdg1_e.asp#eff

TBS - Operational Security Standard - (MITS)

www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/23recon-1_e.asp

TBS - Management of Information Technology Security (MITS)

www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/23RECON_e.asp

Privacy Commissioner of Canada

www.privcom.gc.ca/index_e.asp

Health Canada - Info Source Publications

infosource.gc.ca/inst/shc/fedtb_e.asp

Health Canada - Personal Information Banks

infosource.gc.ca/inst/shc/fed07_e.asp

Government Information Management

www.cio-dpi.gc.ca/cio-dpi/pols_e.asp#IM

Provincial and Territorial Legislation - Protection of Personal Information

www.hc-sc.gc.ca/ohih-bsi/theme/priv/index_e.html#prov

Protection of Personal Health Information

www.hc-sc.gc.ca/ohih-bsi/theme/priv/index_e.html