9.
PRIVACY COMPLIANCE

Overview

This chapter covers

- privacy compliance reviews;
- privacy considerations when planning or implementing new or modified programs, information systems or administrative practices;
- privacy impact assessments;
- reviewing forms and other collection instruments;
- developing security policies;
- conducting threat and risk assessments; and
- privacy considerations for data matching and data sharing arrangements.

9.1 Privacy Compliance Reviews

Compliance with **Part 2** of the *FOIP Act* can be determined by reviewing a public body's practices, activities, programs and systems in which personal information is collected, maintained, used and disclosed. A privacy compliance review process will assist program managers and administrators responsible for personal information banks in assessing their current level of compliance and in identifying necessary and appropriate steps to bring the public body into compliance, if required.

Public bodies should have policies and organizational structures in place that will facilitate the integration of privacy protection requirements and practices into the ongoing management of personal information banks, programs, activities and information systems.

The privacy compliance review process will

- support the public's right to know what personal information the public body is collecting and how this information is used;
- support the right of individuals to access their own personal information;
- assure individuals that their personal information will be collected, used and disclosed only as authorized; and
- maintain public confidence in the public body's systems and programs with respect to the handling of personal information.

The following framework, based upon the applicable *FOIP Act* sections, can be used to review how a program, activity or information system protects personal information.

Protection of personal information analysis

Sections 33 to **42** of the *FOIP Act* control the manner in which personal information is collected, used and disclosed and the requirements for protecting, correcting, retaining and assuring the accuracy of such information. This framework identifies what a public body is required to do under the Act and also, in some instances, what a public body may want to consider doing in addition to what is required under the Act. **Part 2** of the Act and Chapter 7 should be referred to while using the framework.

Authority for collection

Section 33 **Section 33** limits the collection of personal information by public bodies. Collection must be authorized under **section 33(a)**, **(b)** or **(c)**.

What is required?

- An enactment of Alberta or Canada must specifically authorize collection of the personal information; that is, the enactment must expressly refer to the activity of collecting personal information for specified purposes; or
- The personal information must be collected for the purposes of law enforcement; or
- The personal information must relate directly to and be necessary for an operating program or activity of the public body (the collection cannot be for a prospective program or activity that does not currently exist and personal information must not be collected "just in case").

For consideration

- When establishing new programs or reviewing existing programs and activities, consider putting a process in place to ensure that the minimum amount of personal information necessary to carry out the program or activity is collected.

Manner of collection

Section 34(1) **Section 34(1)** requires a public body to collect personal information directly from the individual the information is about except in certain limited circumstances.

What is required?

- Personal information must be collected directly from the individual the information is about (direct collection) unless the public body is authorized to collect information indirectly.
- If the personal information is collected from a source other than the individual the information is about (indirect collection), there must be authority in **section 34(1)(a)** to **(o)** for indirect collection.

If a public body is not authorized to collect personal information indirectly under **section 34(1)(a)** to **(o)**, the public body must either collect the personal information directly from the individual or not collect the personal information at all. The only

exception to this would be if **section 34(3)** applies (information collected directly would be inaccurate).

For consideration

- **Section 34(1)(a)** to **(o)** permits indirect collection in a number of different circumstances. However, a public body should consider collecting personal information directly unless indirect collection is necessary in the specific circumstances of the program or activity.

Notification of collection

Section 34(2) When personal information is collected directly from an individual, notification of the purposes of and authority for the collection must be provided to the individual.

What is required?

- If personal information is collected directly, the notification provided to the individual from whom the information is collected must include
    - the specific purposes for which the information will be used;
    - the specific legal authority for the collection of information (the public body's own governing legislation or the *FOIP Act*); and
    - the title, business address and telephone number of an official in the public body who can answer questions about the collection of personal information.
- If notification is not given to the person from whom the information is collected,
    - one of the paragraphs in **section 34(1)(a)** to **(o)** must apply; or
    - the head of a public body must have decided that the direct collection requirement or the notification requirement could reasonably be expected to result in the collection of inaccurate information.
- The method of notification must be appropriate in the circumstances. Examples of different methods of notification include notice on a form, in a pamphlet or other publication, on a card or sign on a desk or counter, on a website, or in a pop-up notice on a computer screen. Oral notice can be given either in person or by recorded message.

For consideration

- Consider whether a client may need to refer to the information in the notice in the future or whether the program area may need to retain evidence of the notice that was given. In these cases, provide a copy of the notification to the individual from whom the personal information is collected and keep a copy of the notification on file.
- Consider providing notification even in cases where a public body is not required to do so (that is, in cases where the public body is authorized to collect personal information indirectly). For example,
    - In cases where a public body collects personal information indirectly for the purpose of a common or integrated program or service, consider notifying the client of the collection of his or her personal information by

the various public bodies that are involved in the delivery of the program or service, at the time a client registers in the program or requests the service.
    - In cases where a public body collects personal information indirectly for the purpose of determining the suitability of an individual for a scholarship or bursary, consider notifying the individual what information will be collected and from whom, at the time the individual applies for the scholarship or bursary.
- Consider the most appropriate methods of providing notification for collection of personal information by telephone or electronically. For oral collection, consider having a policy on providing notification (e.g. recording on client files that notice has been provided), and monitoring compliance.

Accuracy of personal information

Section 35(a) A public body must make every reasonable effort to ensure that personal information used to make a decision that affects an individual is accurate and complete.

What is required?

- A public body must have procedures in place that ensure that the accuracy and completeness of personal information is appropriate for the purpose for which the personal information is used. Some procedures that may assist are:
    - verifying the identity of an individual from whom personal information is collected (especially important when personal information is collected by telephone or electronically);
    - using validation processes for data within electronic systems;
    - providing for regular updating, if necessary, and recording when personal information in a record was last updated;
    - using the most reliable sources to update personal information and recording the source of the information;
    - allowing individuals to review their own personal information and request correction or annotation in case of errors or omissions.

Correction of personal information

Section 36 **Section 36** requires a public body to respond to requests for correction of personal information and to notify other public bodies, or third parties to which the information has been disclosed, about the request and about any correction or annotation that was made in response to the request.

What is required?

- Procedures must be in place to ensure that a public body can respond to a request by an individual for access to his or her own personal information and to a request for correction of that information. It should not normally be necessary for an individual to make an access request under the *FOIP Act* before requesting a correction of personal information.

- Procedures must in place so that notification of a correction or annotation of personal information can, if necessary, be sent to any other public body or third party to which the information has been disclosed during a one-year period prior to the request for the correction or annotation.
- A record of purpose must be maintained for any use or disclosure of personal information that is not included in the public body's Directory of Personal Information Banks. The record of the purpose for the disclosure must be either attached or linked to the personal information (**section 87.1(3)**).

Directories of personal information banks

Section 87.1 The head of a public body is responsible for maintaining and publishing a directory of its personal information banks, either in printed or electronic form. The directory of personal information banks must include

- the title and location of the personal information bank;
- a description of the kind of personal information and the categories of individuals whose personal information is included;
- the authority for collecting the personal information in the bank; and
- the purposes for which the personal information is collected or compiled and the purposes for which it is used or disclosed.

What is required?

- A public body must publish a directory of personal information banks that includes the elements listed in **section 87.1(2)**. The description of the personal information and the statement regarding the purposes for which the information is used or disclosed must provide sufficient detail to be meaningful to individuals whose information may be included in the personal information bank.
- The directory must be kept as current as is practicable, and access to the directory made available to the public at an office of the public body (**section 87.1(4)**).
- Each time personal information is used or disclosed for a purpose that is not included in the directory, a record of the new purpose must be kept and the record of that new purpose must be either attached or linked to the personal information (**section 87.1(3)(a)**).
- The new purpose(s) must be included in the next publication of the directory (**section 87.1(3)(b)**).

For consideration

The Act establishes minimum requirements for the directory. Public bodies may wish to consider including additional information, such as a list of the public body's information-sharing agreements and information about retention periods.

Retention of personal information

Section 35(b) **Section 35(b)** requires retention of personal information used to make a decision about an individual for one year from the date of last use in most cases.

What is required?

- Personal information must be retained for a least one year after it is used to make a decision affecting an individual (including a decision relating to a request under the *FOIP Act*). This requirement overrides any retention period in a public body's records retention and disposition schedule. For example, personal information used by a public body to determine an individual's eligibility for a program or service must be retained for one year after it is used, even if the public body's records retention schedule would normally require the information to be disposed of at an earlier date. The one-year period gives individuals an opportunity to request access to personal information used to make the decision, to ensure that it is accurate.
- If personal information is retained for a shorter period of time, there must be an agreement to that effect in writing between the individual, the public body and the body that approves the records retention and disposition schedule.

For consideration

- Records retention and disposition schedules should be in place for information in personal information banks and for the administrative or electronic systems in which they operate.

Protection of personal information

Section 38 A public body must make reasonable security arrangements for the protection of personal information against such risks as unauthorized access, collection, use, disclosure, and destruction. The basic attributes for a comprehensive security policy and practices are provided in section 9.5 of this chapter.

What is required?

A public body must have safeguards in place that are appropriate under the specific circumstances. The type and level of security measures will depend upon a range of factors, most importantly, the sensitivity of the personal information. The following are guidelines; these security arrangements may not be required in all circumstances.

- A public body should have a written security policy and procedures governing operations that involve personal information.
- There should be a responsible official who has authority for information security.
- There should be documented procedures for collecting, processing, accessing, transmitting, storing, and disposing of personal information.
- Security procedures should cover administrative, physical and technological security, including
    - a threat and risk management methodology;
    - a process for designating sensitive information;
    - a system of authorization and access procedures (e.g. identification cards, keys, codes, combinations, badges and system passwords), and the maintenance of control records for gaining access to sensitive personal information;

- controls over authorization to add, change and delete personal information in an electronic information system, and audit capacity;
- procedures to ensure that qualified personnel are involved in the maintenance of electronic systems in order to ensure configuration control of equipment, systems, networks, and the updating of operating procedures;
- procedures for ensuring communications security;
- procedures for personnel screening that are commensurate with the sensitivity of the personal information involved;
- controls that restrict use of personal information to the purposes for which the information has been collected and restrict access to those officials and employees who have a "need to know" the information (i.e. access is limited to the specific portions of the personal information needed for the function being performed);
- appropriate physical security measures, such as security access zones, locked rooms, storage cabinets, controlled positioning and access to computer terminals and faxes (to prevent random access), as well as checkout and secure transmission procedures for files;
- technological security measures appropriate to the nature of the personal information stored on a device and the type of device used (e.g. encryption and password protection for portable data devices); and
- secure disposal procedures for records and equipment commensurate with the level of sensitivity of the personal information and its vulnerability to compromise.

- There should be procedures for monitoring and reviewing the general effectiveness of security measures, including those relating to the protection of personal information.
- There should be written sanctions or consequences for contravention of security procedures and policies.

Use

Section 39 **Section 39** limits the purposes for which public bodies may use personal information.

What is required?

- The personal information in a system or program must be used only
  - for the purpose for which it was collected or for a use consistent with that purpose,
  - with the consent of the individual; the form of consent must be in accordance with **section 7** of the FOIP Regulation,
  - for a purpose for which information may be disclosed under **section 40**, **42** or **43** of the Act, or
  - in the case of personal information in the alumni records of post-secondary educational bodies, for the purposes of their own fund-raising activities; this use must be discontinued at the request of an individual whose personal information is being used in this way.

- The amount and type of personal information used must be limited to what is necessary for the public body to carry out its purpose in a reasonable manner.

Disclosure

Section 40 A public body may disclose personal information only in accordance with the provisions of **section 40**.

What is required?

- Any disclosure must be permitted by one of the provisions of **section 40(1)**, **section 40(2)** or **section 40(3)** of the Act.
- The amount and type of personal information disclosed must be limited to what is necessary for the public body to carry out its purpose in a reasonable manner.
- If disclosure is not permitted under **section 40(1), (2)** or **(3)** of the Act, persons or bodies outside the organizational unit that operates and uses the system or program must not have access to information in the system, program or personal information bank, either directly through electronic means or through receipt of hard copy, tapes, disks or other copies.

Research or statistical purposes

Section 42 A public body may disclose personal information for a research purpose only under specified conditions.

What is required?

- Access to personal information in individually identifiable form must be necessary to reasonably accomplish the purpose of the research, or the Information and Privacy Commissioner must have approved the research purpose.
- Any record linkage must not be harmful to the individuals the information is about.
- The benefits of the record linkage must clearly be the public interest.
- The researcher must have signed an agreement to comply with security and confidentiality conditions, to meet a schedule for the destruction of individual identifiers and to ensure that there is no subsequent use or disclosure of the information in individually identifiable form without express authorization.
- The agreement must meet the requirements set out in **section 9** of the FOIP Regulation.

All of the above requirements must be in place before personal information may be disclosed under **section 42**.

Data sharing and data matching

Data sharing and data matching involve the disclosure or comparison of personal information for an authorized purpose. These activities may involve public bodies only or public bodies and other organizations. The data sharing or matching may

occur through electronic or other forms of transmission and may consist of single transactions or programs that continue over a period of time. These activities are subject to the provisions of **Part 2** of the *FOIP Act*.

See section 9.7 of this chapter for definitions and a detailed discussion of data sharing and data matching. Also, see the *Guide for Developing Personal Information Sharing Agreements*, published by Access and Privacy, Service Alberta.

What is required?

- In any data sharing or data matching,
    - there must first be authority to collect the information under **section 33** and to collect information indirectly under **section 34**;
    - the uses must meet the requirements of **section 39**;
    - if a disclosure is for research purposes, the requirements of **section 42** or **43** must have been met.

If the above requirements are not met, the data sharing or matching may not be in compliance with **Part 2** of the *FOIP Act* and the public body must modify or discontinue this activity.

For consideration

- Consider notifying the individuals whose personal information may be the subject of data sharing or data matching at the time the information is collected.

9.2 Privacy Considerations when Planning New Programs, Administrative Practices or Information Systems

Public bodies should establish practices and procedures that take into consideration the requirements of Part 2 of the Act in the planning, design, development of specifications, and implementation of new or modified personal information systems, programs, administrative practices or legislation.

To ensure that privacy protection requirements, as set out in **Part 2** of the *FOIP Act*, are taken into account in the application of new technologies, or when an administrative practice or program is being developed or modified, public bodies may need to conduct a privacy impact assessment and submit it to the Information and Privacy Commissioner for review. The program official responsible for developing or implementing the new technology, administrative practice or program should develop a privacy impact assessment, as part of a development team that could include IT specialists, the FOIP Coordinator, the records manager, etc. The privacy impact assessment would be developed as part of the business needs analysis or project initiation stage of the project. See section 9.3 of this chapter for detailed information on how and when to conduct a privacy impact assessment and who to involve in its development.

Privacy and security measures should not be viewed as barriers to applying innovative technology. Rather, they are essential components of modern systems that serve to build public confidence in the use of technology. In the last decade, a number

of technologies have been specifically developed to be privacy-enhancing technologies. Technologies such as encryption, digital signatures, anonymous electronic cash and service delivery systems, and "pseudo-identification" can often enhance privacy at little or no extra cost to the program. These technologies may also have the advantage of providing more secure identification to reduce fraud, more secure networking to reduce losses from theft, and more secure payment systems to eliminate the administrative costs of cash transactions.

Systems development should take into consideration the privacy rights of individuals and the protection of personal information. This applies to all aspects of the management of information, including collection or compilation, controls on accuracy, use and disclosure, protection, and disposal. Privacy considerations should be integrated at the earliest stages of development of automated information systems to ensure that such systems meet legal and policy requirements.

9.3 Privacy Impact Assessments

A *privacy impact assessment* (PIA) is a process that assists public bodies in reviewing the impact that a new program, administrative process or practice, information system or legislation may have on individual privacy. The process is designed to ensure that the public body evaluates the project or initiative for technical compliance with the *FOIP Act* and also assesses the broader privacy implications for individuals. A PIA is both a due diligence exercise and a risk management tool. Although only real breaches of privacy contravene the privacy provisions of the *FOIP Act*, even the perception that privacy may not be adequately protected can seriously damage the reputation of a public body, as well as the public's confidence in a particular program or initiative.

The PIA process requires a thorough analysis of the potential impact of the initiative on privacy and a consideration of measures to mitigate or eliminate any negative impact. The PIA is an exercise in which the public body identifies and addresses privacy risks that may arise in the course of its operations. While PIAs are focused on specific projects, the process should also include an examination of organization-wide practices that could have an impact on privacy. Organizational privacy and security policies and procedures, or the lack of them, can be significant factors in the ability of the public body to ensure that privacy protection measures are available for specific projects.

A PIA provides documented assurance to the public body, to the Information and Privacy Commissioner and to the public that all privacy issues related to the initiative have been appropriately identified and addressed. Once the Office of the Information and Privacy Commissioner is satisfied that the public body has addressed the relevant considerations and is committed to the provision of the necessary level of privacy protection, the Commissioner or a staff member will accept the PIA. Acceptance is not approval. It merely reflects that Office's acceptance that the organization has made reasonable efforts to protect privacy.

When is a privacy impact assessment needed?

Public bodies that are custodians and therefore subject to the *Health Information Act* for health information in their custody or under their control, should note that there

are express requirements under the *Health Information Act* to conduct privacy impact assessments in certain situations. Some of the public bodies under the *FOIP Act* that are affected by those requirements are the Alberta Health Services Board and the department and Minister of Alberta Health and Wellness.

Privacy impact assessments are not mandatory under the *FOIP Act* but are recommended for major projects that involve the collection, use or disclosure of personal information. **Section 53(1)(f)** of the *FOIP Act* provides authority for the Commissioner to comment on the implications for freedom of information or for protection of privacy of proposed legislative schemes or programs of public bodies.

Public bodies should consider conducting a PIA when

- new data elements will be collected and added to an existing personal information database, or a new database is proposed;
- system access will be rolled out beyond current parameters, controls, levels or numbers of users;
- the use of personal information will be expanded to include data linkage or matching or other purposes;
- limited disclosure or reporting about selected individuals will be expanded to enable broad disclosure of information about a larger population base;
- the way in which the system is accessed, managed or secured from a technical or managerial perspective is changed significantly (e.g. use of internet technology);
- initiatives involving multiple public and/or private sector bodies that result in the compilation of personal information;
- management or security of the system is outsourced; or
- the retention period for personal information in the system will be changed.

As information systems become more complex, the probability of having an unexpected impact on privacy increases. Initiatives that appear to involve minor technical enhancements for client convenience and public body efficiency may significantly impact individual privacy.

The Office of the Corporate Chief Information Officer, Government of Alberta, is responsible for ensuring that government information and communications technology (ICT) projects, especially cross-government projects, comply with all applicable privacy legislation. The Office coordinates policy development, privacy impact assessment procedures and privacy architecture development for ICT in the Government of Alberta.

What is the process for a PIA?

Consider establishing a PIA development team

Determine which staff can best provide the information that is needed for the PIA. The team could include the FOIP Coordinator, the project or program sponsor, records manager, project manager, IT specialists, legal services, communications specialist and a senior or executive manager.

Identify someone to lead the process and write the PIA. Ideally, this would be someone who understands the *FOIP Act* and privacy principles and issues, has technical writing skills, has project management experience and can synthesize input from a variety of sources.

Consider when to start the process

If the PIA is viewed as an obstacle to the initiative being launched, it has been started too late. If decisions about the initiative are not firm, resources have not been committed and questions about privacy implications cannot be answered, it is too early to start the process.

According to the Office of the Information and Privacy Commissioner, the PIA is a dynamic document that should be updated from time to time as changes are contemplated for the program; it is rarely ever finished. Public bodies are expected to advise the Commissioner's Office of any changes or modifications to the program and to provide documentation so that the PIA on file is always up to date.

If the project is complex, a cross-government initiative, or involves a high volume of personal information, consider consulting with Access and Privacy, Service Alberta to provide input on project design.

Determine who will approve the PIA internally

The internal approval of a PIA should be based on the public body's established internal approval process and should include approval from the members of the PIA development team.

Consider whether public consultation is needed

It may be appropriate to consult with stakeholders or the broader public on major initiatives or on significant overhauls of existing programs. Focused public discussion conducted early in the process can help program or system designers anticipate public reaction to proposals or help to eliminate options that meet with significant resistance. The public body should address in the PIA how it intends to educate and consult with affected stakeholders respecting the proposed initiative. Alternatively, the justification for not consulting should be set out in the PIA.

Understand the role of the Office of the Information and Privacy Commissioner

To give the Commissioner's Office time to formally review and comment, public bodies should provide the PIA to the Office at least 45 working days before implementing the proposed new or changed practice or system. In practice, however, the role of the Commissioner's Office starts long before the formal review. The process for interaction with the Commissioner's Office is as follows:

- The public body (usually the FOIP Coordinator) advises the Commissioner's Office of the project well in advance of implementation.
- If necessary, the PIA development team meets with the staff of the Commissioner's Office to review the project and determine whether a PIA is required. The Commissioner's Office decides whether a PIA is advised and requests the public body to conduct one.

- If a PIA is required, it must be submitted to the Commissioner by the head of the public body.
- The PIA development team prepares the PIA by completing the PIA Questionnaire (published by the Office of the Information and Privacy Commissioner), with the necessary elaboration and enclosures and submits it (through the head) to the Commissioner. The FOIP Coordinator may send a working copy of the document to the staff of the Commissioner's Office prior to the head's submission.
- Questionnaire responses are reviewed by the Commissioner's Office and discussed with the PIA development team or its leader, as required. Further information may be requested, which could result in an extension to the optimal 30-day review period.
- Upon final acceptance by the Commissioner's Office, the head of the public body receives a letter of acceptance from the Commissioner.
- The PIA is filed in the library of the Commissioner's Office and is available for public review. Public access to some confidential information, such as details of sensitive security measures, is sometimes restricted. Any such restrictions are limited and specific.
- The public body provides updates to the PIA as changes to the project are implemented over time.

The Commissioner's Office may use the PIA as a starting point for any investigation into a breach of privacy.

The Office of the Information and Privacy Commissioner publishes a document on the PIA process called *Privacy Impact Assessment: Instructions and Annotated Questionnaire*. The Office also publishes a *Privacy Impact Assessment: Supplementary Organization Questionnaire* that is intended for use in projects involving more than one organization. These packages are available from the Commissioner's website at www.oipc.ab.ca, or by requesting a PIA package by contacting the Office (780- 422-6860; or toll free 1-888-878-4044).

Privacy impact assessment questionnaire

The PIA Questionnaire will be considered a public document by the Office of the Information and Privacy Commissioner. Any appendices or attachments will also be considered public documents unless they are explicitly designated as confidential. Examples of appendices would be an organizational strategic or business plan addressing privacy protection or physical or information security plans and access control documentation. Appendices that are designated as confidential must be accompanied by the reasons for the confidentiality.

The PIA Questionnaire must be submitted to the Commissioner with a covering letter from the head of the public body in order to receive a formal response.

For public bodies that are also custodians under the *Health Information Act*, there are statutory requirements for privacy impact assessments in sections 46, 64, 70, and 71 of that Act that must be complied with. Those bodies may use the same PIA

Questionnaire for conducting a PIA under the *Health Information Act* with a few modifications. (For more information on conducting PIAs for purposes of the *Health Information Act*, see Chapter 5, section 5.2.7 of the *Health Information Act Guidelines and Practices Manual*, published by Alberta Health and Wellness.)

The questionnaire is divided into two parts:

- Part A: Organizational Privacy Management; and
- Part B: Project Privacy Management.

Each part contains a series of questions. The checkboxes on the questionnaire provide for summary responses to the questions. The note fields provide for elaboration of the responses, as necessary. There is also a column that can be used to cross-reference separate enclosures. The questionnaire can be completed either in paper or electronic formats.

Part A: Organizational Privacy Management

This part of the questionnaire is intended to provide background on facets of privacy management across the public body which may affect the management of privacy issues for the specific project. If this information has been provided with a previous PIA and has not changed, it does not have to be resubmitted. One set of questions in Part A is designed to provide information, including documentation if available, from the public body about its privacy protection policies, controls and procedures. This would include such things as a privacy charter, policy or strategic plans relating to privacy protection and any procedures that have been developed with respect to information security, records management, disposition processes, need to know, etc.

The second set of questions deals with the structure and organization for dealing with security and privacy protection within the public body. This would include information on whether a position in the organization has been designated as responsible for privacy and security; the management reporting process for dealing with privacy compliance issues and training of new staff in privacy protection.

Part B: Project Privacy Management

In this part of the questionnaire, the public body provides information specific to the proposed project. The information requested includes

- a project description, including a listing of data elements to be collected, used or disclosed; an information flow diagram; and a listing of who will have access to the information;
- an analysis of the proposed information flows in relation to the rules in the governing privacy or other legislation regarding collection, use, disclosure, protection, accuracy, retention and disposition of personal information;
- a privacy risk assessment in which the public body identifies the privacy risks of the project and shows whether those risks have been successfully addressed through system design or policy measures or through other proposed options for mitigation. The residual risks that cannot be addressed through the proposed options should also be identified. Where possible, the likely implications of those risks in terms of public reaction and project success should be analyzed;

- a description and relevant documentation related to the privacy controls and security measures or procedures for the specific project; and
- the arrangements that have been made for audit, compliance and enforcement mechanisms for the proposed project, including information about how audits would be conducted and how any identified privacy issues would be addressed.

When the development of personal information systems is contracted out, the need to develop privacy impact assessments should be among the privacy requirements included in any management or operations contract governing the project and should be identified in the Request for Proposals or Tender documentation.

For more information, see *Managing Contracts under the FOIP Act: A Guide for Government of Alberta Contract Managers and FOIP Coordinators*, published by Access and Privacy, Service Alberta.

9.4 Reviewing Forms and Other Collection Instruments

Section 34(2) of the *FOIP Act* establishes a notification requirement for public bodies when collecting personal information. Public bodies must notify individuals whose information is being collected of the purpose for which personal information is being collected, the legal authority for the collection, and the title, business address and business telephone number of someone who can answer questions about the collection.

Forms are a common way of collecting personal information, so it is particularly important to ensure that paper and electronic forms comply with the requirements respecting collection and notification in **sections 33** and **34** of the Act. Compliance with these requirements

- supports the right of individuals to know what personal information public bodies collect about them and how this information is used;
- supports the right of individuals to access information about themselves; and
- helps maintain confidence among individuals that public bodies are protecting their personal information from unauthorized collection, use and disclosure.

As indicated in sections 7.1 and 7.2 of Chapter 7, ensuring compliance with **sections 33** and **34** of the Act requires ongoing review of a public body's collection activities. This review should include an assessment of all new forms used to collect information directly from individuals to ensure that the forms comply with the Act and that the public body is not collecting personal information without the legal authority to do so.

In cases where some personal information on a form should no longer be collected, public bodies should inform staff and clients that certain fields must not be filled out or staff should cross them out, where possible. These instructions should be provided in writing to staff. In some instances, it may be possible to black out fields that are no longer required.

A review of the collection of personal information should cover all collection instruments, including survey questionnaires in print or electronic form. For information on privacy protection when conducting surveys, see *Conducting Surveys: A Guide to Privacy Protection,* published by Access and Privacy, Service Alberta.

A review should also consider collection of personal information through the public body's website, and particularly in forms submitted from websites. For further information on developing privacy statements for websites, see the *Guide to Developing Privacy Statements for Government of Alberta Web Sites*, published by Access and Privacy, Service Alberta.

A review of forms and other collection instruments may be combined with the privacy compliance review, discussed in section 9.1 of this chapter.

Notification

The notification (collection notice) may be printed on the collection form itself, on a separate or covering document that explains the form and how to fill it out, or it may be given orally. Oral notification is practical when information is taken personally over the telephone or taken during an interview.

When the collection notice is provided orally, the individual may be provided with a copy of the notice, either at the office where collection takes place or with the documentation sent to an individual to confirm collection of information over the telephone or electronically.

An example of notification is as follows.

This personal information is being collected under the authority of [state Act or program mandate] *and will be used to* [state all of the known purposes]. *It will be treated in accordance with the privacy protection provisions of* ***Part 2*** *of the Freedom of Information and Protection of Privacy Act. If you have any questions about the collection, contact* [position, address, and business telephone number of responsible official or employee].

Optional practices

There are a number of practices for the collection of personal information through forms that reflect good management of personal information but are not mandatory under the *FOIP Act*.

Here are some best practices.

- Design forms to ensure that the individual from whom the information is collected is given a copy of the notification and that a copy of the notification is also retained by the public body;
- Design forms to place the collection notice either at the top of the form (before any personal information is collected) or just above the signature line, where practicable;
- Provide detailed notifications, where appropriate, to inform the individual about his or her right to request correction of inaccurate or incomplete information, the

right to appeal refusals of corrections and the role of the Information and Privacy Commissioner in reviewing such refusals;

- In consultation with the FOIP Coordinator or FOIP Office, conduct a central review of all new forms and proposed revisions before finalization for printing, including review of privacy issues; and
- Where personal information is collected from a source *other than the individual the information is about* (indirect collection), include provisions to inform individuals generally that information about them is being sought from a variety of specific sources. Such explanations should be included in documentation or brochures given to individuals who are the subjects of the indirect collection. They are also required in your personal information bank description. Notifying individuals about indirect collection may not be possible or practical in cases where the personal information collected is about the spouse, dependent or emergency contact of an applicant.

Collecting information on-line

When collection of personal information takes place in an electronic environment, public bodies should have the capacity to audit the public body's authority to collect the personal information, its manner of collection and its notification of collection and use. The following practices or other comparable audit practices should be in place.

- Establish a policy and accountability structure to ensure that electronic forms, which are often generated on a decentralized basis, include notification;
- When new forms software is under consideration, consider whether it permits the easy addition of notices in ways that are convenient and that effectively inform the individual filling out the electronic form of his or her privacy rights;
- Provision should be made for authorization of indirect collection and for authorization of additional uses or disclosures of the information on electronic forms where this is appropriate, as well as for a signature or other verification of the identity of the individual providing the authorization;
- If necessary and practicable, a hard copy of the form should be provided to the individual the information is about, including the collection notice on the form; and
- The public body should be able to retain a copy of the notice and authorization, if applicable.

9.5 Developing a Security Policy

Section 38 of the Act requires a public body to protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.

Reasonable security arrangements are usually practices and procedures expressed through a security policy approved for use within a public body. This policy should be based on a threat and risk assessment of the information and assets in the custody or under the control of a public body, and include physical, administrative and technological security.

Public bodies that are also custodians under the *Health Information Act* must comply with section 60 of the *Health Information Act* and section 8 of the Health Information Regulation in order to ensure that the privacy of individuals and the confidentiality of their health information is protected. For more information about developing a health information security policy, see Chapter 11, section 11.3.4 of the *Health Information Act Guidelines and Practices Manual*, published by Alberta Health and Wellness.

Government of Alberta departments should refer to the *Information Technology Security Policy* and the *Policy for the Transmission of Personal Information Via Electronic Mail and Facsimile*, produced by the Office of the Corporate Chief Information Officer, Government of Alberta.

The Office of the Information and Privacy Commissioner has also produced a document entitled *Information Security Plan*, which is Appendix 1 to the *Privacy Impact Assessment: Instructions and Annotated Questionnaire*, produced by that Office. In its *Security Plan*, the Office of the Information and Privacy Commissioner recommends that the following policies outlining end-user responsibilities relative to the computing environment be developed:

- computer usage policy and guidelines;
- e-mail policy and guidelines; and
- internet policy and guidelines.

Government of Alberta departments and agencies should refer to the *Internet and E-mail Use Policy*, available on the Corporate Human Resources website, and *Managing Electronic Mail in the Government of Alberta*, published by Records and Information Management, Service Alberta. Public bodies should also consider policies related to the use of wireless technology.

Basic attributes of a comprehensive security policy

Many organizations have security policies that apply to specific security issues, such as access to classified information, administrative security or information technology security. A more comprehensive approach to security administration, including all aspects of physical, administrative and technological security, is both necessary and practical.

The sharing and use of personal information by a number of public bodies creates an additional challenge. The Act requires reasonable protective measures for such information, but this will now require more consistency among public bodies in how they handle and protect such information. Being able to compare protective measures among public bodies doing public business with each other is essential.

Authority

A security policy should contain a statement of the authority or authorities under which the security policy is being issued and a direction from the senior officer of the public body on its effective implementation.

What needs to be safeguarded

All assets of a public body, including information, require good basic care. Some assets, however, are more sensitive or valuable and require additional safeguards. A security policy should include a requirement to carefully identify sensitive information, valuable assets and information systems that may need additional safeguards.

Sensitive information

Certain information must be withheld from access under the *FOIP Act* because it would reveal particular sensitive information or pose possible injury to public or private interests. These categories of information are described in the exceptions to access in **sections 16** to **28** of the Act. Public bodies should take greater care in protecting these categories of information than they would information that is generally available to the public.

Among these categories is personal information. The Act defines personal information in **section 1(n)**, and **section 17** provides guidance as to what may be an unreasonable invasion of personal privacy. **Section 17** is considered in detail in section 4.3 of Chapter 4 of this publication. The categories in **section 17** help to identify sensitive personal information that may need safeguards. Health information, financial information, pay and benefits information, and criminal records are particularly sensitive and require special protection.

Threat and risk assessments

The security policy should require a threat and risk assessment to be conducted. This should include identification of what information is likely to require safeguards and an assessment of threats and risks to the information and information systems. This analysis provides the basis for assigning safeguards at a level commensurate with the risk. The security measures can be monitored and adjusted over time. To assist in the threat and risk assessment process, the security policy should

- require program areas to maintain complete and up-to-date inventories of personal information and personal information systems; and
- provide for the review of potential threats (e.g. how could sensitive personal information be lost or changed?, what impact would this have on client confidence in the programs?, who would be affected and how?).

The Government of Alberta's *Information Technology Security Policy* requires all information systems to be given a risk classification (scaled from no-risk to critical applications) depending upon the nature and use of the system. Critical applications need to be included in business continuity plans and to have the most stringent security mechanisms in place for protection.

See section 9.6 of this chapter for more detailed information on conducting threat and risk assessments.

Types of safeguards

Administrative safeguards. Examples of administrative safeguards include:

- designating a position that has overall responsibility for security within the public body;
- ensuring that staff understand their responsibilities and the public body's security procedures by providing them with written procedures and instituting training programs;
- arranging to resume operations in the case of loss of computer-based data or capabilities;
- checking the references and background of an officer or employee to ensure that he or she is a suitable person to have access to sensitive information, information systems and the facilities where they are located;
- implementing the "need-to-know" principle where access to particular information or systems can be limited to certain officers and employees who have a need for such access because it is necessary to perform their duties;
- conducting process audits and periodically reviewing access logs, etc.; and
- establishing sanctions for breaches of the security policy and a process for reporting and investigating breaches.

Physical safeguards. Examples of physical safeguards include:

- periodic reviews of physical security features, such as alarms, fences, and codes for cipher locks;
- use of physical barriers, security zones, access and authorization mechanisms, and locked containers to restrict access;
- use of proper containers and procedures for the secure processing, storage, transmission and disposal of information and other assets;
- specifying adequate fire and fire safety procedures; and
- designating off-site storage facilities with a similar level of physical and environmental security.

Technological safeguards. The security of computer and telecommunications equipment and systems requires special consideration. This is partly because of the need to protect sensitive information, such as certain categories of personal information, and because of the significant extent to which many public body operations and services are dependent on information technology.

In addition to protecting the confidentiality of the information in these systems, it is necessary to protect the integrity and availability of a public body's information technology systems. Defining the importance of the availability of information and services is the first step in making plans to resume business within acceptable time and resource limits in the event of loss of data, programs or systems.

Also important is the identification of potentially vulnerable communications systems. The risk of someone overhearing sensitive personal information on the telephone or through a data line should not be neglected, given the ease of such

access. Facsimile machines warrant special attention because of the chance of misdirecting sensitive information through an error in transmission and because they are generally accessible to anyone in an office area.

Examples of technological safeguards include:

- using software, hardware or operating system access controls such as passwords, termination on inactivity, clearance of display screens, transaction logs and error logs;
- using secure communications and encryption, especially for mobile devices such as laptops;
- providing adequate virus protection for new and existing computer equipment;
- establishing security controls for remote access to information systems;
- restricting the use of less secure forms of communications (e.g. cellular telephones); and
- conducting audit checks of data and system integrity, and establishing procedures for database recovery and back-up.

Breaches, sanctions and review

A security policy should establish what are considered to be breaches of security and should require that all breaches be reported to the chief officer of the public body.

A security breach is an unauthorized access to or collection, use, disclosure or disposition of personal information. A breach may be accidental or intentional.

The security policy should state how an investigation into a breach of security would be conducted. The policy should also set out any administrative or disciplinary sanctions that will be applied if a breach is found. Sanctions may consist of the removal of access to sensitive information or information systems, verbal or written reprimand, suspension without pay, or dismissal. The sanction will depend on the policies of the public body, the circumstances and the record of the officer or employee.

Sections 92(1) and **92(2)** of the *FOIP Act* provide that a person must not collect, use or disclose personal information, or attempt to gain or gain access to personal information in contravention of the Act. A person who does so is guilty of an offence and liable of a fine up to $10,000 (see sections 2.10 and 2.11 of Chapter 2 of this publication for a further discussion of liability, offences and penalties).

A security policy should ensure a fair and equitable process for dealing with individuals who have consented to personnel security checks or are subject to disciplinary action related to security. A clear process for appeal and review should be put in place.

Security in contracting

Protective arrangements under **Part 2** of the Act apply to personal information in the custody or under the control of public bodies. This may include information that is collected, compiled, used, disclosed or disposed of by a contractor. A security policy should state that its provisions apply to persons working under contract to a public

body when they are required to handle sensitive personal information or have access to information systems or facilities where such information is handled or stored. The physical, technological and administrative security requirements for individual contracts will have to be decided on a case-by-case basis.

A security policy should also include a process for determining the conditions under which the processing or storage of personal information can be outsourced. Special consideration should be given where the personal information is sensitive in nature, or where the contractor is located outside Alberta or Canada.

For information on establishing security and other requirements during the contracting process, see *Managing Contracts under the FOIP Act: A Guide for Government of Alberta Contract Managers and FOIP Coordinators*, published by Access and Privacy, Service Alberta, and *Public-Sector Outsourcing and Risks to Privacy*, from the Office of the Information and Privacy Commissioner.

9.6 Conducting Threat and Risk Assessments

While no system, including an information technology system, can be made absolutely secure, it is possible to manage the impact of threats to business processes and to individual privacy. This is done through development of security management processes to reduce, transfer, avoid or accept risks. The senior management of a public body must find an appropriate balance between the potential threats and risks and the cost of protection. To properly identify those risks, threat and risk assessments should be undertaken for the personal and other sensitive or confidential information in the custody or under the control of a public body.

In Government of Alberta departments, Chief Information Officers are responsible for initiating appropriate threat and risk assessments prior to the approval of design specifications for new information systems, whenever a significant change occurs to the systems, or on a yearly basis. If a new system or program or an enhancement to an existing system or program deals with the collection, use or disclosure of personal information, a privacy impact assessment may be necessary (or required, for public bodies that are also custodians under the *Health Information Act*). In other public bodies, the person responsible for information security could adopt the same approach as that of government departments regarding when threat and risk assessments should be initiated.

The threat and risk assessment process should be flexible enough to be able to recognize new risks as they arise. Current threats may need to be re-evaluated and potential or anticipated threats identified as the nature of the information in the custody or under the control of a public body changes.

For information regarding the development of a comprehensive security policy, see section 9.5 of this chapter.

Components of a threat and risk assessment

Determine what needs to be protected and what level of protection is required

Information in the custody or under the control of a public body should be grouped according to the function, process, program or service it supports. Within each group, determine the requirements that the information may have for its protection. All the

data elements or information, software, users, administrators, analysts, storage facilities, storage media, system documentation, etc. should be listed.

Define the threats to protect against

For each grouping of personal or other sensitive information,

- identify the potential agents or events that could place the information at risk (e.g. theft, unauthorized access, viruses, power loss, etc.);
- classify each agent or event by the type of threat;
- determine the likelihood that the event may occur; and
- identify the potential consequences and rate the impact of the event if it were to occur.

Threats to the security of information may be

- *a threat to the confidentiality of information*, where information is made available or disclosed to unauthorized individuals, entities or processes;
- *a threat to the integrity of information*, where data and information technology systems are altered or destroyed from their intended form in an unintentional or unauthorized manner; and
- *a threat to availability of information*, where information is not consistently retrievable to enable public bodies to meet their business and legal obligations (e.g. under the *FOIP Act*'s access to information provisions).

Some examples of these threats are:

- unauthorized access to a database as a result of an error in the way access controls have been configured – this may affect the confidentiality, integrity and availability of information;
- malicious code being inserted by a disgruntled or misguided employee into a network – this may affect the confidentiality, integrity and availability of information;
- unauthorized access to a database as a result of password interception, cracking or network/operating system vulnerability – this may affect the confidentiality, integrity and availability of the information;
- unauthorized access to information as a result of verbal disclosure by an employee, leaving information where it can be viewed by unauthorized persons, electronic interception of information from a fax line or cellular phone, faxing or e-mailing information to the wrong fax number or e-mail address.
- access by an unauthorized individual to information stored on an employee's or contractor's home or laptop computer – any of these occurrences may affect the confidentiality and integrity of the information;
- service interruption as a result of a power failure, labour dispute, or denial of service attack on an Internet server or provider – this may affect the availability of information;

- accidental or deliberate loss of data as a result of physical damage to hardware, wilful destruction of recorded information, information destroyed in a flood or fire – this may affect the availability of information;
- removal of equipment, such as theft of a laptop or file containing sensitive information – this may affect the confidentiality, integrity and availability of information; and
- records being misdirected or misfiled, or destroyed in a manner that is not in accordance with approved records retention and disposition schedules or policies – this may affect the confidentiality and availability of information.

Estimate the likelihood of the threat scenario occurring and the potential impact or injury that could result

Public bodies should determine the likelihood (low, medium or high) of each or any of the above threats occurring. Then, the potential consequences of the events need to be identified and their seriousness rated. Some of the potential harms would be

- litigation;
- loss of trust by clients;
- loss or delay of service;
- loss of confidentiality;
- cost of notifying affected individuals; and
- cost of system repair.

Assess whether current or proposed security measures are appropriate to reduce the risk

Given the potential threats to the information that have been identified and the likelihood and impact of an event occurring that would place each group of personal or other sensitive information at risk, public bodies should assess the adequacy of existing safeguards and current resources to protect against those potential threats.

This assessment involves listing the existing safeguards that protect against the threat or event, considering whether the information might still be vulnerable and rating the risk. A low risk will require some attention and consideration for safeguard implementation. Moderate risk requires attention and safeguard implementation in the near future. A high risk requires immediate attention and immediate safeguard implementation.

Identify how to manage the residual risk after implementing safeguards

Identify any additional safeguards recommended to lower the risk to an acceptable level and describe the proposed measures or safeguards. Different safeguards provide different levels of protection. Selection of the most appropriate safeguard will depend upon the availability of resources and the acceptable level of risk. Implementing some safeguards to lower the projected risk level may, in some cases, not be practical because of technical or physical limitations or because of time or financial constraints.

9.7 Privacy Considerations for Data Sharing and Data Matching

Data sharing

Data sharing refers to one public body collecting information from or disclosing information to another public body or other organization for such purposes as

- determining or verifying the eligibility of a client for a program, benefit or service;
- detecting duplicate payment of benefits from two public bodies;
- determining an individual's suitability for an honour or award; and
- delivering a joint program.

There are no specific controls over data sharing in **Part 2** of the *FOIP Act*. However, the collection, use and disclosure provisions of the Act govern how such activities can be carried out and the Information and Privacy Commissioner may comment on the privacy implications of the proposed data sharing (**section 53(1)(g)**).

When a public body determines that sharing some of the personal information it holds is necessary, and the sharing is authorized under the disclosure provisions of the *FOIP Act*, this should be supported by a written personal information sharing agreement.

Using a personal information sharing agreement to establish the terms and conditions that will apply to a transfer of personal information has the benefit of

- providing a formal mechanism for the efficient and timely sharing of personal information;
- limiting the type and amount of personal information that will be disclosed and the purposes for which it will be used; and
- providing additional privacy protection, both during and after the sharing, by binding the parties to enforceable terms and conditions.

For further information on data sharing, including the components of a personal information sharing agreement, see the *Guide to Developing Personal Information Sharing Agreements*, published by Access and Privacy, Service Alberta.

Data matching

Data matching means the comparison (often by computer) of one or more databases or sets of records of personal information held by one public body or organization with one or more other databases or sets of records held by a different public body or organization, where the computer matching program creates or merges files on identifiable individuals, and where the matched data is used to make decisions about the individuals to whom the data relates. Data matching tends to involve electronic data because its effectiveness is generally based on the comparison of databases containing large volumes of transactional data.

Related to data matching is *data linkage*, also known as *data profiling*, which is a computerized use of personal information from a variety of sources, including

personal information banks, to merge and compare files on identifiable individuals or categories of individuals for administrative purposes. This linkage or profiling activity generates a new body of personal information.

Data matching and data linkage may have a valuable role to play in increasing the efficiency of a wide variety of public body programs. They can, however, also have a major impact on the privacy of individuals. For this reason, there is a need to balance the requirements for efficiency in public body programs with the potentially invasive nature of the activity, particularly data linkage. Careful attention needs to be given to the quality and reliability of the data being matched or linked, especially if the purpose of the activity is to pursue administrative actions against individuals.

Public bodies that are custodians under the *Health Information Act* must comply with relevant sections of that Act when they are considering any data matching activities. A custodian cannot collect health information to be used in data matching, or use or disclose health information to be used in data matching or created through data matching in contravention of the *Health Information Act*. For example, there are specific requirements in that Act for privacy impact assessments when a custodian is performing data matching by combining information in its custody or under its control with information in the custody or under the control of another custodian or a non-custodian.

Public bodies that are custodians under the *Health Information Act* may refer to sections 5.4 and 5.2.7 of Chapter 5 of the *Health Information Act Guidelines and Practices Manual*, published by Alberta Health and Wellness, for more information on the rules for data matching as they apply to health information in the custody or under the control of custodians.

When carrying out data matching, public bodies should

- determine whether the collection, use and disclosure of the personal information that is the subject of the data matching is permitted by provisions of **Part 2** of the *FOIP Act*;
- prior to initiating a matching program, conduct a preliminary assessment of the feasibility of the proposed matching, including the potential impact on the privacy of individuals and the costs and benefits of the data matching program;
- notify the Information and Privacy Commissioner of a new matching program by providing that Office with a copy of this assessment at least 60 days before the program is to commence;
- ensure that data matching programs are authorized by the head of the public body or the designated official to whom this authority has been delegated;
- ensure that all matching activities are accounted for in relevant personal information bank descriptions; and
- verify information generated by a matching program against original or additional authoritative sources before that information is used for an administrative purpose.

Public bodies that are not custodians do not need to conduct a preliminary assessment or send the assessment to the Commissioner if the matching involves

- information not used for an administrative purpose directly affecting an individual;
- two or more databases of information collected and held by the same public body for the same purpose;
- programs that review the contents of a records system to remove or correct items where there is no intention to take administrative action;
- programs that co-locate items previously in separate locations, provided the purposes for which the information collected or compiled continue to apply; or
- information used for research, statistical or program evaluation purposes, if the output is in a form that is not individually identifying, provided **section 42** has been complied with.

Preliminary assessment

When considering a data matching program, a preliminary assessment should be carried out to determine whether matching data is the most practical and convenient approach to the need and whether there is a basis for proceeding in **Part 2** of the *FOIP Act*. The following are the steps for preliminary assessment of a matching program.

- Assess the advantages of the proposed matching program against alternative control, management or enforcement approaches.
- Verify that the collection involved in a matching program is authorized by a statute or regulation of Alberta or Canada, is for the purpose of law enforcement, or relates directly to and is necessary for an operating program or activity of a public body (**section 33**).
- Examine the possibility of collecting the information directly from the individual to whom it relates or whether collection through data matching is permissible under the *FOIP Act*. Indirect collection is permitted if the individual has authorized indirect collection, the public body could obtain the information from another source without the consent of the individual under **section 34(1)**, or direct collection might result in the collection of inaccurate information (**section 34(3)**).
- Determine whether it is necessary to notify individuals of the new use of their personal information, and if so, the best procedures for notification, or if not, the justification for not notifying the individual (**section 34(2)**).
- Describe the means for ensuring that the information used in the matching program, as well as the information generated, is accurate and complete (**section 35**).
- Determine whether the consent of individuals to the use or disclosure of their personal information is required, and if so, the procedures for obtaining any required consent, or if not, the reason for not obtaining consent (**section 40(1)(d)**).
- Determine whether there is other authority for the use or disclosure of the personal information under **section 39** or **40**.
- Set the start and completion dates for the matching program and, where applicable, the schedule for any required periodic or continuing matching programs.

- Describe the results of any pilot projects designed to test the proposed matching programs (whenever possible, matching public bodies should test the programs to evaluate their effectiveness).
- Determine the costs and the benefits of the proposed data-matching program.

At this stage, the public body should also determine the procedures available to

- establish a records retention and disposition schedule for information used in matching programs, including the program protocols used to establish the link between sets of personal information;
- ensure that any new use or disclosure of personal information is included in the directory of personal information banks held by the public body; and
- establish a personal information bank for the personal information generated as a result of the matching program.

Cost–benefit analysis

A second step is a basic cost–benefit analysis. Public bodies should determine the costs of a matching program relative to its benefits. This analysis should be in terms of the level of a public body's resources (e.g. staff, equipment and materials needed to perform a matching program) and the amount of effort required to develop and to implement it. The importance of the cost–benefit factor to the decision to proceed with a matching program will vary with the context in which the public body operates. Projected or actual resource expenditures should be examined in relation to direct costs, data processing and telecommunications costs, administrative overhead, and any costs associated with contracting out activities.

The cost–benefit analysis should quantify and document the following savings, as appropriate:

- funds that may be recouped through voluntary repayments or formal collection action;
- savings due to termination of ineligible benefits;
- savings due to the denial of benefits that would otherwise have been approved;
- savings due to the deterrent effect of the program; and
- savings relative to other methods of data collection or compilation.

It may be appropriate in some instances to provide evidence of a substantive impact on society or the economy that would result if the program were not implemented.

Notification of the Information and Privacy Commissioner

As a third step, public bodies should consult with the Office of the Information and Privacy Commissioner on data matching projects. To allow for this external review before implementation, public bodies should give the Information and Privacy Commissioner advance notification of their intention to initiate a matching program. Providing the Commissioner's Office with the preliminary feasibility assessment may serve this purpose.

A reasonable time frame for such notification is at least 60 days before the matching is scheduled to begin. This ensures that the Office of the Information and Privacy Commissioner is informed of new consistent uses and new data matches. After the review, the Commissioner may advise the head of the public body that, in his or her opinion, the uses or activities are not in accordance with the provisions of the *FOIP Act*.

Approval

A fourth step is to get final approval for the matching activity or program within the public body that is the matching recipient. It is recommended that the final approval for a data matching program be given by the head of the public body undertaking the program or by a senior official specifically delegated under the *FOIP Act* to authorize such programs.

When a public body is frequently involved in matching activities and the size and organization of the body merit it, the head may establish an internal review body. This might consist of senior program officials, information management or information technology staff and the FOIP Coordinator. The group would review proposed matching programs for compliance with **Part 2** of the *FOIP Act* and make recommendations to the head concerning matching programs for which the public body is either the matching recipient or the matching source.

Public notification of a matching program

The *FOIP Act* requires that a public body account publicly for the use and disclosure of personal information. One way to do this effectively is to notify the general public, or specific groups of clients, of a matching program. The inclusion of current, accurate information about all ongoing data matching activities in the directories of personal information banks held by public bodies is an effective way of providing public notification.

Special conditions relating to the disclosure of information for matching programs

When a public body is asked to disclose personal information for data matching purposes (a matching source), there are a number of factors that must be taken into consideration. Disclosure of personal information requested for matching purposes can only be made under the conditions set out in **Part 2** of the *FOIP Act*.

The public body disclosing the information should

- request and review the preliminary assessment and any other available documentation on the proposed matching to assist in making an informed judgment as to whether the proposed match is justified by program needs as well as the requirements of the Act. The public body must be able to demonstrate that it can disclose the information under **section 40** of the Act;
- determine whether additional information or action will be required for verification purposes and whether such disclosure or action is acceptable;
- ensure that when a disclosure is made for matching purposes, it is sanctioned by a written agreement signed by senior officials representing both the matching

source and the matching recipient. The agreement should include any further conditions that should apply; and

- ensure that any contract involving a matching program stipulates that the contracted activities will be conducted in accordance with the provisions of the *FOIP Act* and the public body's policy on data matching.

Verification process

It is a good administrative practice for public bodies to subject information generated by a matching program to a verification process involving original or additional authoritative sources. This verification process should be carried out before the information is used in decision-making that directly affects an individual. Furthermore, an individual should be given an opportunity to refute the information produced by a matching program before any administrative action concerning the individual is taken.

Security

Personal information and computer systems should be safeguarded from accidental and deliberate threats to confidentiality and to data integrity, including authenticity, accuracy, currency, and completeness. Security safeguards implemented by the matching recipient should be at least equivalent to those of the matching source.

Retention and disposition

A matching recipient should establish retention and disposition standards for personal information used and generated by a matching program. These standards are established through records retention and disposition schedules or agreements.