

Privacy Impact Assessment: Instructions and Annotated Questionnaire

Office of the Information and Privacy Commissioner Alberta, Canada

Introduction

This document is one of three or four documents in the Privacy Impact Assessment (PIA) package that you have received. The following is the list of documents in the package, whether you received them electronically or as hardcopy:

- 1) Questionnaire Instructions (this document)
- 2) Full Questionnaire
- 3) Supplementary Organization Questionnaire
- 4) README file (electronic package only)

If all these documents were not included in your package, please go to the Alberta Information and Privacy Commissioner's web site at www.oipc.ab.ca to download them. Alternatively, you may e-mail a request to ipcab@planet.eon.net or telephone 780-422-6860.

The PIA questionnaire may be reviewed periodically, but will not be changed between such reviews. The instructions, however, are revised as necessary to incorporate responses to frequently asked questions and to address new issues. This is especially the case for the annotations to the questionnaire, which appear later in this document. We recommend that you check the web site for a new version of the questionnaire instructions before each new PIA is begun. This will ensure that each PIA begins with current information about the PIA process.

Alberta's *Freedom of Information and Protection of Privacy* (FOIP) Act provides the authority for the Information and Privacy Commissioner to "*comment on the implications for freedom of information or for protection of privacy of proposed legislative schemes or programs of public bodies*" (section 51(1)(f)). Privacy impact assessments are not mandatory under the FOIP Act, but are recommended for major projects¹ that involve the collection, use or disclosure of personal information.

Alberta's *Health Information Act* (HIA) requires that the Information and Privacy Commissioner receive a privacy impact assessment for "*review and comment*" before a custodian implements "*proposed administrative practices and information systems relating to the collection, use or disclosure of individually identifying health information*" (section 64).

¹ Throughout this document and the accompanying questionnaires, the term 'project' is used for the sake of brevity. The term 'project' is intended to subsume the words 'scheme', 'program', 'initiative', 'application' and 'system', as well as any other word or term that refers to a defined course of endeavour.

Privacy impact assessments are mandatory under the HIA, if the project fits the foregoing definition.

The Office of the Information and Privacy Commissioner has developed the Privacy Impact Assessment (PIA) process to assist public bodies in reviewing the impact that the new project may have on the individual privacy. The process is designed to ensure that the public body evaluates the program or scheme to ensure compliance with Part 2 of the *Freedom of Information and Protection of Privacy Act* and Section 64 of the *Health Information Act*.

Organizations² that are or will be subject to the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) can also use the PIA questionnaire to assist with internal privacy reviews, but the Alberta Information and Privacy Commissioner does not review PIA's prepared for compliance with PIPEDA. Alberta's Commissioner has no authority in PIPEDA matters. Those who require further information about conducting PIA's in the PIPEDA context should contact the office of the [Privacy Commissioner of Canada](#).

The PIA process requires a thorough analysis of potential impacts on privacy and a consideration of measures to mitigate or eliminate any such impacts. The privacy impact assessment is a due diligence exercise, in which the organization identifies and addresses potential privacy risks that may occur in the course of its operations. While PIA's are focussed on specific projects, the process should also include an examination of organization-wide practices that could have an impact on privacy. Organizational privacy policy and procedures, or the lack of them, can be significant factors in the ability of the public body to ensure that privacy protecting measures are available for specific projects.

Because the onus always remains on the public body to ensure adequate levels of privacy protection, as required in the applicable legislation, the Commissioner will not "approve" a PIA submitted to him by an organization. Once satisfied that the organization has addressed the relevant considerations and is committed to the provision of the necessary level of privacy protection, the Commissioner will "accept" the PIA. Acceptance is not approval; it merely reflects the Commissioner's acceptance that the organization has made reasonable efforts to protect privacy. A PIA cannot be used to obtain a waiver of, or relaxation from, any requirement of the relevant legislation.

The Commissioner will use the PIA process to ensure that the project sponsor has assessed the privacy implications of any new program or scheme and possesses the legal authority to proceed with the project. The Commissioner may comment after reviewing the PIA, if it is found that legislative authority is unclear or missing, or that impacts on privacy are significant and unmitigated, or that the risks to privacy outweigh the benefits of the program or scheme. If the Commissioner provides comments to the organization, it will be up to the organization to accept the comments and provide clarification or proceed without further review by IPC. The Commissioner may also comment publicly on the project, if he considers such comment to be appropriate.

² Throughout this document and the accompanying questionnaires, the term 'organization' is used to refer to a public body under the *Freedom of Information and Protection of Privacy Act* or a custodian under the *Health Information Act*. When appropriate, it may also refer to an affiliate under the *Health Information Act*.

The Privacy Impact Assessment process is as follows:

1. The organization advises the Office of the Information and Privacy Commissioner (IPC) of the project to be undertaken.
2. If necessary, the organization meets with IPC staff to determine if a PIA is required. The Commissioner decides if a PIA is required. If NO, the process is concluded. If YES, the organization is advised that a Privacy Impact Assessment is requested.
3. If a PIA is required, it must be submitted to the Commissioner by the Head of the organization (if the organization is governed by the FOIP Act) or by the chief executive officer of the organization (if the organization is governed by the *Health Information Act*).
4. The organization prepares the PIA by completing the PIA questionnaire, with the necessary elaboration and enclosures, and submits it from the Head or CEO to the Commissioner.
5. Questionnaire responses are reviewed by the OIPC within 30 working days and discussed with the organization as required. Further information may be requested, in which case the review period may exceed 30 working days.
6. Upon final acceptance by the IPC, the organization receives a letter of acceptance from the Commissioner. This letter also advises of any future activity from the IPC office.
7. The PIA is filed in the office of the IPC 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, in keeping with FOIP Act exceptions to disclosure.)
8. The organization provides updates to the PIA as changes to the project are implemented over time.

On occasion, the Commissioner will use the expertise of outside individuals to assist in the review of a Privacy Impact Assessment. This will usually occur when the project is very complex or the personal information being discussed is very sensitive. Public bodies should be aware that if this process is used, the time frame for the Commissioner's comments will be extended.

It is the view of the Office of the Information and Privacy Commissioner that a Privacy Impact Assessment is rarely ever finished. It is a dynamic document that should be updated from time to time as changes are contemplated for the program. It is expected that an organization will advise the Commissioner's Office of any changes or modifications of the program and provide documentation so that the assessment on file is always up to date.

The Information and Privacy Commissioner may utilize the privacy impact assessment as a starting point for any investigation into a breach of privacy.

Questionnaire Instructions

The questionnaire requests information of two general types: that related to organizational privacy management and that related to privacy management specifically for the proposed project. The organizational privacy management section is intended to provide background on organization-wide facets of privacy management that may affect the management of privacy issues for the specific project. The project management section provides information specific to the proposed project.

The questionnaire provides for responses in two forms. Checkboxes provide summary responses to the questions posed. Note fields provide for the elaboration of those responses as necessary. The questionnaire also has a column to provide for cross-references to separate enclosures. Note fields and enclosures may be used in combination or interchangeably - either approach is equally acceptable.

The questionnaire can be completed as a paper form or as an electronic form using Microsoft Word 97 or later. If used as a paper form, elaboration and notes are best provided as separate enclosures. If used as an electronic form, the "Note/Elaboration" field for each question will expand to hold as much text as necessary. You can either type directly into these fields or cut and paste text from other documents into them. Note that you will have little control over formatting; the fields are pre-formatted for review by the Commissioner's office. The electronic form displays response fields with grey backgrounds.

When you open the electronic form, you may get a message warning that the form contains macros and asking if you wish to enable them. The form will only function properly with macros enabled. **If you received the PIA questionnaire from any source other than the Office of the Information and Privacy Commissioner, you are advised to scan it for macro viruses before opening it.** Your information technology staff will be able to advise you further in this regard.

More detailed information about installing and using the electronic forms can be found in the README.TXT file that is included with the download package.

Whether provided in the note fields or in separate enclosures, the elaboration of checkbox responses is important to ensure the review and acceptance of the PIA within a reasonable time. Checkbox responses that lack any elaboration will be more likely to raise additional questions at the time of review than responses for which appropriate elaboration has been provided initially. Elaboration need not necessarily be extensive. Brief elaborations that are to the point will often be as informative as lengthy elaborations that are less focussed. Please ensure that, as much as possible, elaborations are limited to the question to which they respond.

Nevertheless, feel free to provide as much elaboration as necessary to respond to the questions posed. You may provide any additional information that is relevant to the management of privacy in the organization as a whole or the specific project, as appropriate. Any and all relevant information provided will be considered in the review.

	QUESTION	Yes	Yes and No (partial, incomplete, in preparation, etc.)	No	N/A	Encl. Ref.
A: Organizational Privacy Management						
A1a	Has organizational privacy management information for questions A2 through A7 previously been provided with another PIA?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Note/Elaboration:

Question number

Check in this column if your response is a firm "Yes" with little or no qualification.

Check in this column if your response is neither a firm "Yes" nor a firm "No". Be sure to provide elaboration of any responses in this column.

Check in this column if your response is a firm "No" with little or no qualification.

Check in this column if the question is **not applicable** to your organization or project, or if the requested information is **not available**. Be sure to provide elaboration of any responses in this column.

"Enclosure Reference": a number or other reference that identifies a separate enclosure or part of an enclosure. Whenever you provide an enclosure, please also provide an enclosure reference.

If you are using the electronic form, this field will appear with a grey background. It will expand to hold unlimited explanatory text. If you are using the paper form, please use separate enclosures.

Suggested Enclosures

The inclusion of these enclosures, if available, is highly recommended.

Enclosure	Question
Organizational Privacy Management	
Organizational strategic plan or business plan addressing privacy protection	A2
Organizational privacy policy or privacy charter	A3
Organizational privacy procedures, guidelines and controls	A4, A6, A7
Physical security and access control documentation	A7
IT security and access control documentation	A7
Records management policies and procedures for personal information	A7
Project Privacy Management	
Project summary and description	B1
Listing of all personal information or personal data elements for project	B2
Personal information data flow diagram	B3
Personal information access documentation ("access matrix")	B4
Statutory authority documentation	B5

Enclosures may be excerpted as appropriate. For example, records management policies and procedures usually deal with much more than just personal information. Only those parts that relate to privacy or personal information need be included.

PUBLIC DOCUMENT: The PIA questionnaire will be considered a public document by the Office of the Information and Privacy Commissioner. Enclosures will also be considered public documents, unless they are explicitly designated as "Confidential". Enclosures designated as "Confidential" must be accompanied by the reason(s) for confidentiality. Reasons must be consistent with one or more exceptions to release under Part 1, Division 2 of the FOIP Act.

Privacy Impact Assessment Questionnaire - *Annotated*

Privacy impact assessments must be submitted to the Information and Privacy Commissioner with a covering letter from the Head of the FOIP public body or the CEO of the HIA custodian.

PIAs will receive no formal response unless they are submitted to the Information and Privacy Commissioner from the Head of a FOIP public body or the CEO of a HIA custodian. Draft PIA's and other preliminary documents may be submitted by other persons in the organization and will be reviewed as appropriate, but they will not be formally acknowledged or accepted by the Commissioner.

Project ³ Information	
Project Name: This should be the full name of the project for which the PIA has been prepared.	Date: Date of submission.
Organization: The name of the organization with primary responsibility or control of the proposed project. Other public bodies may be identified and their organizational information provided on supplementary organizational questionnaires. A copy of the supplementary questionnaire is included in the questionnaire package.	

Contact Information:	
Name: The name of the person who will be the working contact for the Office of the Information and Privacy Commissioner during the review of the PIA. This person should be capable of responding to detailed questions concerning the PIA or identifying persons who can. The contact person will normally be either the drafter of the PIA document or the organization's FOIP Coordinator or chief privacy officer. The contact person should not be the Head of the public body or the CEO of the custodian organization, unless he or she can respond to detailed questions about the PIA.	
Title: Title of the contact person.	
Office: Office address of the contact person.	
Phone: Office telephone number	Fax: Office facsimile number
Email: Office e-mail address	

³ Throughout this questionnaire, the term 'project' is intended to subsume the words 'scheme', 'program', 'initiative', 'application' and 'system', as well as any other word or term that refers to a defined course of endeavour.

#	QUESTION	Yes	Yes and No (partial, incomplete, in preparation, etc.)	No	N/A	Encl. Ref.
---	----------	-----	---	----	-----	---------------

Remember to identify the relevant section or page range of your enclosure package in the "Encl. Ref." column whenever you provide an enclosure. This applies to ALL questions in the questionnaire. It is recommended that your package of enclosures be page numbered sequentially from beginning to end, for ease of reference. This will speed the review process.

A: Organizational Privacy Management						
<p>The questions in this section relate to privacy management throughout the organization. They are not restricted to the project that is the focus of the PIA. Project specific questions appear in Section B.</p> <p>If more than one organization is involved in the proposed project, such as in shared services or data sharing proposals, Section A should be completed for each participating organization. A supplementary organizational questionnaire, which includes Section A but omits Section B, is included for this purpose. Project details in Section B need be provided only once, regardless of the number of organizations involved.</p>						
PREVIOUS PIA SUBMISSIONS						
A1a	Has organizational privacy management information for questions A2 through A7 previously been provided with another PIA?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Note/Elaboration: If your organization has previously submitted a PIA containing the information requested in Section A of this questionnaire, check "Yes" and provide the title and date of the previous PIA in the Note/Elaboration field. To the extent that this information has not changed since the previous PIA was submitted (see next question), you will not have to re-submit it. The Office of the Information and Privacy Commissioner will refer back to the file for the previous PIA and draw the necessary information from there. If you have not previously submitted a PIA with the requested information, check "No" and proceed to question A2.

A1b	If so, has any of this information changed since the previous PIA was submitted? <i>If "No", please note the title and date of the previous PIA and proceed to section B of the questionnaire.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
-----	--	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: If the organizational information previously provided for Section A has not changed, check "No" and proceed to question B1. If any previously submitted organizational information has changed, check "Yes" and enclose the changed information. You need not re-submit previously submitted information that has not changed, but you should be sure to enclose all information that *has* changed.

PRIVACY POLICIES AND CONTROLS						
A2	Is there an organizational strategic plan or business plan that addresses privacy protection? <i>If so, please enclose.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Note/Elaboration: If your organization has a strategic plan, business plan, or other similar document *that addresses privacy considerations*, please enclose a copy. Documents responsive to this question will usually govern the entire organization, in all its business operations. Some organizations may have divisional business or strategic plans; if such plans address privacy issues, they may also be enclosed. Specific policies and procedures governing privacy-related matters, such as records management and security, can be provided in response to questions A4 and A6.

A3	Does a written privacy charter or policy exist? <i>If so, please enclose.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
----	---	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: Question A2 refers to organizational plans that include privacy measures; this question refers to a plan, policy or mission statement that is specifically related to the protection of privacy and related issues. Such documents are often referred to as privacy charters or privacy policies. Documents that are responsive to this question will normally apply to the entire organization, not to a specific business area or project.

#	QUESTION	Yes	Yes and No (partial, incomplete, in preparation, etc.)	No	N/A	Encl. Ref.
---	----------	-----	---	----	-----	---------------

A4	Have privacy guidelines been developed for various aspects of the organization's operations? <i>If so, please enclose.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
----	--	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: This question relates to privacy-related guidelines (including policies) guiding specific aspects of the organization's operations. Such guidelines, if they exist, will be separate from any organization-wide privacy policy or charter, which is dealt with in question A3. Privacy guidelines may form part of broader policies or procedures. If so, it is only necessary to enclose those excerpts that relate to privacy protection.

A5	Is the organization subject to statutory provisions regarding privacy and confidentiality, other than those provided by the Freedom of Information and Protection of Privacy Act and the Health Information Act? <i>Please enclose details.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
----	---	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: Details of any statutory powers or obligations related to privacy protection that are **NOT** derived from the FOIP Act or the HIA should be provided here. Please cite specific sections of the relevant acts or regulations. Remember that in this section the focus is on the organization as a whole, not a specific project. Therefore statutory provisions that respond to this question will likely arise from broadly applicable enabling legislation (e.g., *Municipal Government Act* for municipalities, *School Act* for school boards). If this legislation is explicitly paramount over the FOIP Act or the HIA in any respect, please identify such paramountcies. If a large number of paramountcies is involved, a summary will suffice.

A6	Are organizational policies or procedures in place to ensure that:					
	▪ There is a business purpose for all personal information collected	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ There is statutory authority for the collection of all personal information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Individual consent is obtained whenever possible	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Individuals are duly informed of the purpose and authority for collection	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Information about personal information collected is readily available to individuals	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Personal information correction and annotation are available when required	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Physical records are appropriately stored and managed to maintain privacy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<i>Please enclose copies.</i>						

Note/Elaboration: This question relates to several key aspects of the content of policy, guidelines or procedures that may have been identified in questions A3 and A4, as well as privacy-related content in other such documents. The individual points in this question are key elements of most privacy legislation and generally accepted fair information practices.

A7	Are privacy controls in place in the organization?					
	▪ Need-to-know policies and procedures for personal information access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Physical security and access controls	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ IT security and access controls	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Waste management controls for personal information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Records management & disposition schedules	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Others	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<i>Please enclose copies of related documents.</i>						

#	QUESTION	Yes	Yes and No (partial, incomplete, in preparation, etc.)	No	N/A	Encl. Ref.
---	----------	-----	---	----	-----	---------------

Note/Elaboration: This question relates to operational controls which, although their primary purpose may not be privacy protection, are important elements in the organization's ability to minimize privacy risks.

If your organization has developed an information security plan, please enclose a copy in response to this question. General suggestions for the contents of information security plans are attached for your reference as Appendix A. You may also wish to refer to the Government of Alberta's Freedom of Information and Protection of Privacy Guidelines and Practices, which discusses both privacy impact assessments and security impact assessments. This document may be found at www.gov.ab.ca/foip or by telephoning the Government of Alberta's Information Management and Privacy Branch at 780-422-2657.

IMPORTANT NOTE: If your organization adheres to a generally accepted industry or government standard for information security, please identify that standard in your elaboration for this question and indicate whether your organization has been certified.

PRIVACY STRUCTURE AND ORGANIZATION						
A8	Is there an appointed privacy director or champion within the organization? <i>If so, please identify the position.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Note/Elaboration: If no person has been assigned overall responsibility for privacy issues in the organization, check "No". Otherwise, if yours is a public body under the FOIP Act, this person will often be the FOIP Coordinator, although some FOIP delegation instruments make privacy protection a responsibility of individual business units. If your organization is a custodian under the HIA, please specify which position, if any, has been designated as the person with overall responsibility for privacy issues.

A9	Does a management reporting process exist to ensure that management is informed of any privacy compliance issues?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
----	---	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: If a reporting policy exists to identify such compliance issues, please enclose a copy. If not, please describe how, when and at what level management would be informed of any alleged or actual failures to comply with applicable legislation or policy in matters of privacy protection.

A10	Is senior management actively involved in the development, implementation and/or promotion of privacy measures within the organization?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
-----	---	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: If senior or executive managers are involved in privacy matters, please describe the nature of their involvement. If your organization has a FOIP coordinator or privacy officer, please describe the nature of his or her reporting relationship and position within the organization. How closely does he or she work with your organization's senior and executive managers?

A11	Are employees with access to personal information provided training related to privacy protection?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
-----	--	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: Please identify any privacy-related training that your organization's employees undergo. This question relates mainly to general training within the organization, such as new employee orientations, general FOIP or HIA training, and the like. Project-specific training information may be provided in response to question B15. Training information should note the length and frequency of training, which employees receive it and how they are selected. *Note that for the purposes of the FOIP Act and the privacy impact assessment, contractors are considered employees.*

For the purposes of this question and throughout the questionnaire, 'employee' is defined per S.1(1)(e) of the FOIP Act, and includes appointees, volunteers, students, contractors and agencies.

#	QUESTION	Yes	Yes and No (partial, incomplete, in preparation, etc.)	No	N/A	Encl. Ref.
---	----------	-----	---	----	-----	---------------

B: Project Privacy Management

This section provides information specific to the proposed project. Responses should relate specifically to the proposed project that is the subject of the PIA. Questions B1 through B5 are particularly important.

PROJECT DESCRIPTION

B1	Has a summary of the proposed project been prepared, including a description of the needs behind the development of project, and how the proposed project will meet those needs? <i>If so, please enclose.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
----	--	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: This is an important enclosure because it provides the basic rationale for the project. PIA's without this description may experience lengthened review times.

B2	Has a listing of all personal information or data elements to be collected, used or disclosed in the project been prepared? <i>If so, please enclose.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
----	---	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: This enclosure is important because it illustrates the scope and nature of personal information involved in the proposed project.

B3	Have diagrams been prepared depicting the flow of personal information for this project? <i>If so, please enclose.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
----	--	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: There are many ways to prepare information flow diagrams, and your choice will depend in part on the nature of the proposed project. The Office of the Commissioner does not recommend any particular format, although examples can be made available on request. The information flow diagram should illustrate how personal information is collected, how it circulates within the proponent organization(s), and how it is disseminated beyond the proponent organization(s). In some cases it may be possible to incorporate the response to question B4 into the information flow diagram.

B4	Have documents been prepared showing which persons, positions, or employee categories will have access to which personal information? <i>If so, please enclose.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
----	---	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: This enclosure is important to illustrate the application of 'need-to-know' principles and to complement the data flow diagram requested in question B3. In some cases it may be possible to incorporate this information into the information flow diagram for question B3; if you have done so, please note that fact in your response to this question.

AUTHORITY FOR COLLECTION, USE AND DISCLOSURE

B5	Has the legal authority for the collection, use and disclosure of all personal information for this project been established? <i>Please enclose relevant documentation.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
----	---	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: The PIA questionnaire is legislation-independent; it does not refer specifically to the provisions of any one Act or regulation. This question provides the opportunity to elaborate on the project's compliance with the privacy legislation governing it, whether that legislation is the FOIP Act, the Health Information Act, and/or other legislation. **In the case of the FOIP Act, your elaboration should address sections 32 through 40 (see Appendix 2), plus any other sections or considerations that may apply. In the case of the Health Information Act, your elaboration should address sections 57 through 72 (see Appendix 3), plus any other sections or considerations that may apply.** If you also derive authority from legislation other than the FOIP Act or HIA, please quote the applicable sections of that legislation and address them as appropriate.

#	QUESTION	Yes	Yes and No (partial, incomplete, in preparation, etc.)	No	N/A	Encl. Ref.
---	----------	-----	---	----	-----	---------------

B6	Does individual consent provide the primary basis for the collection, use and disclosure of personal information for this project?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
----	--	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: Under the FOIP Act it is not unusual for statutory authority to replace consent as the primary authority for personal information collection, use and disclosure. This may also occur under other legislation. If individual consent does NOT form the basis for the collection, use and disclosure of personal information, please identify the alternative authority that applies. You may wish to cross-reference your response to question B5, if appropriate.

B7	Have arrangements been made to provide full disclosure of all purposes for which personal information is collected? <i>Please elaborate.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
----	--	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: Disclosure of the purposes to which personal information is to be put is an important privacy protection measure, especially when consent is being sought, and is a requirement of both the FOIP Act and the HIA. Your elaboration should identify the measures that will be taken to ensure that disclosure.

B8	Have the purposes for which the personal information is collected been documented? <i>If so, please enclose.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
----	--	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: Please enclose any documentation which clearly sets out the purposes for which personal information will be collected. If this information has been provided in response to other questions, please cross-reference as necessary.

B9	Is personal information used exclusively for the identified purposes and for uses that an individual would reasonably consider consistent with those purposes?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
----	--	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: If you checked "Yes", this question will probably require little elaboration. If you checked "Yes and No" or "No", please elaborate and identify any measures you will take to ensure that the use of personal information is consistent with identified purposes.

PRIVACY RISK ASSESSMENT						
--------------------------------	--	--	--	--	--	--

B10	Will personal information collected or used in this project be disclosed to any persons who are not employees of the responsible organization?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
-----	--	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: A "No" response to this question identifies a project for which personal information is limited to the internal purposes of a single organization. Such projects may be contrasted with those in which personal information serves the purposes of more than one organization or, while serving one organization, is disseminated beyond that organization.

B11	Will this project involve the collection, use or disclosure of any personal information beyond Alberta's borders? <i>If so, please provide details.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
-----	---	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: The transborder movement of personal information raises a number of special privacy issues, among them the application of Alberta privacy legislation, the adequacy of contractual provisions to protect privacy, the equivalence of privacy legislation in other jurisdictions, and others. If the project involves the international transfer of personal information, these issues may be further complicated. Please provide full details of any plans to transfer personal information between Alberta and any other jurisdiction.

B12	Have this project's potential risks to privacy been assessed? <i>If so, please provide documentation.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
-----	---	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: An important part of a privacy impact assessment is a general review of the possible impact of the project on the privacy of individuals whose personal information may be collected, used or disclosed. This is an opportunity to consider what the overall privacy impact of the project may be. In part this involves identifying, from the perspective of the individuals whose information is involved, how the project may affect their privacy interests.

#	QUESTION	Yes	Yes and No (partial, incomplete, in preparation, etc.)	No	N/A	Encl. Ref.
---	----------	-----	---	----	-----	---------------

B13	If potential risks to privacy have been identified, have means to avert or mitigate those risks been incorporated into the project design?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
-----	--	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: If potential privacy risks have been identified in response to question B12 or other questions, measures will usually need to be taken to avert or mitigate these risks. The nature of these measures should be outlined in response to this question. If they have already been described in response to other questions, you may cross-reference those questions or the enclosures provided in response to those questions. However, this question should respond to any issues identified in question B12.

B14	Have key stakeholders been provided with an opportunity to comment on the privacy protection implications of the proposed project?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
-----	--	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: When projects involve large volumes of personal information, or when that information is particularly sensitive, it is worthwhile to consult those who have privacy interests in the project. If this has been done for this project, please provide a description of the results of such consultations here.

B15	Are project staff trained in the requirements for protecting personal information and aware of the relevant policies regarding breaches of security or confidentiality?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
-----	---	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: Please describe your plans for project training related to the privacy and security measures and policies you plan to implement. Note that this question deals with specific training for the proposed project; more general privacy training programs should be described in response to question A11.

B16	Are personal identifiers used to link or cross-reference multiple databases?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
-----	--	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: Please describe any component of the project that will link or cross-reference separate databases through the use of personal identifiers. Please include an explanation of the need for such linkages and the effect on the project if such linkages were not possible. For the purposes of this questionnaire, 'link' means to create a new combined record from two or more other records by use of a personal identifier. 'Cross reference' means to identify a record of personal information by use of a personal identifier found in another record, but without creating a new record.

PRIVACY CONTROLS AND SECURITY						
--------------------------------------	--	--	--	--	--	--

B17	Have security procedures for the collection, transmission, storage, and disposal of personal information, and access to it, been documented? <i>If so, please enclose.</i>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
-----	--	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: Please provide copies of policies and procedures related to the management of personal information in conjunction with this project. To the extent that you are relying on organization-wide security procedures, please note this and make reference to any relevant enclosures provided in response to question A7.

B18	Are privacy controls in place for the project?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Need-to-know policies and procedures for personal information access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Physical security and access controls	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ IT security and access controls	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	▪ Others	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<i>Please enclose related documentation.</i>						

Note/Elaboration: Measures to control authorized access and use, prevent unauthorized access or disclosure, avoid inadvertent disclosure, and address related issues are important for the protection of privacy. Please describe the measures you have taken in each of the areas noted in this question, as well as any other related areas that are relevant to the proposed project. Your response to this question may overlap with your response to question A6, A7 or B17; if so, please cross-reference as necessary.

#	QUESTION	Yes	Yes and No (partial, incomplete, in preparation, etc.)	No	N/A	Encl. Ref.
---	----------	-----	---	----	-----	---------------

B19	If personal information will be used in the electronic delivery of services, have technological tools and system design techniques been considered which may enhance both privacy and security (e.g. encryption, technologies of anonymity or pseudo-anonymity, or digital signatures)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
-----	---	--------------------------	--------------------------	--------------------------	--------------------------	--

Note/Elaboration: The electronic delivery of services via e-commerce or e-government initiatives can raise special security and privacy issues associated with the technological solutions chosen. If the proposed project involves the electronic delivery of services, please provide details of any privacy-enhancing technologies that will be used. If the project involves no electronic service delivery or if such delivery involves no personal information, check "N/A".

AUDIT AND ENFORCEMENT						
B20	Have arrangements been made for audit, compliance and enforcement mechanisms for the proposed project, including fulfillment of the commitments made in the PIA?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Note/Elaboration: A number of commitments will have been made in responses to this questionnaire. Statements of policy and procedure will have been provided. Security measures will have been described. Other measures to protect privacy will have been identified. This question seeks information concerning how the organization will demonstrate its compliance with (a) the applicable legislative requirements and (b) its own commitments. Please elaborate as necessary to describe how audit, compliance and enforcement will be achieved.

General Notes: This field may be used for any elaboration not provided in response to specific questions.

APPENDIX 1

Information Security Plan

Three broad areas should be addressed relative to developing an Information Security Plan:

1. Sensitive systems and data should be identified.
2. Policies and procedures for ensuring security and control of such systems and data should be created.
3. Personnel training programs should be developed and in place.

Conducting a risk analysis (threat and risk assessment), in conjunction with a department wide inventory of all information assets, will identify sensitive systems and data, as well as potential threats. Upon review of the inventory and risk analysis, individual procedures and safeguards can be developed relative to the specific requirements of the business environment and the components of the system or program being implemented.

Essential components to any Information Security Plan are policies outlining end-user responsibilities relative to the computing environment. These may take the form of:

- Computer usage policy and guidelines
- E-mail policy and guidelines
- Internet policy and guidelines

Once developed, the Information Security Plan is subject to amendment as systems, the environment, and circumstances change. It should be reviewed and updated on a regular and ongoing basis by senior management and personnel assigned to administer and maintain security.

Depending upon the specific organization, the overall Information Security Plan may comment on any or all of the following general business environments:

- Internal and External Networks
- Internal Servers
- External Servers
- Desktop and Portable Computers
- Workspace
- Outsourcing
- File Room
- Mailroom
- Facsimile
- Replication
- Telecommunications
- Transportation

Depending upon the specific organization, the overall Information Security Plan may recommend implementing any or all of the following general safeguards:

Personnel Controls, Security Checks:

Procedures to implement control over the hiring, transfer, absence termination etc. of computer users (including employees, temporary staff, consultants, contractors etc.). Controls to ensure appropriate segregation of duties and proper management supervision of the computing environment.

Security Awareness Training:

A fundamental element in any security plan is programs that are developed to make employees aware of their responsibilities for security of information assets and the potential threats to those assets.

Investigation, Monitoring, Audit:

Procedure outlining requirements for monitoring and investigating suspicious activity across the computing environment. Policy regarding requirements for regular internal and external audits of the entire computing environment.

Continuity Planning, Disaster Recovery:

Procedures outlining specific action to preserve information and essential technology assets in the event of major disruptions (natural and man-made) to normal business operations.

Access Control:

Procedures that outline the process and mechanisms in the operating system, software package, hardware unit, file room mailroom etc. by which all users of information assets are identified and properly authorized to access information and system resources.

Encrypted Storage and Transmission:

Procedures outlining when and how sensitive or confidential information assets may be encrypted for storage or transmission.

Fault Tolerant and Redundant Equipment:

Procedures outlining level and type of systems redundancy within a business environment.

Identification and Authentication:

Safeguard outlining authentication codes or password policy and procedures in the business environment.

Microcomputing Controls:

Policy and plans to implement controls over individual microcomputers in a computing environment including such items as software legitimacy, inventory and virus controls.

Physical Security:

Procedures to implement controls over physical access to areas that house (temporarily or permanently) sensitive information or systems assets.

APPENDIX 2

Excerpts from the *Freedom of Information and Protection of Privacy Act* (unofficial version)

Sections 32 through 40

Purpose of collection of information

32 No personal information may be collected by or for a public body unless

(a) the collection of that information is expressly authorized by an enactment of Alberta or Canada,

(b) that information is collected for the purposes of law enforcement, or

(c) that information relates directly to and is necessary for an operating program or activity of the public body.

1994 cF-18.5 s32;1999 c23 s19

Manner of collection of information

33(1) A public body must collect personal information directly from the individual the information is about unless

(a) another method of collection is authorized by

(i) that individual,

(ii) another Act or a regulation under another Act, or

(iii) the Commissioner under section 51(1)(h) of this Act,

(b) the information may be disclosed to the public body under Division 2 of this Part,

(b.1) the information is collected in a health or safety emergency where

(i) the individual is not able to provide the information directly, or

(ii) direct collection could reasonably be expected to endanger the mental or physical health or safety of the individual or another person,

(b.2) the information concerns an individual who is designated as a person to be contacted in an emergency or other specified circumstances,

(b.3) the information is collected for the purpose of determining suitability for an honour or award, including an honorary degree, scholarship, prize or bursary,

(b.4) the information is collected from published or other public sources for the purpose of fund-raising,

(c) the information is collected for the purpose of law enforcement,

(d) the information is collected for the purpose of collecting a fine or a debt owed to the Government of Alberta or a public body,

(e) the information concerns the history, release or supervision of an individual under the control or supervision of a correctional authority,

(f) the information is collected for use in the provision of legal services to the Government of Alberta or a public body,

(g) the information is necessary

(i) to determine the eligibility of an individual to participate in a program of or receive a benefit, product or service from the Government of Alberta or a public body and is collected in the course of processing an application made by or on behalf of the individual the information is about, or

(ii) to verify the eligibility of an individual who is participating in a program of or receiving a benefit, product or service from the Government of Alberta or a public body and is collected for that purpose,

(h) the information is collected for the purpose of informing the Public Trustee or the Public Guardian about clients or potential clients,

(i) the information is collected for the purpose of enforcing a maintenance order under the Maintenance Enforcement Act,

(j) the information is collected for the purpose of managing or administering personnel of the Government of Alberta or the public body, or

(k) the information is collected for the purpose of assisting in researching or validating the claims, disputes or grievances of aboriginal people.

(2) A public body that collects personal information that is required by subsection (1) to be collected directly from the individual the information is about must inform the individual of

(a) the purpose for which the information is collected,

(b) the specific legal authority for the collection, and

(c) the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

(3) Subsections (1) and (2) do not apply if, in the opinion of the head of the public body concerned, it could reasonably be expected that the information collected would be inaccurate.

1994 cF-18.5 s33;1996 c28 s21;1999 c23 s20

Accuracy and retention

34 If an individual's personal information will be used by a public body to make a decision that directly affects the individual, the public body must

(a) make every reasonable effort to ensure that the information is accurate and complete, and

(b) retain the personal information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it, or for any shorter period of time as agreed to in writing by

(i) the individual,

(ii) the public body, and

(iii) if the body that approves the records and retention and disposition schedule for the public body is different from the public body, that body.

1994 cF-18.5 s34;1999 c23 s21

Right to request correction of personal information

35(1) An applicant who believes there is an error or omission in the applicant's personal information may request the head of the public body that has the information in its custody or under its control to correct the information.

(1.1) Despite subsection (1), the head of a public body must not correct an opinion, including a professional or expert opinion.

(2) If no correction is made in response to a request under subsection (1), or if because of subsection (1.1) no correction may be made, the head of the public body must annotate or link the personal information with that part of the requested correction that is relevant and material to the record in question.

(3) On correcting, annotating or linking personal information under this section, the head of the public body must notify any other public body or any third party to whom that information has been disclosed during the one year before the correction was requested that a correction, annotation or linkage has been made.

(3.1) Despite subsection (3), the head of a public body may dispense with notifying any other public body or third party that a correction, annotation or linkage has been made if

(a) in the opinion of the head of the public body, the correction, annotation or linkage is not material, and

(b) the individual who requested the correction is advised and agrees in writing that notification is not necessary.

(4) On being notified under subsection (3) of a correction, annotation or linkage of personal information, a public body must make the correction, annotation or linkage on any record of that information in its custody or under its control.

(5) Within 30 days after the request under subsection (1) is received, the head of the public body must give written notice to the individual that

(a) the correction has been made, or

(b) an annotation or linkage has been made pursuant to subsection (2).

(6) Section 13 applies to the period set out in subsection (5).
1994 cF-18.5 s35;1999 c23 s22

Transferring request to correct personal information

35.1(1) Within 15 days after a request to correct personal information under section 35(1) is received by a public body, the head of the public body may transfer the request to another public body if

(a) the personal information was collected by the other public body, or

(b) the other public body created the record containing the personal information.

(2) If a request is transferred under subsection (1),

(a) the head of the public body who transferred the request must notify the applicant of the transfer as soon as possible, and

(b) the head of the public body to which the request is transferred must make every reasonable effort to respond to the request not later than 30 days after receiving the request unless the time limit is extended pursuant to section 35(6).

1999 c23 s23

Protection of personal information

36 The head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.

1994 cF-18.5 s36;1996 c28 s21

Division 2
Use and Disclosure of Personal
Information by Public Bodies

Use of personal information

37(1) A public body may use personal information only

(a) for the purpose for which the information was collected or compiled or for a use consistent with that purpose,

(b) if the individual the information is about has identified the information and consented, in the prescribed manner, to the use, or

(c) for a purpose for which that information may be disclosed to that public body under section 38, 40 or 41.

(2) Despite subsection (1), but subject to subsection (3), a post-secondary educational body may use personal information in its alumni records for the purpose of its own fund-raising activities.

(3) A post-secondary educational body must, when requested to do so by an individual, discontinue using that individual's personal information under subsection (2).

(4) A public body may use personal information only to the extent necessary to enable the public body to carry out its purpose in a reasonable manner.

1994 cF-18.5 s37;1999 c23 s24

Disclosure of personal information

38(1) A public body may disclose personal information only

(a) in accordance with Part 1,

(a.1) if the disclosure would not be an unreasonable invasion of a third party's personal privacy under section 16,

(b) for the purpose for which the information was collected or compiled or for a use consistent with that purpose,

(c) if the individual the information is about has identified the information and consented, in the prescribed manner, to the disclosure,

(d) for the purpose of complying with an enactment of Alberta or Canada or with a treaty, arrangement or agreement made under an enactment of Alberta or Canada,

(e) for any purpose in accordance with an enactment of Alberta or Canada that authorizes or requires the disclosure,

(f) for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body having jurisdiction to compel the production of information or with a rule of court that relates to the production of information,

(g) to an officer or employee of the public body or to a member of the Executive Council, if the information is necessary for the performance of the duties of the officer, employee or member,

(g.1) to an officer or employee of a public body or to a member of the Executive Council, if the disclosure is necessary for the delivery of a common or integrated program or service and for the performance of the duties of the officer or employee or member to whom the information is disclosed,

(h) for the purpose of enforcing a legal right that the Government of Alberta or a public body has against any person,

(i) for the purpose of

(i) collecting a fine or debt owing by an individual to the Government of Alberta or to a public body, or to an assignee of either of them, or

(ii) making a payment owing by the Government of Alberta or by a public body to an individual,

(j) for the purpose of determining or verifying an individual's suitability or eligibility for a program or benefit,

(k) to the Auditor General or any other prescribed person or body for audit purposes,

(l) to a member of the Legislative Assembly who has been requested by the individual the information is about to assist in resolving a problem,

(m) to a representative of a bargaining agent who has been authorized in writing by the employee the information is about to make an inquiry,

(n) to the Provincial Archives of Alberta or to the archives of a public body for permanent preservation,

(o) to a public body or a law enforcement agency in Canada to assist in an investigation

(i) undertaken with a view to a law enforcement proceeding, or

(ii) from which a law enforcement proceeding is likely to result,

(p) if the public body is a law enforcement agency and the information is disclosed

(i) to another law enforcement agency in Canada, or

(ii) to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority,

- (q) so that the spouse, relative or friend of an injured, ill or deceased individual may be contacted,
 - (r) in accordance with section 40 or 41,
 - (s) to an expert for the purposes of section 17(2),
 - (t) for use in a proceeding before a court or quasi-judicial body to which the Government of Alberta or a public body is a party,
 - (u) when disclosure is by the Minister of Justice and Attorney General or an agent or lawyer of the Minister of Justice and Attorney General to a place of lawful detention,
 - (v) for the purpose of managing or administering personnel of the Government of Alberta or the public body,
 - (w) to the Director of Maintenance Enforcement for the purpose of enforcing a maintenance order under the Maintenance Enforcement Act,
 - (x) to an officer of the Legislature, if the information is necessary for the performance of the duties of that officer,
 - (y) for the purpose of supervising an individual under the control or supervision of a correctional authority,
 - (z) when the information is available to the public,
 - (aa) to a relative of a deceased individual if, in the opinion of the head of the public body, the disclosure is not an unreasonable invasion of the deceased's personal privacy,
 - (bb) to a lawyer or student-at-law acting for an inmate under the control or supervision of a correctional authority,
 - (cc) if the head of the public body believes, on reasonable grounds, that the disclosure will avert or minimize an imminent danger to the health or safety of any person, or
 - (dd) to the Administrator of the Motor Vehicle Accident Claims Act or to an agent or lawyer of the Administrator for the purpose of dealing with claims under that Act.
- (1.1) A post-secondary educational body may disclose personal information in its alumni records for the purpose of fund-raising activities of the post-secondary educational body if the post-secondary educational body and the person to whom the information is disclosed have entered into a written agreement
- (a) that allows individuals a right of access to personal information that is disclosed about them under this subsection, and
 - (b) that provides that the person to whom the information is disclosed must discontinue using the personal information of any individual who so requests.

(1.2) A post-secondary educational body may, for the purpose of assisting students in selecting courses, disclose teaching and course evaluations that were completed by students.

(2) A public body may disclose personal information only to the extent necessary to enable the public body to carry out the purposes described in subsections (1), (1.1) and (1.2) in a reasonable manner.

1994 cF-18.5 s38;1995 c17 s12;1996 c28 s21;1999 c23 s25

Consistent purposes

39 For the purposes of sections 37(1)(a) and 38(1)(b), a use or disclosure of personal information is consistent with the purpose for which the information was collected or compiled if the use or disclosure

(a) has a reasonable and direct connection to that purpose, and

(b) is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information.

1994 cF-18.5 s39;1999 c23 s26

Disclosure for research or statistical purposes

40 A public body may disclose personal information for a research purpose, including statistical research, only if

(a) the research purpose cannot reasonably be accomplished unless that information is provided in individually identifiable form or the research purpose has been approved by the Commissioner,

(b) any record linkage is not harmful to the individuals the information is about and the benefits to be derived from the record linkage are clearly in the public interest,

(c) the head of the public body has approved conditions relating to the following:

(i) security and confidentiality,

(ii) the removal or destruction of individual identifiers at the earliest reasonable time, and

(iii) the prohibition of any subsequent use or disclosure of the information in individually identifiable form without the express authorization of that public body,

and

(d) the person to whom the information is disclosed has signed an agreement to comply with the approved conditions, this Act and any of the public body's policies and procedures relating to the confidentiality of personal information.

APPENDIX 3

Excerpts from the *Health Information Act* (unofficial version)

Sections 57 through 72

PART 6

DUTIES AND POWERS OF CUSTODIANS RELATING TO HEALTH INFORMATION

Division 1 General Duties and Powers

Duty to collect, use or disclose health information with highest degree of anonymity possible

57(1) In this section, "aggregate health information" means non-identifying health information about groups of individuals.

(2) A custodian that intends to collect, use or disclose health information must first consider whether collection, use or disclosure of aggregate health information is adequate for the intended purpose, and if so, the custodian must collect, use or disclose only aggregate health information.

(3) If the custodian believes that collecting, using or disclosing aggregate health information is not adequate for the custodian's intended purpose, the custodian must then consider whether collection, use or disclosure of other non-identifying health information is adequate for the intended purpose, and if so, the custodian may collect, use or disclose other non-identifying health information.

(4) If the custodian believes that collecting, using or disclosing aggregate and other non-identifying health information is not adequate for the custodian's intended purpose, the custodian may collect, use or disclose individually identifying health information if the collection, use or disclosure

(a) is authorized by this Act, and

(b) is carried out in accordance with this Act.

(5) This section does not apply where the collection, use or disclosure is for the purpose of

(a) providing health services, or

(b) determining or verifying the eligibility of an individual to receive a health service.

Duty to collect, use or disclose health information in a limited manner

58(1) When collecting, using or disclosing health information, a custodian must, in addition to complying with section 57, collect, use or disclose only the amount of health information that is essential to enable the custodian or the recipient of the information, as the case may be, to carry out the intended purpose.

(2) In deciding how much health information to disclose, a custodian must consider as an important factor any expressed wishes of the individual who is the subject of the information relating to disclosure of the information, together with any other factors the custodian considers relevant.

Duty to obtain consent before disclosing by electronic means

59(1) A custodian that intends to disclose individually identifying diagnostic, treatment and care information about an individual by electronic means must obtain the individual's consent to the disclosure or ensure that the individual's consent has been previously obtained.

(2) A consent referred to in subsection (1) must be provided in writing or electronically and must include

(a) an authorization for any custodian to disclose individually identifying diagnostic, treatment and care information about the individual by electronic means for all of the purposes listed in section 27,

(b) an acknowledgment that the individual providing the consent has been made aware of the reason for disclosure by electronic means and the risks and benefits to the individual of consenting or refusing to consent,

(c) the date the consent is effective, and

(d) a statement that the consent may be revoked at any time by the individual providing it.

(3) A disclosure of health information pursuant to this section must be carried out in accordance with the terms of the consent.

(4) A revocation of a consent must be provided in writing or electronically.

(5) A consent or revocation of a consent that is provided in writing must be signed by the person providing it.

(6) A consent or revocation of a consent that is provided electronically is valid only if it complies with the requirements set out in the regulations.

(7) This section does not apply where the disclosure is for the purpose of obtaining or processing payment for health services.

Duty to protect health information

60(1) A custodian must take reasonable steps in accordance with the regulations to maintain administrative, technical and physical safeguards that will

(a) protect the confidentiality of health information that is in its custody or under its control and the privacy of the individuals who are the subjects of that information,

(b) protect the confidentiality of health information that is to be stored or used in a jurisdiction outside Alberta or that is to be disclosed by the custodian to a person in a jurisdiction outside Alberta and the privacy of the individuals who are the subjects of that information,

(c) protect against any reasonably anticipated

(i) threat or hazard to the security or integrity of the health information or of loss of the health information, or

(ii) unauthorized use, disclosure or modification of the health information or unauthorized access to the health information,

and

(d) otherwise ensure compliance with this Act by the custodian and its affiliates.

(2) The safeguards to be maintained under subsection (1) must include appropriate measures for the proper disposal of records to prevent any reasonably anticipated unauthorized use or disclosure of the health information or unauthorized access to the health information following its disposal.

Duty to ensure accuracy of health information

61 Before using or disclosing health information that is in its custody or under its control, a custodian must make a reasonable effort to ensure that the information is accurate and complete.

Duty to identify responsible affiliates

62(1) Each custodian must identify its affiliates who are responsible for ensuring that this Act, the regulations and the policies and procedures established or adopted under section 63 are complied with.

(2) Any collection, use or disclosure of health information by an affiliate of a custodian is considered to be collection, use or disclosure by the custodian.

(3) Any disclosure of health information to an affiliate of a custodian is considered to be disclosure to the custodian.

(4) Each affiliate of a custodian must comply with

(a) this Act and the regulations, and

(b) the policies and procedures established or adopted under section 63.

Duty to establish or adopt policies and procedures

63(1) Each custodian must establish or adopt policies and procedures that will facilitate the implementation of this Act and the regulations.

(2) A custodian must at the request of the Minister or the Department provide the Minister or the Department, as the case may be, with a copy of the policies and procedures established or adopted under this section.

Duty to prepare privacy impact assessment

64(1) Each custodian must prepare a privacy impact assessment that describes how proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information may affect the privacy of the individual who is the subject of the information.

(2) The custodian must submit the privacy impact assessment to the Commissioner for review and comment before implementing any proposed new practice or system described in subsection (1) or any proposed change to existing practices and systems described in subsection (1).

Power to transform health information

65 A custodian may, in accordance with the regulations, strip, encode or otherwise transform individually identifying health information to create non-identifying health information.

Power to enter agreement with information manager

66(1) In this section, "information manager" means a person or body that

(a) processes, stores, retrieves or disposes of health information,

(b) in accordance with the regulations, strips, encodes or otherwise transforms individually identifying health information to create non-identifying health information, and

(c) provides information management or information technology services.

(2) A custodian may enter into an agreement with an information manager in accordance with the regulations for the provision of any or all of the services described in subsection (1).

(3) A custodian that has entered into an agreement with an information manager may disclose health information to the information manager without the consent of the individuals who are the subjects of the information for the purposes authorized by the agreement.

(4) An information manager to which information is disclosed pursuant to subsection (3) may use or disclose that information only for the purposes

authorized by the agreement.

(5) An information manager must comply with

- (a) this Act and the regulations, and
- (b) the agreement entered into with a custodian

in respect of information disclosed to it pursuant to subsection (3).

(6) Notwithstanding subsection (5)(a), a custodian continues to be responsible for compliance with this Act and the regulations in respect of the information disclosed by the custodian to the information manager.

Power to charge fees

67(1) A custodian may charge the fees provided for in the regulations for services provided under Part 2.

(2) Subsection (1) does not permit a custodian to charge a fee in respect of a request for access to an applicant's own health information, except for the cost of producing the copy.

(3) A custodian must give an applicant an estimate of the total fee for its services before providing the services.

(4) A custodian may excuse an applicant from paying all or part of a fee if, in the opinion of the custodian, the applicant cannot afford the fee or in any other circumstances provided for in the regulations.

(5) If an applicant has requested a custodian to excuse the applicant from paying all or part of a fee and the custodian has refused the applicant's request, the custodian must notify the applicant that the applicant may ask for a review by the Commissioner.

(6) The fees referred to in subsection (1) must not exceed the actual cost of the services.

Division 2

Data Matching

Prohibition

68 A custodian must not

- (a) collect the health information to be used in data matching, or
- (b) use or disclose the health information to be used in data matching or created through data matching

in contravention of this Act.

Data matching by custodian

69 A custodian may perform data matching using information that is in its custody or under its control.

Data matching by custodians

70(1) A custodian may perform data matching by combining information that is in its custody or under its control with information that is in the custody or under the control of another custodian.

(2) Before performing data matching under this section, the custodian in whose custody and control the information that is created through data matching will be stored must prepare a privacy impact assessment and submit the assessment to the Commissioner for review and comment.

(3) A privacy impact assessment referred to in subsection (2) must

(a) describe how the information to be used in the data matching is to be collected, and

(b) set out how the information that is created through data matching is to be used or disclosed.

Data matching by custodian and non-custodian

71(1) A custodian may perform data matching by combining information that is in its custody or under its control with information that is in the custody or under the control of a person that is not a custodian.

(2) Before performing data matching under this section, the custodian must prepare a privacy impact assessment and submit the assessment to the Commissioner for review and comment.

(3) A privacy impact assessment referred to in subsection (2) must meet the requirements of section 70(3).

Data matching for research

72 If data matching is performed for the purpose of conducting research, sections 48 to 56 must be complied with before the data matching is performed.

APPENDIX 4

Organization for Economic Co-operation and Development

GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

(for more information see the OECD web site at www.oecd.org)

PREFACE

The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data. Privacy protection laws have been introduced, or will be introduced shortly, in approximately one half of OECD Member countries (Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, Sweden and the United States have passed legislation. Belgium, Iceland, the Netherlands, Spain and Switzerland have prepared draft bills) to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data.

On the other hand, there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers; these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new computer and communications technology. Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance.

For this reason OECD Member countries considered it necessary to develop Guidelines which would help to harmonise national privacy legislation and, while upholding such human rights, would at the same time prevent interruptions in international flows of data. They represent a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it.

The Guidelines, in the form of a Recommendation by the Council of the OECD, were developed by a group of government experts under the chairmanship of The Hon. Mr. Justice M.D. Kirby, Chairman of the Australian Law Reform Commission. The Recommendation was adopted and became applicable on 23rd September, 1980.

The Guidelines are accompanied by an Explanatory Memorandum intended to provide information on the discussion and reasoning underlining their formulation.

**RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE
PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA**
(23rd September, 1980)

THE COUNCIL,

Having regard to articles 1(c), 3(a) and 5(b) of the Convention on the Organisation for Economic Co-operation and Development of 14th December, 1960;

RECOGNISING:

that, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;

that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices;

that transborder flows of personal data contribute to economic and social development;

that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows;

Determined to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries;

RECOMMENDS

1. That Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines contained in the Annex to this Recommendation which is an integral part thereof;
2. That Member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data;
3. That Member countries co-operate in the implementation of the Guidelines set forth in the Annex;
4. That Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.

Annex to the Recommendation of the Council of 23rd September 1980

GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

PART ONE: GENERAL

Definitions

1. For the purposes of these Guidelines:

a) "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf:

b) "personal data" means any information relating to an identified or identifiable individual (data subject);

c) "transborder flows of personal data" means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.

3. These Guidelines should not be interpreted as preventing:

a) the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;

b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or

c) the application of the Guidelines only to automatic processing of personal data.

4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:

a) as few as possible, and

b) made known to the public.

5. In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.

6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

PART TWO: BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- a) with the consent of the data subject; or
- b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

- a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- b) to have communicated to him, data relating to him
 - within a reasonable time;

- at a charge, if any, that is not excessive;
- in a reasonable manner; and
- in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

PART THREE: BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

PART FOUR: NATIONAL IMPLEMENTATION

19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:

- a) adopt appropriate domestic legislation;
- b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;
- c) provide for reasonable means for individuals to exercise their rights;
- d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and
- e) ensure that there is no unfair discrimination against data subjects.

PART FIVE: INTERNATIONAL CO-OPERATION

20. Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries which comply with these Guidelines.

21. Member countries should establish procedures to facilitate:

- information exchange related to these Guidelines, and
- mutual assistance in the procedural and investigative matters involved.

22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.