Office of the Information and Privacy Commissioner
for Newfoundland and Labrador

Privacy Audit

A Compliance Review Tool

May 2005

Table of Contents

Introduction

This Privacy Audit, is designed for Newfoundland and Labrador public bodies to assess their compliance with the privacy provisions of the *Access to Information and Protection of Privacy Act* (ATIPPA). A Privacy Audit may also be referred to as a Privacy Impact Assessment. This tool may be used to review existing programs and, as well, to ensure that privacy compliance is built into new programs/activities or the modification of existing programs/activities.

The Audit should be completed by a Privacy Working Committee of each public body. The Committee's report should ensure that each question is fully addressed.

The Privacy Working Committee's Final Report will answer each question, broken down by activity or program, and will include explanatory notes, existing/proposed privacy policy documents which comply with ATIPPA. Where deficiencies are identified, an action plan to achieve compliance is to be attached.

Privacy:

The right of individuals to control the collection and use of personal information about themselves.

Robert Ellis Smith

The Privacy Working Committee should be represented by senior staff members of each major operating area of the public body and any staff member designated with responsibilities for the protection of personal information under ATIPPA. As well, it is recommended that an observer from outside the organization be available to the Committee for consultation, as required.

All members of the Privacy Working Committee should become thoroughly familiar with the privacy provisions of ATIPPA (Part IV) and undertake the audit using the policy and guidance provided in Chapter 5 of the ATIPPA Policy and Procedures Manual.

Undertaking a comprehensive audit of its personal information handling practices will enable a public body to

- develop privacy policies
- identify deficiencies and areas needing attention
- assure compliance with ATIPPA

Inventory and Purposes for Collection

1. Describe the type of personal information or personal data elements collected. Identify the type and amount of personal information collected for each program and activity, from whom it is collected, by whom it is used, and to whom it is disclosed. You may use a narrative description, flow chart, or table (as in the example below), or a combination of these.

Example

	Activity	Personal Info	Collected From	Used By	Disclosed To
1	Moose/Caribou License	Name Address Tel. No. MCP No. Hunter Certificate No. Height Weight Hair Colour Eye Colour Date of Birth	Individual	• Wildlife Division • Science Division	• Conservation Officers & Regional /District Clerks, Forest Resources & Agrifoods • xwave

2. Section 32 states that personal information may be collected only if such collection is:

   (a) expressly authorized by or under an Act, or
   (b) collected for law enforcement purposes, or
   (c) relates directly to and is necessary for an operating program or activity of the public body

   Under what authority is the personal information collected? Specify the legislation, program/activity or law enforcement purpose. Is the collection of personal information demonstrably necessary to meet one of the conditions stated in Section 32? Will the collection of personal information effectively accomplish the purpose for which it has been undertaken? Is there a less privacy-invasive means of achieving the same end?

   Remember: Any collection of personal information not authorized by Section 32 is being collected in contravention of ATIPPA. Section 32 applies to information collected for a public body by a third party (ie. a contractor) as well as to information collected by the public body itself.

Limiting Collection

3. How is the personal information collected? Personal information must be collected directly from the individual the information is about unless another method of collection is authorized under subsection 33(1). Is the personal information collected directly from the individual it is about or his/her authorized representative?

    - If so, is the individual informed of the purpose, authority for collection, and how to contact an officer or employee who can answer his/her questions about the collection?[1]

    - If not, is the indirect collection authorized under subsection 33(1)?

4. Is the amount of personal information collected kept to the minimum amount required to carry out the purpose for which it is being collected?

5. Describe written policies and procedures regarding the collection of personal information. Personal information may be gathered in a variety of ways: interviews, questionnaires, surveys, video recordings, polls, application forms, etc. Are all application forms and other instruments which collect personal information updated so that they comply with ATIPPA?

6. Are staff handling personal information trained in the protection of privacy principles of ATIPPA?

Accuracy, Access and Correction

7. What steps are taken to ensure that personal information which will be used to make a decision directly affecting an individual is accurate and complete? (Section 34)

8. What procedures are in place to deal with access requests by individuals seeking information about themselves? [Subsection 7(1)]

9. What steps are taken to ensure that an access request is from the individual to whom the information applies?

[1] There may be occasions when the duty to notify an individual of the purpose and authority for the collection does not apply. See subsection 33(3) of ATIPPA.

If there is any doubt about the identity of the individual seeking access to personal information, a procedure to verify identity needs to be in place.

10. Is the authority to modify or correct personal information clearly established to ensure that those without authority may not or are unable to alter records containing personal information?

11. What procedures are in place to permit individuals who wish to have their personal information corrected to do so? (Section 35)

12. What steps are in place to ensure that all copies of the information are corrected or annotated?

13. If the personal information which has been corrected or annotated was disclosed to any third party during the one year period before the requested correction, what steps are in place to identify those third parties and to ensure that these copies held by them are corrected or annotated?

Protection

ATIPPA requires public bodies to protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure and disposal. (Section 36) Records of personal information in all formats – paper, audio, video, electronic or other media – are to be protected.

14. Identify the public body's security policy, practices and procedures which meet the requirements of section 36 of ATIPPA.

15. Are internal access rights provided only on a need-to-know basis, consistent with the purpose for which the information is collected?

16. Are systems in place to identify and deal with security violations?

Use

Use of personal information is permitted only in accordance with section 38.

17. Is the personal information being used

    - For the purpose for which that information was obtained or compiled, or for a use consistent with that purpose as described in section 40?

- Where the individual the information is about has identified the information and has consented to the use?

- For a purpose for which that information may be disclosed to the public body under sections 39 to 42?

If none of the above three conditions of use applies, the information is being used in contravention of ATIPPA.

18. What controls are in place to ensure that only the minimum amount of personal information needed to carry out the program or activity is used?

19. Are physical, administrative and technical controls in place to limit internal access to identifiable personal information to those who have a "need to know?"

Disclosure

Personal information may be disclosed by a public body only in accordance with section 39 of ATIPPA. The disclosure of personal information must be limited to the minimum amount of information necessary to accomplish the purpose for which it is disclosed. Disclosure may be to a third party, another public body, or a division within a public body. Even within the public body itself, disclosure of personal information among employees must be limited. [Paragraph 39(1)(f)]

20. Is personal information disclosed to other public bodies or to third parties?

    - If so, what is the authority for disclosure under section 39 of ATIPPA?

    - Is the disclosure limited to the minimum amount of information necessary to accomplish the purpose for which it is being disclosed?

    - If disclosure is required and authorized, are the amount and type of disclosed information limited to a "need to know" basis?

21. Is identifiable personal information disclosed for research purposes?

    - If so, does the disclosure follow the requirements of section 41 of ATIPPA?

    - Is a signed agreement in place between the researcher(s) and the public body in accordance with paragraph 41(d)?

22. Are physical, administrative and technical controls in place to limit disclosure of identifiable personal information to those within the public body who have a "need to know?"

23. If personal information is being disclosed for archival or historical purposes, is the disclosure in compliance with section 42?

Management of Personal Information

24. What procedures are in place to ensure that personal information used to make a decision affecting an individual is retained for at least one year after using it in order to permit the individual a reasonable opportunity to obtain access to his/her personal information. (Section 37)

25. Has a person been delegated to be responsible for each personal information bank or system?

26. Have the needs for managing personal information been integrated into records management systems?

27. Is any personal information in electronic form? If so, is this information managed in the same way as paper records? If not, describe the principles and practices applied to electronic records.

28. Are all staff who handle personal information trained in the principles of privacy protection?

29. Are systems in place to provide periodic checks for compliance with the privacy provisions of ATIPPA?

30. Are systems in place to ensure that new programs/activities or modifications to existing programs/activities are assessed for compliance with ATIPPA?

31. Is a procedure in place to deal with and correct any breach of the privacy provisions of ATIPPA?