Health Canada | Santé Canada

Final Report

Audit of Privacy Practices

December 7, 2012

Table of Contents

Executive summary

The focus of this audit was on the privacy practices at Health Canada and adherence to the *Privacy Act* which provides the legal framework for the federal government's collection, use and disclosure of personal information. Health Canada collects, uses and retains more personal information than most any other federal department. The Department also stands out for the type and sensitivity of personal information under its control. Protection of personal information is a shared responsibility between the Access to Information and Privacy Division (ATIP) and programs within the branches. ATIP plays a leading role in the development and support of privacy practices across the Department while the branches have day-to-day responsibility for the protection and handling of personal information.

The audit was conducted in accordance with the Treasury Board *Policy on Internal Audit* and the *International Standards for the Professional Practices of Internal Auditing*. Sufficient and appropriate procedures were performed and evidence gathered to support the audit conclusion.

Overall, Health Canada is managing personal information under its control with care and consideration. Indeed, the Department benefits from a strong culture of security and confidentiality in the delivery of core program activities. But ensuring the security and confidentiality of personal information is not, in and of itself, synonymous with protecting an individual's privacy.

While Health Canada has made important improvements in meeting its legislative requirements under the Act, the Department will benefit from finalizing, approving and implementing its privacy management framework. The Framework will serve to guide and enforce good privacy practices across the Department. The Department will also benefit from better integration of privacy matters into strategic decision making and other risk management processes within the branches.

Based on a review of a sample of forms used for the collection of personal information in select branches, the Department will benefit from reviewing its forms under the guidance of the ATIP Director in order to obtain compliance with the notification provisions under the Act and its supporting directive.

As well, Program areas rely on standard operating procedures, as derived from enabling statutes and regulations, to govern the collection and use of personal information. In some cases, these standard operating procedures include provisions relating to privacy and for the sound handling of personal information. In other cases, standard operating procedures and guidelines for the handling of personal information do not provide sufficient information to front line staff on the personal information handling requirements under the Act. Branches will benefit from collaborating with the ATIP Division to review and update Program standard operating procedures, guidelines and protocols in order to strengthen controls for the collection, use, disclosure and retention of personal information.

While privacy training and awareness is steadily improving, the vast majority of Health Canada employees, many of whom are actively involved in the management and handling of sensitive data, have not yet received formal privacy training.

Notwithstanding the above findings, the audit noted several instances of good privacy practices at Health Canada which are noted throughout the report. Evidence shows that where individual programs have taken the lead to fund dedicated resources toward privacy, the Program area has been able to advance its privacy practices.

Management agrees with the six recommendations and has provided an action plan to strengthen privacy practices in the Department.

A - Introduction

1. Background

The *Privacy Act* provides the legal framework for the federal government's collection, use, and disclosure of personal information. The Act, which came into force on July 1, 1983, was founded on the principle that individuals have a right to know what information is being collected about them and how it will be used in the administration of government services and programs.

By law, federal institutions must limit their collection of personal information to that which directly relates to an operating program or activity of the institution. Once collected, they must also manage it with care and consideration. In order to comply with the Act and its supporting policies and directives, federal departments are required to have sufficient policies and practices in place to protect personal information under its care and control.

The Treasury Board of Canada Secretariat is responsible for monitoring departmental compliance with the Act. It exercises its oversight responsibilities largely through the analysis and review of institutional reports, including Treasury Board submissions, departmental performance reports, and the results of audits, evaluations and independent studies.

In addition to the oversight activities of the Treasury Board of Canada Secretariat, the Government has charged the Office of the Privacy Commissioner of Canada (OPC) with the responsibility of investigating complaints from individuals regarding the handling of personal information by federal institutions. The Privacy Commissioner also has the authority to conduct compliance reviews of the privacy practices of government institutions in relation to the collection, retention, accuracy, use, disclosure and disposal of personal information.

Where a department is found to have not met its legal or policy obligations, the President of the Treasury Board, upon notification of a systemic compliance issue, may review and revoke select duties and functions of the Minister, as provided for under paragraph 71 of the Act. The Board may also impose additional reporting requirements in annual reports to Parliament and/or under its Management Accountability Framework on an institution.

Examples of personal information at Health Canada

- Name, address, gender, religion, social insurance number.
- Medical, psychiatric, psychological and laboratory records.
- Records of occupational radiation exposure.
- Records of communicable diseases.
- Genetic information.

Health Canada collects, uses and retains more personal information than most any other federal department. The Department also stands out for the type and sensitivity of personal information under its control. Personal information is defined as information about an identifiable individual which is recorded in any form.

Under the Act, heads of federal institutions are required to identify, describe and publicly report personal information and classes of personal information in the annual Treasury Board of Canada Secretariat publication - Info Source. Personal Information Bank descriptions are the vehicles through which a government informs the public about the personal information it collects. Through these descriptions, individuals can also learn how their personal information is used, and for how long the information is being retained.

For the year ending 2011, Health Canada had an estimated 45 registered banks. The following table summarizes the Department's recorded inventory of personal information by program branch and program activity architecture:

RESPONSIBLE BRANCH	PRIMARY PROGRAM ACTIVITIES (PROGRAM ACTIVITY ARCHITECTURE)	PIBs	%PIB *
Healthy Environments and Consumer Safety Branch (HECSB)	▪ Environmental Risks to Health ▪ Consumer Product Safety ▪ Substance Use and Abuse ▪ Radiation Protection	21	46%
Health Products and Food Branch (HPFB)	▪ Health Products ▪ Food Safety and Nutrition	8	18%
First Nations and Inuit Health Branch (FNIHB)	▪ First Nations and Inuit Primary Health Care ▪ Supplementary Health Benefits for First Nations and Inuit	8	18%
Regions and Programs Bureau (RAPB)	▪ Canadian Health System ▪ Specialized Health Services	7	16%
Pest Management Regulatory Agency (PMRA)	▪ Pesticide Safety	1	2%
Total registered personal information banks (PIB)		45	100%

*** Note:** the number of PIBs in the table above does not reflect the number of data sets held by any given branch or program area. PIBs do however provide a fair estimate of where the Department is most active in the collection and use of personal information. Based on the above, Health Canada's management of personal information is largely held within HECSB, HPFB and FNIHB.

Health Canada Privacy Practices

As a result of its collection, use and disclosure of personal information, Health Canada is subject to the requirements of the *Privacy Act*. It is also subject to the policies and directives issued by the Treasury Board which support the Act's administration, mainly the *Policy on Privacy Protection*, the *Directive on Privacy Practices*, and the *Directive on Privacy Impact Assessment.*

General responsibilities for the administration of the Act rest with Health Canada's Access to Information and Privacy (ATIP) Division. The ATIP Division reports to the Assistant Deputy

Minister, Corporate Services Branch through the Director General, Planning, Integration and Management Services. It is currently divided into six units: Early Intake and Professional Practices, Policy Advisory (Privacy), Drugs Portfolio, Public Interest and Other, Backlog/Privacy Operations, and Public Health Agency of Canada Support. The Division had a base budget for both privacy activities and access to information activities of approximately $4.2 million for the year ended 2011-2012 and currently employs 42 full time equivalents, approximately 9 of whom are dedicated to privacy.

ATIP is responsible for a broad range of corporate services. Under the direction of the Director and ATIP Coordinator, the Division is charged with responding to information and privacy requests from the public, for promoting staff awareness and privacy training, and for developing corporate-wide access to information and privacy policies and practices. ATIP is also responsible for reviewing proposed legislation and policies affecting privacy, and for advising program managers on their obligations vis-à-vis the collection, use and disclosure of personal information under the Act. This includes coordinating and overseeing the Department's Privacy Impact Assessment (PIA) process.

Whereas ATIP plays a leading role in the development and support of privacy practices across the Department, responsibility for the protection and handling of personal information at Health Canada is a shared responsibility between ATIP and program branches. While the authorities delegated under the *Privacy Act* are to the Director of ATIP, program branches must support the functional lead by managing personal information under branch control in a consistent and lawful manner. This involves, among other things, safeguarding personal information in a manner commensurate with its sensitivity, bringing to ATIP's attention privacy issues and concerns as they arise in the handling of personal information, initiating a Privacy Impact Assessment when required, and notifying ATIP immediately of breaches. Branches are also required to inform ATIP of updates and or amendments to its personal information holdings.

2. Audit objective

The objective of the audit was to assess the adequacy and effectiveness of policies, practices, and controls at Health Canada which support departmental compliance with the *Privacy Act* and its supporting policy and directives.

3. Scope and approach

The audit focused on the privacy management responsibilities of the Corporate Services Branch and the practices of the program branches that are most actively engaged in the handling of personal information. At the time the audit was initiated, three branches accounted for approximately 82 percent of the Department's registered personal information holdings. Together, they were responsible for program activities which were collecting, using and disclosing the most voluminous and sensitive sets of personal data.

Based on preliminary risk assessment, it was been determined that a review of the privacy practices of these three program branches (HECS, HPFB and FNIHB) along with a review of strategic and policy initiatives under the responsibility of the Corporate Services Branch

(specifically ATIP) would provide the best possible assessment of the Department's overall privacy practices. Excluded from the scope of this audit was personal information belonging to Health Canada employees, which will be included in 2013-14 planned *Audit of PeopleSoft* as well as personal information belonging to Specialized Health Services – Public Service Health Program which was examined as a part of the 2012 *Audit of the Public Service Health Program*.

The audit examined both the design and operation of Health Canada's privacy management practices, as measured against the requirements of the Act and its supporting policy and directives. Audit activities were carried out within branches in accordance with the *Policy on Internal Audit*. The audit approach included: interviews and observation; a review of documentation, policies, standards, guidelines and frameworks; inquiry, testing and analysis.

4. Statement of assurance

In the professional judgment of the Chief Audit Executive, sufficient and appropriate procedures were performed and evidence gathered to support the accuracy of the audit conclusion. The audit findings and conclusion are based on a comparison of the conditions that existed as of the date of the audit, against established criteria that were agreed upon with management. Further, the evidence was gathered in accordance with the *Internal Auditing Standards for the Government of Canada* and the *International Standards for the Professional Practice of Internal Auditing.*

B - Findings, recommendations and management responses

1. Governance

1.1 Privacy management framework

Audit criterion: *The Department has developed and implemented a privacy management framework to support the management and monitoring of privacy practices department-wide.*

Under the government's *Privacy Policy*, heads of institutions are required to establish management practices to fairly and consistently administer the *Privacy Act*. Compliance with the Act presupposes the existence of an administrative infrastructure to guide and support the handling and protection of personal information. Most frequently, management practices are governed by way of a departmental privacy management framework.

A privacy management framework outlines the rules and practices by which senior management defines privacy expectations, assigns or delegates powers and responsibilities and accountability for compliance with the Act and its supporting policies. Beyond demonstrating a capacity to comply with the Act and its supporting policy and directives, a privacy management framework assists in: clarifying departmental roles and responsibilities relating to privacy, therein providing a basis for determining the structures, resources and skills needed for sound privacy management practices across all branches; promoting accountability and the continuous improvement of personal information handling practices through program reporting, audit and evaluation, and the provision of ongoing privacy training to employees; establishing clear standards for the collection, use, disclosure and retention of personal information, as well as best practices or effective controls for the promotion and enforcement of privacy.

Core components of a privacy management framework

- Organizational commitment (buy-in from the top)
- Clearly defined roles and responsibilities for privacy compliance
- Training and education requirements
- Breach and incident management response protocols
- Reference to privacy policy and risk assessment tools
- Mechanisms for oversight and review

While the most obvious outcome of a privacy management framework is the demonstrable capacity to comply with the provisions of the *Privacy Act*, if effective, the existence of such a framework would also support departments and agencies to effectively manage privacy risks thereby preserving a department's reputation in the eyes of Canadians as a trusted custodian of sensitive information.

The importance of a privacy management framework to guide the handling of personal information has long been recognized as a priority for Health Canada. As early as 2001, senior management has raised the need for a centralized, coordinated and coherent approach to privacy management across all branches which would include supporting tools and policies. In 2010, under the leadership of ATIP, Health Canada developed and began implementing a 'Privacy Strategy' to help increase privacy awareness amongst employees. However, the "strategy" was not effective at establishing governance and accountability structures to allow for the identification and monitoring of privacy related responsibilities

department-wide. As well, the strategy alone does not meet the practice management requirements set out in Treasury Board's *Privacy Policy*.

Recently, ATIP has begun to develop a privacy management framework which remains in draft. It will be important for the Department to advance its privacy practices by approving and implementing the draft framework.

Recommendation 1

It is recommended that the Assistant Deputy Minister, Corporate Services Branch implement a privacy management framework to support the management and monitoring of departmental privacy practice.

Management response

Management agrees with this recommendation.

A performance management framework will be finalized to outline the rules and practices by which senior management defines privacy expectations, assigns or delegates powers and responsibilities, and accountability for compliance with the Act and its supporting policies.

It should be noted that since June 2012, Health Canada has been providing corporate services to the Public Health Agency of Canada, and that the Performance Management Framework, when finalized, will be used by both institutions.

1.2 Roles and responsibilities

Audit criterion: *The Department has designated an individual or individuals who are accountable for the institution's compliance with the Privacy Act, policies and directives. Privacy roles and responsibilities are understood and appropriately assigned.*

According to the *Privacy Act*, heads of government institutions may delegate select powers, duties or functions under the Act to one or more officers or employees. Once a delegation order has been signed, the powers, duties and functions delegated may only be exercised or performed by the deputy head, or by the named officers or employees. While delegates are accountable for decisions rendered under the order, ultimate responsibility for compliance with the Act rests with the deputy head.

Among the several responsibilities assigned to deputy heads or delegates are: privacy awareness – making employees aware of policies, procedures and legal responsibilities under the Act; Privacy Impact Assessments – ensuring that PIAs are developed, maintained and published; and monitoring compliance with the *Privacy Policy* as it relates to the administration of the Act.

In addition to the above mandated responsibilities for department heads or delegates, Treasury Board has prescribed a series of complementary responsibilities to executives and

senior officials within departments who manage programs or activities involving the creation, collection and handling of personal information. These responsibilities run parallel to the notice, collection, use, disclosure and accuracy provisions of the Act. Together, the government's *Privacy Policy* and *Directive on Privacy Practices* are intended to set out clear responsibilities for decision-making on discretionary matters under the Act, and accountability for the management of personal information within institutions.

Privacy responsibilities at Health Canada are described in several internally available documents, most notably: the Department's Privacy Wiki, its proposed Privacy Policy, and the Draft Privacy Management Framework. While the assignment of privacy responsibilities are generally consistent with the responsibilities set out by Treasury Board of Canada Secretariat, the roles and responsibilities should be more prescriptive on the privacy responsibilities specific to the nature of Health Canada's regional and operating branches. They could also improve in setting out the general privacy responsibilities of front line staff and divisional managers most active in the handling of personal information.

Whereas responsibility for managing personal information within Health Canada is generally accepted as a shared responsibility between branch heads and the Access to Information and Privacy (ATIP) Division, few of the program respondents interviewed were able to clearly articulate where their privacy responsibilities began and ended.

Privacy contacts

- Program Privacy/Information Management Officer
- Divisional Compliance Analyst
- Branch Privacy Analyst
- Branch Privacy Champion
- Branch Privacy Coordinator
- Branch Information Management Advisor (BIMA)
- Regional Information Management Advisor (RIMA)
- Departmental Privacy Committee Member
- ATIP, Policy Advisory Group
- Legal Services, Information Management Group

On matters related to privacy policy, ATIP sees itself primarily as a subject matter expert, offering advice and guidance when engaged. By default, control over the collection, use and disclosure of personal information rests with program managers. But many privacy requirements under the Act require the participation of both operations and ATIP. In such cases, shared responsibilities are often misunderstood to be the responsibility of the other, leading to potentially weak accountability. It is perhaps also the result of the proliferation of 'privacy contacts' within the Department and increasing confusion across all branches as to the substantive privacy responsibilities of each position. Over the course of the audit, the auditors identified no less than ten primary points of contact for privacy issues emanating from branch operations. Not only were the roles and responsibilities of each position unclear, they were inconsistently staffed or provisioned.

An approved and implemented privacy management framework which should set out the roles and responsibilities of those who handle and oversee the management of personal information across the Department will serve to strengthen privacy practices. (see Recommendation 1).

Delegation order

Delegations under the *Privacy Act* vary across government institutions as they are dependent on the size, mandate and culture of the institution. Delegation is entirely at the discretion of the deputy head and occurs only if it is considered appropriate. The Policy clarifies that, in cases where the deputy head decides to delegate, a delegation order must be signed, and the delegated officers or employees must be at an appropriate level to be able to fulfill the duty.

Health Canada has a delegation order which was signed in 2007 which provides full delegated authority to the Director of ATIP for all assignable privacy responsibilities under the Act. The Department administers several statutes and programs involving the disclosure of personal information. In each case, program heads remain best informed of the contextual considerations attached to the collection, use and disclosure of personal information within the respective program areas. Similarly, while the ATIP Director is responsible for disclosures made pursuant to subsection 8(2) of the Act, he or she does not have control over the personal information to be disclosed. As a result, there is a risk that the Department will render a decision under the *Privacy Act* without fully understanding and assessing the risks arising out of the specific legal requirements applicable to the program in question. Given the amount of personal information under Health Canada's control combined with the need to collect and disclose such information routinely, operational necessities do not practically allow for the direct involvement of the ATIP Director in every disclosure. While Legal and ATIP should continue to play a consultative role in the application of delegated functions, accountability for privacy should lay with the program head that controls the personal information in question.

The Department would benefit from reviewing the Delegation Order in light of the practical application of privacy practices by branch personnel and given it has been five years since it was last reviewed and signed.

Recommendation 2

It is recommended that the Assistant Deputy Minister, Corporate Services Branch review and update its Delegation Order under the Privacy Act so as to identify clear accountability for privacy responsibilities.

Management response

Management agrees with this recommendation.

The Delegation Order will be reviewed to determine whether it is necessary and/or appropriate to re-assign powers, duties and functions under the *Privacy Act*. If necessary, a modified Delegation Order will be put in place following the review.

2. Risk management

2.1 Privacy impact assessment

Audit criterion: *The Department has an effective privacy impact assessment process in place to identify, assess and mitigate the privacy risks associated with new or modified activities that involve the use of personal information.*

As of 2002, all departments and agencies were responsible to identify, assess and mitigate the privacy risks and impacts of new or substantially modified programs or activities involving personal information. Privacy impact assessments are the risk management process that enables organizations to anticipate and analyze the privacy risks attached to a proposed program, service or policy. According to the Office of the Privacy Commissioner of Canada, PIAs are the most comprehensive model in place to evaluate the effects of a specific service delivery initiative on an individual's privacy and are a core component of the federal government's privacy management framework. The end product of a PIA is the assurance that potential privacy issues have been identified and mitigating strategies are developed.

Departments are expected to have in place the infrastructure to support the completion of PIAs commensurate with the level of risk related to the privacy invasiveness of the program or activity under review. An effective PIA process should include: a policy which informs staff and other stakeholders of the *PIA Directive* and its requirements, and formally defines departmental PIA responsibilities and accountabilities therein; a system to effectively report all new initiatives that require a PIA; a system to track and monitor PIAs for departmental compliance with the reporting requirements for PIAs under the *PIA Directive*; and appropriate resources and expertise committed to support departmental PIA obligations.

In 2006, Health Canada put in place a formal administrative process for managing and directing the completion of privacy impact assessments. The department's ATIP Division released a 'Privacy Impact Assessment Toolkit' which, among other things, stresses the importance of privacy considerations in departmental projects, notes privacy related roles and responsibilities, describes the Department's PIA process, and provides tools for program personnel responsible for the completion of PIAs. The PIA Toolkit has been updated periodically since 2006, most recently to reflect new Treasury Board of Canada Secretariat requirements under the new Directive. Prior to that time, the process was ad hoc and informal relying near exclusively on the participation of ATIP staff in outreach activities. While such measures were somewhat successful in creating an awareness of the privacy impacts associated with large system developments, this activity was not able to fully support the conduct of PIAs for non-information technology related projects.

In 2007 the Office of the Privacy Commissioner produced a Privacy Impact Assessment Maturity Model in order to establish a reasonable benchmark for the evaluation of management control frameworks. At that time, Health Canada was situated at a level one on the maturity scale. Since then, based on the internal audit results, the Department has moved to a level three - see rating. (see below)

Status of Health Canada's PIA Environment (based on the Office of the Privacy Commissioner's 2007 PIA Maturity Model)

OPC 2007 Assessment of Health Canada PIA Maturity (OPC)
IA 2012 Assessment of Health Canada PIA Maturity (Internal Audit)

MATURITY LEVEL		STATUS OF HEALTH CANADA'S PIA ENVIRONMENT
0	Non-existent	There is no recognition of the need for PIAs. Privacy (including proper personal information handling practices more generally), is not part of the organization's culture. There is a high risk of non-compliance with the Policy and a high likelihood of privacy deficiencies or incidents. In such an environment, few, if any, PIAs are completed when required.
1	Initial/ad-hoc (IA)	There is some recognition of the *PIA Directive* and the need for an administrative infrastructure to manage the PIA process within the organization. The entity's approach to meeting Directive requirements is ad hoc and disorganized, and lacks formal leadership, guidance or monitoring by senior management. Deficiencies in the manner in which PIAs are conducted have not been considered or identified. Employees are not aware of their responsibilities within the organization or with respect to the PIA Directive government-wide. In such an environment, some PIAs are likely completed, but many are not, and the quality of privacy impact analysis is likely poor.
2	Recognized but intuitive	A PIA framework is in place but lacks critical elements to support the Policy's objectives and requirements. Control weaknesses exist within the PIA process and have not been adequately identified or addressed by management; the impact of such deficiencies may be significant. Management may or may not be aware of their obligations under the Directive. Employees may not be aware of their responsibilities within the PIA process. The quality of PIAs and the manner in which a PIA is completed (including whether or not a PIA is initiated) is dependent on the knowledge and motivation of individual employees.
3	**Defined PIA process (OPC)**	A formal PIA process is in place and documented. Management is fully aware of their PIA obligations and has begun introducing PIA guidelines into their overall operations. However, the process is not adequately enforced and there are some remaining control weaknesses within the PIA process. While management is able to deal predictably with most privacy issues which arise from operations, some control weaknesses persist within the PIA process and impacts could still be severe. Employees are aware of their responsibilities but the organization lacks adequate resources to support the department's obligations under the Directive.
4	Managed and measurable	A formal PIA process is in place and documented. Management is fully aware of their PIA obligations and is meeting their requirements and obligations under the Directive. Responsibilities/accountabilities under the Directive have been formally defined and both management and employees are proactively involved in all aspects of the PIA process. Programs are in place to inform staff and other stakeholders of the Policy's objectives and requirements and adequate resources have been committed to support the department's obligations under the Directive. An effective system of reporting of all new initiatives requiring a PIA exists. For the most part, high quality PIAs are completed, when required, in a timely manner.
5	Optimized	The assessment of operational privacy impacts has been integrated into the entity's overall risk management framework (at the center of which exists a formal PIA process). Organization wide controls ensure continuous and effective monitoring for compliance with the organization's own PIA process and the Treasury Board Directive. An individual/body is charged with overseeing compliance with the Policy and a body composed of senior personnel is charged with reviewing and approving PIA candidates once complete. The organization conducts performance monitoring on key financial, operational and human resource aspects of PIA operations, and the results of PIAs are integrated into ongoing project management.

Recognizing this progress, additional efforts are still required to fully meet the Department's obligations under the new Directive. Privacy impact assessment processes continue to vary across branches. For example, assessments are not always completed and if completed they are not timely enough to build privacy considerations into new or substantially modified programs involving personal information. In addition, despite a requirement for branches to seek the formal approval, endorsement or sign-off from the ATIP Director for all PIAs, ATIP is often unaware of PIAs undertaken by branches or branch decision to not complete an assessment. The audit did note a good program practice within the Health Products and Food Branch (HPFB) that consistently uses PIAs to inform its program.

Privacy Impact Assessments • Marketed Health Products Directorate - HPFB

In the past several years, Health Canada's Marketed Health Products Directorate has initiated over eight Privacy Impact Assessments or privacy risk reviews to assess the privacy impacts of new programs (or amendments to existing programs) involving personal information. Each assessment included an expert analysis of program plans against the privacy requirements under the *Privacy Act* and the CSA's Model *Code for the Protection of Personal Information.* At the time of the audit, the Directorate maintained a repository of PIAs and was tracking the status of privacy recommendations to ensure that privacy issues raised are being appropriately mitigated.

Health Canada would benefit from some additional internal controls such as a mandatory and formal screening process to identify all potential projects involving personal information. Branch contacts interviewed noted that they did not have policies or processes in place to identify all activities within the branch requiring a privacy impact assessment. A screening process acts as a trigger point for any privacy impact analysis – precludes program managers from properly assessing the extent to which there may be privacy risks associated with a new initiative. Such a control would limit the instances of PIA omissions noted in the audit.

Recommendation 3

It is recommended that the Assistant Deputy Minister, Corporate Services Branch improve the Department's Privacy Impact Assessment process to better align it with the Treasury Board Directive.

Management response

Management agrees with this recommendation.

The existing Privacy Impact Assessment Toolkit has been in place since 2006, but will be reviewed, improved and updated for the use of both Health Canada and the Public Health Agency of Canada.

The Branch will develop an internal communications strategy to promote employee understanding of the need and the process involved in finalizing a Privacy Impact Assessment. This multi-faceted strategy will include posting the toolkit to the Health Canada Intranet.

2.2 Awareness and training

Audit criterion: *The Department has an effective privacy training and awareness program.*

The Government of Canada - *Privacy Policy*, expects deputy heads or the delegates to be responsible for making employees aware of policies, procedures and legal obligations under the Act. At Health Canada, this responsibility resides with the Director of ATIP.

In October 2010, ATIP launched a departmental Privacy Strategy to: increase employees' general awareness of privacy; and to build a greater understanding of best practices in personal information handling in program areas identified as high risk. The first phase of the Strategy was implemented during the reporting period 2011-12. Phase two of the Strategy is to be executed in the year 2012-13.

Health Canada's centerpiece for privacy training is its 'Privacy 101' course. The course, which ranges in duration from 90 minutes to 2 hours, covers a broad range of topics, most importantly departmental obligations under the Act and its supporting policy and directives. As designed, the course is intended to offer employees a primer on privacy responsibilities under the Act. While it has proven successful in creating privacy awareness among attendees, the course does not speak in great detail to departmental Privacy Impact Assessment requirements, privacy breach protocols, or the registration and update of personal information banks at Health Canada. Since the Fall of 2010, 'Privacy 101' has been regularly offered from September through May. Going forward, it is ATIP's intention to make the course available year round.

In addition to the Department's 'Privacy 101' offering, ATIP also offers customized privacy training to program areas, if and when requested. In such cases, the 'Privacy 101' course is customized to the program area recipient. 'Privacy 101' is also delivered annually to "targeted groups" identified by the Department's Executive Committee for Internal Services. While fifteen minutes of privacy training is said to be included in employee orientation through the Department's "Information Management Accountable Program", such training, where offered, focuses only on the confidential handling of personal information and not on the broader privacy responsibilities of federal employees under the Act. While Health Canada

also benefits from an online learning tool for privacy, ATIP is currently unaware of the take up.

For the fiscal year ending 2012, ATIP reports having delivered "privacy awareness training" underscoring the "importance of safeguarding personal information" to 3,122 Health Canada employees (or approximately 29 percent of Health Canada's full time equivalents). Included in this figure is the delivery of 'Privacy 101' training to 896 Health Canada employees across the country. This is commendable given the limited resources dedicated to the delivery of privacy training. Notwithstanding the training momentum engendered by the Department's Privacy Strategy, actual privacy training at Health Canada has been sometimes sporadic. For example, in an effort to deliver privacy training to remote locations in Canada deemed "high risk", ATIP put its training program on compact discs which were shipped to various communities. Yet interviews noted that uptake of the training was unclear. ATIP would have benefited from following up after delivery of the training packages to determine if training occurred.

Where knowledge of privacy exists, it appears to have been obtained from other employees, anecdotal sources or through experience with other departmental privacy issues. Evidence shows that where individual programs have taken the lead to fund dedicated resources toward privacy training the program area has been able to advance privacy practices.

Privacy Training • Medical Marijuana Medical Access Division (Healthy Environments and Consumer Safety Branch)

In October 2010, Health Canada's Medical Marijuana Division was identified as a program area of potentially high privacy risk. Recognizing the need for greater privacy awareness among front line employees and managers, the Program has since provided specialized privacy training to 100 percent of its staff. Not only has the training program (delivered by ATIP) heightened employee sensitivity surrounding stakeholder privacy, it has led to improvements in the collection, use and disclosure practices for personal information.

In conclusion, while there a strong departmental culture of confidentiality and a general awareness of the need to safeguard personal information and across all branches, specific requirements relating to the handling of personal information (in particular amongst front line staff) are less well understood. Evidence gathered in the course of the audit suggests that employees have a limited understanding of what constitutes "personal information" under the Act, and a very cursory appreciation of their responsibilities surrounding the collection, use and disclosure of personal information.

Recommendation 4

It is recommended that the Assistant Deputy Minister, Corporate Services Branch enhance its privacy awareness and training strategy with specific training requirements for Health Canada employees most actively involved in the handling of personal information.

Management response

Management agrees with the recommendation.

A comprehensive privacy awareness strategy will be developed that identifies specific training requirements for those Health Canada and Public Health Agency of Canada employees most actively involved in the handling of personal information.

3. Internal control

3.1 Notice

Audit criterion: *The Department has controls in place to inform individuals whose personal information is being collected of the purpose of collection (except as provided by law).*

Under subsection 5(2) of the *Privacy Act*, federal institutions must inform individuals from whom it collects personal information of the purpose for which the personal information is being collected. Notice may not be required in exceptional circumstances, where indicating the purpose for collection might result in the collection of inaccurate information, or prejudice the use for which the personal information is being collected. The requirement to provide notice regarding the purpose for collection extends to indirect collections from third parties.

In ensuring that departments are providing fair notice of the purposes for which personal information is being collected, Treasury Board of Canada Secretariat has issued guidelines for notification. Under paragraph 6.2.9 of the *Directive on Privacy Practices*, departments must notify the individual whose personal is collected directly of the following:

1. The purpose and authority for the collection
2. Uses or disclosures that are consistent with the original purpose
3. Uses or disclosures that are not related to the original purpose
4. Legal or administrative consequences for refusing to provide the personal information
5. Rights of access to, correction of and protection of personal information under the Act

By virtue of the Department's broad mandate for healthcare, research, policy and enforcement, Health Canada relies on hundreds of different forms for the collection of personal information. In many cases, forms used for the collection of personal information are outdated, some dating prior to the introduction of the Act. Others, while comparatively more current, have not been reviewed for some time, despite significant changes to the programs to which they are attached and the personal information requirements of those programs. Based on a review of a sample of forms used for the collection of personal information in select branches, the Department will benefit from reviewing its forms under the guidance of the ATIP Director in order to obtain compliance with the notification provisions under the Act and its supporting directive.

Recommendation 5

It is recommended that the Assistant Deputy Minister, Corporate Services Branch collaborate with the other Branches to coordinate a review of forms in use by program directorates for the collection of personal information for compliance with the notice provision of the Act and Directive on Privacy Practices.

Management response

Management agrees with this recommendation.

The Access to Information and Privacy Division will review, in conjunction with the appropriate branch, those forms identified in the audit as not complying with the notice provisions of the Act in order to identify whether changes need to be made.

A review will be completed of all departmental forms used for the collection of personal information to ensure that the respective branches are aware of the requirements, and make amendments as required.

3.2 Collection, use, disclosure, retention

Audit criterion: *The Department has controls in place to limit the collection, use, disclosure and retention of personal information to that provided by law.*

Pursuant to section 4 of the *Privacy Act*, personal information can only be collected by a department/agency if it relates directly to an operating program or activity of the institution. Federal institutions must limit collection of personal information to that which is demonstrably necessary. Similar restrictions apply to the *use* and *disclosure* of personal information by federal institutions where personal information can only be used or disclosed for the purposes for which it was collected, except with the individual's consent (or in exceptional cases without consent). While retention periods for personal information will vary by program and the prescribed regulations attached to those programs, subsection 6(1) of the Act requires that personal information used for an administrative purpose be retained for such a period of time after it is used to allow that individual reasonable opportunity to obtain access to the information.

In order to limit its collection, use, disclosure and retention of personal information, the Department is required to have appropriate administrative controls in place to manage and monitor its personal information holdings. The audit revealed however that there are no formal and documented controls in place for collecting, using, disclosing and retaining personal information in a manner compliant with the Act. In most cases, program areas rely on standard operating procedures, as derived from enabling statutes and regulations, to govern the collection and use of personal information. In some cases, these standard operating procedures include provisions relating to privacy and or the sound handling of personal information. In other cases, standard operating procedures and guidelines for the handling of personal information do not provide sufficient information to front line staff on

the personal information handling requirements under the Act. Despite these findings, the audit did note two good practices in the First Nations Inuit Health Branch which demonstrate the Branch's strong commitment towards handling of personal information.

A Publicly Available Privacy Code • (FNIHB)

In an effort to encourage the fair, transparent and consistent handling of personal information, Health Canada's Non-Insured Health Benefits (NIHB) Program has publicly set out its commitment to protect the confidentiality of data that it collects and uses in the delivery of its program through the creation of a formal 'Privacy Code'. The NIHB Privacy Code applies to all employees of the NIHB Program and all individuals, groups or organizations that collect, use, disclose or access personal information to administer non-insured health benefits. In addition to helping ensure that the Program remains in compliance with the *Privacy Act*, the Privacy Code demonstrates a strong commitment to protecting the privacy of First Nation communities and to safeguarding the personal information of individuals under its control.

Nursing Guides for Personal Information Sharing • Internal Client Services (FNIHB)

Sharing personal information is often indispensable in the provision of primary health care. Providing appropriate and timely care often requires the disclosure of personal health information to specialists within a patient's "circle of care" or to others with a legitimate need to access personal health information under limited and specific circumstances. In order to disclose personal information where appropriate, bearing in mind the need to balance an individual's right to privacy with the legitimate needs of others to collect, use and disclose information in the delivery of primary health care, FNIHB has developed Privacy Standard Operating Procedures for the disclosure of personal information. These Standard Operating procedures, developed in consultation with Legal Services and ATIP, provide front line employees with a quick reference as to how and when personal information can be shared and the steps to take in protecting patient privacy.

In addition to Standard Operating procedures and documented protocols for the handling of personal information, Health Canada is said to rely on provincial regulations governing the conduct of provincial health practitioners in obtaining assurance over the personal information handling practices medical providers (particularly in the provision of health care to First Nations and Inuit populations).

A sample analysis of such regulations however indicates that they are not equivalent to those outlined in the *Privacy Act*. In some instances, a medical practitioner's professional and ethical duties may in fact conflict with federal privacy laws. As such, program reliance on professional practice guidelines (or provincial policies governing medical professionals) may not be sufficient to meet Health Canada's privacy obligation vis-à-vis the handling of personal information under the Act.

Recommendation 6

It is recommended that the Assistant Deputy Minister, Corporate Services Branch collaborate with the other Branches to coordinate a review to update Program standard operating procedures, guidelines and protocols in order to strengthen controls for the collection, use, disclosure and retention of personal information.

Management response

Management agrees with this recommendation.

Guidelines for the collection of personal information will be issued by the Access to Information and Privacy Division.

A sample of program procedures and protocols will be reviewed by the ATIP Division within one year of the issuance of the above-noted guidelines to ensure that the collection of personal information is being undertaken in accordance with them.

3.3 Accuracy

Audit criterion: *The Department has controls in place to support accurate, complete and up-to-date information that is used to make administrative decisions about an individual.*

As per subsection 5(2) of the *Privacy Act*, government institutions must take all reasonable measures to have personal information, used for administrative purposes, that is accurate, up-to-date and complete as possible. These measures must involve one or more of the following:

- Direct collection or validation with the individual;
- Indirect collection or validation when authorized or when consent was obtained, which may involve verifying the personal information against a reliable source (either public or private); and
- Technological means to identify errors and discrepancies.

In addition to the above, federal institutions must give individuals, whenever possible, the opportunity to correct inaccurate information about them before any decision is rendered which could impact their standing or entitlement to government programs or services.

Health Canada relies on both the direct and indirect collection of personal information in the delivery of its program and services. Where information is collected directly, the Department relies on standard forms which are retained on record for a period sufficient to allow for the update or correction of inaccurate data. Where information is collected indirectly, the Department relies on contractual provisions and consent mechanisms to validate the accuracy of information collected and used for administrative purposes. In some cases, standard operating procedures for select programs encourage the verification of personal information prior to use (see Recommendation 6). Access to – and the ability to update and correct personal information records – is afforded to the individuals through the Department's ATIP Division.

The audit did not uncover any instances where personal information used by the Department was deemed inaccurate or incomplete. For the two years ending in 2012, Health Canada had no complaints or investigations relating to information accuracy.

3.4 Safeguards

Audit criterion: *The Department has controls in place to safeguard personal information under its control from unauthorized use or disclosure.*

Safeguards for the use and disclosure of personal information are set out in the Government of Canada - *Policy on Government Security*. Therein lays a requirement for personal information to be protected by security safeguards appropriate to the sensitivity of the information. Further provisions governing the safeguard of personal information are set out in the Treasury Board of Canada Secretariat *Directive on Privacy Practices*.

While security protocols surrounding personal information vary according to the sensitivity of information at risk, personal data at Health Canada is generally safeguarded by way of: physical measures (for example, locked filing cabinets and restricted access to offices); organizational measures (for example, security clearances and the limited sharing of personal information based on a "need to know" basis); and technological measures, through the use of passwords and encryption for systems containing personal information.

Interviews with officials from the Department's Safety, Emergency and Security Management Division with select regional security officers were completed and a review of the audits results and actions to date from two recent audits which examined information safeguards was completed. The previous audits were the 2011 *Audit of Information Technology Security* and the 2010 *Audit of Information Management.* Finally, the auditors performed walkthroughs of select facilities housing personal information in order to determine the extent to which data were physically secure.

Overall, Health Canada has appropriate controls in place to safeguard personal information under its control from unauthorized use and disclosure. However, issues raised in recently completed audits concerning access controls and control monitoring continue to require management's attention. This position is supported by the work of the Department's Safety, Emergency and Security Management Division which, through Health Canada's Departmental Security Plan, includes plans to help further protect personal information. It was noted at that time of the Audit of IT Security, that Health Canada's network was segregated into two zones while the minimum recommended number is four zones normally associated with a network rated at the Protected-B level. Since then, the Department, in collaboration with Shared Services Canada, has recently taken steps to increase its security posture (moving the network to Protected B status) to better serve Health Canada's business clients.

C - Conclusion

It has been more than ten years since the introduction of government policies and directives supporting the administration of the *Privacy Act*. Health Canada has clearly made progress in applying these policies and directives (such as moving from a level 1 maturity to a level 3 on the Privacy Impact Assessment maturity model) however there are some areas that will benefit from additional work.

More specifically, the Department will benefit from a centralized and coherent framework for the management of privacy practices across all branches. In addition, roles and responsibilities for privacy should be more clearly defined; there should be more and better integration of Privacy Impact Assessment results into strategic decision making and other risk management processes; and lastly, employees working with personal information should receive privacy training. It was also noted that there is a shortage of resources within the Access to Information and Privacy (ATIP) Division for the provision of privacy advice and support.

Over the past two years, ATIP has made significant efforts to promote privacy awareness across the Department. Additional effort is nonetheless required to translate growing privacy awareness into good privacy practices across the Department.

Appendix A – Lines of enquiry and criteria

Audit of Privacy Practices		
Criteria Title		**Audit Criteria**
Line of Enquiry 1: *Governance*		
1.1	Privacy management framework	The Department has developed and implemented a privacy management framework to support the management and monitoring of privacy practices department-wide.
1.2	Roles and responsibilities	The Department has designated an individual or individuals who are accountable for the institution's compliance with the *Privacy Act*, policies and directives. The privacy roles and responsibilities are understood and appropriately assigned.
Line of Enquiry 2: *Risk Management*		
2.1	Privacy impact assessment	The Department has an effective privacy impact assessment process in place to identify, assess and mitigate the privacy risks associated with new or modified activities that involve the use of personal information.
2.2	Awareness and training	The Department has an effective privacy training and awareness program.
Line of Enquiry 3: *Internal Control*		
3.1	Notice	The Department has controls in place to inform individuals whose personal information is being collected of the purpose of collection (except as provided by law).
3.2	Collection, use, disclosure, retention	The Department has controls in place to limit the collection, use, disclosure and retention of personal information to that provided by law.
3.3	Accuracy	The Department has controls in place to support accurate, complete and up-to-date information that is used to make administrative decisions about an individual.
3.4	Safeguards	The Department has controls in place to safeguard personal information under its control from unauthorized use or disclosure.

Appendix B – Scorecard

Criterion	Rating	Conclusion	Rec #
Governance			
1.1 Privacy management framework	**NMO**	The Department is working towards having a privacy management framework in place to support the management and monitoring of privacy practices across all branches.	1
1.2 Roles and responsibilities	**NMO**	Roles and responsibilities for the management and handling of personal information are unclear. Designated responsibilities for the institution's compliance with the *Privacy Act* may not be appropriately assigned.	2
Risk Management			
2.1 Privacy impact assessment	**NMO**	The Department has made significant progress in improving its PIA practices, but additional efforts are required to fully meet the Department's obligations under the government's *PIA Directive*.	3
2.2 Awareness and training	**NMO**	The Department's Privacy Training and Awareness program has improved significantly in the past two years but could benefit from a strategic review. Training is not integrated into employee orientation and should be delivered to all staff involved in the management and handling of personal information.	4
Internal Control			
3.1 Notice	**NMO**	Not all forms used for the collection of personal information at Health Canada meet the notification provisions under the Act.	5
3.2 Collection, use, disclosure, retention	**NMO**	There is a need to review and update the standard operating procedures, guideline and protocols used to control and limit the collection, use, disclosure and retention of personal information.	6
3.3 Accuracy	**S**	The audit did not uncover any instances where personal information used by the Department was deemed inaccurate or incomplete.	None
3.4 Safeguards	**NMI**	Health Canada has adequate controls in place to safeguard personal information under its control from unauthorized use and disclosure.	

S	NMI	NMO	NI	U	UKN
Satisfactory	Needs Minor Improvement	Needs Moderate Improvement	Needs Improvement	Unsatisfactory	Unknown; Cannot Be Measured