PFC2017-0237
Attachment 4

Access Impact Assessment Guidelines

for Proactive Disclosure

September 2016

Office of the Information and
Privacy Commissioner of Alberta

Contents

ACKNOWLEDGEMENT

We would like to thank Gary Dickson, Q.C. and Melissa Arseniuk, University of Ottawa law student, for their contributions to this document.

Introduction

An entity[1] may decide to make certain information it holds public for many reasons, including:

- the entity is required by legislation to disclose the information;
- the information is frequently requested by citizens under the *Freedom of Information and Protection of Privacy Act* (FOIP Act) or otherwise; or
- the entity is promoting openness and transparency through open data initiatives.

Prior to proactively disclosing information, an entity should assess the impacts of making the information publicly available. An Access Impact Assessment (AIA) will help an entity:

- identify its authorities for using and disclosing any personal information involved;
- identify the privacy risks and mitigation strategies around disclosing personal information;
- identify the source(s) of the information being disclosed and map the internal processes for approving and preparing the information for public release;
- ensure the information being released is not more than what is intended to be disclosed; and
- ensure the disclosure meets the principles of open data.

This document provides guidance on how to prepare an AIA for proactive disclosure of information. Building systems that enable efficient and timely responses to general and personal requests for access to information is not within the scope of these guidelines.

Privacy

An AIA will address privacy issues around the use and disclosure of personal information as part of a proactive disclosure initiative; however, a separate Privacy Impact Assessment is recommended (and required under the *Health Information Act*) for the design or implementation of new information systems or initiatives, or changes to existing systems.

Submission to the OIPC

An AIA may be submitted to the Office of the Information and Privacy Commissioner (OIPC) for review and feedback[2]. The intent of the OIPC review is to assist the entity in identifying any remaining issues and to recommend improvements based on applicable legislation and best practices.

---

[1] This guidance document was written to be legislation neutral. The term "entity" refers to any public body under the *Freedom of Information and Protection of Privacy Act* (FOIP Act), a custodian under the *Health Information Act* (HIA), or an organization under the *Personal Information Protection Act* (PIPA).

[2] Under provincial legislation, the Commissioner has the power to comment on the implications for access and privacy of programs proposed by entities.

An OIPC review does not result in an approval or certification that your proactive disclosure initiative complies with access and privacy legislation.

If an AIA is being submitted to the OIPC, the entity should:

- answer all the questions posed in this document; or
- briefly explain why certain questions do not apply to the initiative.

Section A: Project Purpose

Describe your proactive disclosure initiative. If there is another initiative or project driving your disclosure project, state what it is.

Your summary should answer the following questions in relation to your AIA:

- What is the business rationale for the project?
- Who is involved in project delivery, both inside and outside the entity?
- Is there any personal information to be published?
- Where will the information be published?
- Why does the project need to disclose the information to achieve its objectives?

Section B: Information Management and Disclosure

1. Management Structure

How is senior management involved in the proactive disclosure of information?

Describe the entity's structure, with a focus on the position(s) relevant to the proactive disclosure of information. For example:

- Who decides what information is disclosed proactively?
- Who compiles or transforms information prior to its disclosure?
- Who approves the proactive disclosure?

You may include an organizational chart showing how the proactive disclosure function is positioned in your management structure. If applicable, indicate whether your initiative involves or will involve anyone responsible for compliance with access and privacy legislation.

2. Policy Management

How are policies relevant to proactive disclosure developed, approved and implemented?

Describe the process to develop, approve, implement and periodically review the policies supporting your proactive disclosure of information initiatives.

Do you have a policy or established process that allows for exceptions to proactive disclosure?

Note: In order to respond to requests for exceptions from employees, partners or third parties, you should establish a clear process for individuals to make, and the entity to review, requests from any person that may cause an exception to your normal proactive disclosure process. For example, an employee may feel there is a risk to their privacy if information about them was disclosed under a proactive disclosure initiative, even if the disclosure was done in a manner that would not individually identify them.

Questions to answer:

- Is there a policy that mandates or supports proactive disclosure of information?
- Are there specific circumstances under which the entity will release data (either structured or unstructured) without a formal request for access to information?

3. Information Management

How do you manage information generally, including information that supports the proactive disclosure?

Describe the information management practices and how they support the proactive disclosure of information sets while protecting privacy rights.

Discussion topics:

- What policies are in place regarding information management? For example, is there a policy for records retention, records destruction, or a policy establishing a duty to document?
- How does the entity ensure it complies with legal and other regulatory requirements regarding information management?

4. Communication and Awareness

How do you ensure employees are aware of, and understand the concepts of access to information and proactive disclosure of information?

Describe how individuals responsible for the proactive disclosure of information are trained in their respective roles.

Describe how the initiative is communicated to individuals who may be affected by the proactive disclosure of information.

You may provide copies of the training materials and any “train-the-trainer” resources.

Discussion topics:

- What access-related training programs are provided to employees?
- Who receives training?
- Is training voluntary or mandatory?
- How often is training offered?
- How often is the training curriculum reviewed?

Section C: Proactive Disclosure Analysis

1. Information Listing

What information is going to be proactively disclosed in your initiative, and where does it originate from?

Generally, the proactive disclosure of information involves compiling and preparing the information before it is made widely accessible, which is considered a use. List the general, personal information or health information[3] that will be used and/or disclosed as part of your project, including where the information originates from. The source of the information may be provided through the name of the information system or business area holding the information in question.

If your project involves the use and/or disclosure of many pieces of information, making the listing of every data element exceedingly difficult, you may include a table that summarizes the various information types, along with a few examples from each category.

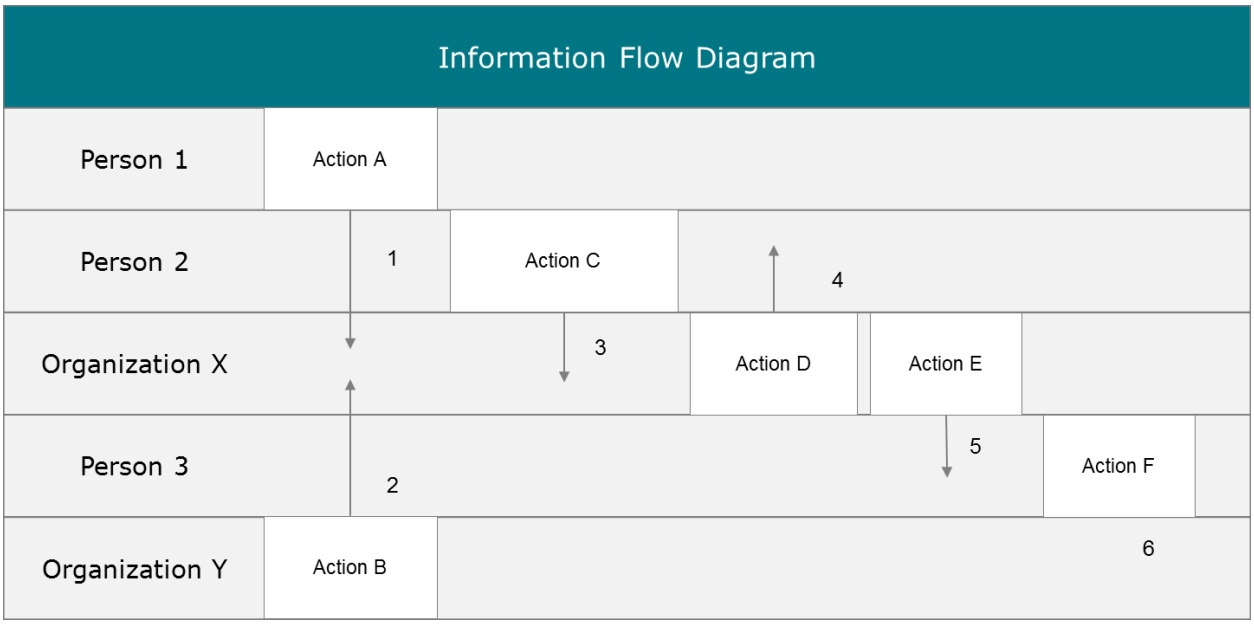
2. Information Flow Diagram

How does information relevant to your initiative flow within the entity and among related third parties?

Prepare a diagram that shows the flow(s) of information related to the process of compiling, reviewing and releasing information under your initiative.

Swim lane diagrams can be used to conveniently present this information for complex projects. For simpler initiatives, a diagram made up of boxes and arrows would be suitable.

[3] As these terms are defined in provincial access and privacy legislation.



3. Legal Authority Table

What is the entity's legal authority to collect, use and disclose the information?

The information flow diagram presented in the previous section can be supplemented by a table that details why the entity is authorized to collect, use or disclose information for the initiative considered.

Flow #	Description	Type of Information	Purpose	Authority for collection / use / disclosure
1	Person 1 performs Action A by doing…	Information element 1, information element 2, etc.…	This information is compiled for the purpose of…	Reference to legislation (and any other instrument) that authorizes the compilation of the information
…	…	…	…	…

Flow #	Description	Type of Information	Purpose	Authority for collection / use / disclosure
6	Entity Y performs Action F by doing…	Information element 1, information element 3, etc.…	This information is disclosed for the purpose of…	Reference to legislation (and any other instrument) that authorizes the disclosure of the information

Note: The authority for the disclosure of the information should be grounded in legislation. Authority grounded in legislation may also be supported by other instruments, such as memos, executive orders, executive decisions, agreements, or memoranda of understanding with service providers or other partners.

4. Open Data Principles – Risks and Mitigation Measures

Is the proactive disclosure of information aligned with best practices?

The OIPC has identified 11 best practices for the publication of open data, or the proactive disclosures of information.[4]

Below, the principles are listed with a brief explanation for each. The descriptions are followed by a table that shows how the risks associated with each principle and the corresponding mitigation measures can be summarized in an AIA.

Open Data Principles

1) Accessibility

Data should be available to the widest range of users for the widest range of purposes. Practically, this means that data must be available online. Proactively disclosed information must be easy to find, search, understand, use and reuse.

2) Timeliness

Data should be made available to the public in a regular, timely manner, as quickly as necessary to preserve the value of the data.

[4] Some of these principles are described in greater detail in the published OIPC report titled "Review of the Government of Alberta's Public Disclosure of Travel and Expenses Policy" available at https://www.oipc.ab.ca/

3) Universality of Use

Accessibility is further advanced when data is freely available to anyone at any time and does not require registration for access. Non-proprietary formats should be used where possible. Data should be released under a licence that does not restrict its use (i.e., no copyrights or patents). Privacy, security and privilege restrictions may be required by law.

4) Primacy and Completeness

Transparency, data reuse and innovation are all maximized when data is collected at the source and released with the finest level of detail permissible (i.e., not aggregated or modified). The published data also should be as complete as possible. All raw data should be disclosed with any notations for necessary redacting.

5) Privacy

A well-crafted open data initiative should address valid privacy and security concerns. Reasonable controls must be in place to ensure that personal privacy of individuals is not inadvertently breached through proactive disclosure of information.

6) Permanence

Data should be located at a stable internet location and made available indefinitely. There should be appropriate archiving over time.

7) Scope

Scope includes an assessment of both the range of topics covered and the categories of information that are the focus to the proactive disclosure. These policy choices should adequately respond to public demand (as reflected by prior requests and other indicators) and meet transparency requirements.

8) Accuracy

Best practice favours disclosing information directly from the source of information, if possible (e.g., the 'touch data only once' principle). The integrity of the data also requires that internal controls exist to ensure that the information presented is accurate and complete.

9) Public Consultation/Input

The public should be consulted in the implementation and ongoing assessment and review of an open data scheme. An entity considering proactive disclosure of information should create meaningful opportunities for public feedback about data quality, quantity, selection and format as well as the user-friendliness of the point(s) of access.

10) Transparency

The policies and processes used to collect and publish the data should be described and made available so that the public has sufficient information to understand the strengths and limitations of the data provided. Transparency is best served when the maximum allowable data about each data element is disclosed. Any limitations on disclosure should be made clear.

11) Accountability

For a proactive disclosure regime to be effective there must be mechanisms by which it is enforced and non-compliance sanctioned. In other words, compliance needs to be reviewable.

Access Risk Mitigation Table

A table can be used to summarize the key risks and mitigation measures identified. **This table includes sample statements only meant to serve as examples.**

Principle	Risk	Mitigation	Policy Reference
Accessibility	Information released is not readily accessible, not searchable, or not machine-readable	There is a procedure in place to ensure the consistent formatting of the published information	*Consistent Data Formatting Procedure*
Timeliness	Information is not released in a timely manner	There is a policy in place to ensure the timely publication of information	*Timely Data Publication Policy*
Universality of Use	Information is released with restrictions or fees attached	There are no restrictions in place; a disclaimer to that effect is published with the information	N/A
Primacy and Completeness	Information released is not complete	…	…
Permanence	Information is taken down before availability period in legislation or policies is met	…	…
Scope	Information released does not conform to scope of intended disclosure	…	…
Accuracy	Lack of integrity of the information disclosed	…	…
Public Consultation /	Public consultation or input not considered	…	…

Principle	Risk	Mitigation	Policy Reference
Input			
Transparency	Process to release information is not transparent	…	…
Accountability	Lack of accountability for information release	The established policy assigned clear responsibilities for this initiative and the related publication(s) of information	*Proactive Disclosure Policy*

Section D: Privacy Risks and Mitigation Plan

The disclosure of information under your proposed initiative may impact individuals' privacy. **If your initiative does not involve any information about identifiable individuals, you may skip this section in its entirety.**

If your initiative involves personal information, or if you believe there are foreseeable privacy risks, this subsection should be included with your AIA to provide an analysis of privacy risks and corresponding mitigation strategies. **This table includes sample statements only meant to serve as examples.**

Project Risk	Description	Mitigation Measures for Project	Policy Reference
Unauthorized access to, use, or disclosure of personal information by internal or authorized parties	An unauthorized employee of the entity has access to all the entity's information.	The responsibility to retrieve information is assigned to an authorized employee who is the only one having access to the information	*Proactive Disclosure Policy*
Unauthorized access to, use, or disclosure of personal information by external parties	…	…	…
Loss of integrity of personal information	…	…	…
Loss, destruction, or loss of use of personal information	…	…	…

Project Risk	Description	Mitigation Measures for Project	Policy Reference
Service provider or business partner accesses, uses or discloses personal information in contravention of applicable privacy legislation or our policies	…	…	…
Third party attempts to re-identify information through inference attack	…	…	…
Other risks that you identify	…	…	…

Section E: Policies and Procedures

1. Entity Documentation

The intent of this section is to compile appendices such as policies, procedures, and other materials that are referenced elsewhere in your AIA, or are relevant to your initiative.

2. Other Documentation

Legislation, guides or other documentation outside of the entity's control

You may use a simple table to organize and summarize your attachments and provide page references. **This table includes a sample statement only meant to serve as an example.**

Topic	Policy Description	Attachment Title	Page Reference
Privacy policy	*Privacy policy description*	*"Access to Information Policy"*	*Page x*

Appendix: Access Impact Assessment Template

This table may be used to voluntarily complete an AIA.

Section A: Project Purpose

Describe your proactive disclosure initiative. If there is another initiative or project driving your disclosure plan, state what it is.

Section B: Information Management and Disclosure

1. Management Structure

How is your senior management involved in the proactive disclosure of information?

2. Policy Management

How are policies relevant to proactive disclosure developed, approved and implemented?

3. Information Management

How does the entity manage information generally, including information that supports the proactive disclosure?

4. Communication and Awareness

How does the entity ensure its employees are aware of, and understand the concepts of access to information and proactive disclosure of information?

Section C: Proactive Disclosure Analysis

1. Information Listing

What information is going to be proactively disclosed in your initiative, and where does it originate from?

2. Information Flow Diagram

How does information relevant to your initiative flow within the entity and among related third parties?
(Swim lane diagrams can be used to conveniently present this information for complex projects. For simpler initiatives, a diagram made up of boxes and arrows would be suitable.)

3. Legal Authority Table

What is the entity's legal authority to collect, use and disclose the information?

Flow #	Description	Type of Information	Purpose	Authority for collection / use / disclosure

Flow #	Description	Type of Information	Purpose	Authority for collection / use / disclosure
1	Person 1 performs Action A by doing…	Information element 1, information element 2, etc.…	This information is compiled for the purpose of…	Reference to legislation (and any other instrument) that authorizes the compilation of the information
…	…	…	…	…
6	Entity Y performs Action F by doing…	Information element 1, information element 3, etc.…	This information is disclosed for the purpose of…	Reference to legislation (and any other instrument) that authorizes the disclosure of the information

4. Open Data Principles – Risks and Mitigation Measures

Is the entity's proactive disclosure of information aligned on best practices? **This table includes sample statements meant only to serve as examples.**

Principle	Risk	Mitigation	Policy Reference
Accessibility	Information released is not readily accessible, not searchable, or not machine-readable	There is a procedure in place to ensure the consistent formatting of the published information	*Consistent Data Formatting Procedure*
Timeliness	Information is not released in a timely manner	There is a policy in place to ensure the timely publication of information	*Timely Data Publication Policy*
Universality of Use	Information is released with restrictions or fees attached	There are no restrictions in place; a disclaimer to that effect is published with the information	N/A

Principle	Risk	Mitigation	Policy Reference
Primacy and Completeness	Information released is not complete	…	…
Permanence	Information is taken down before availability period in legislation or policies is met	…	…
Scope	Information released does not conform to scope of intended disclosure	…	…
Accuracy	Lack of integrity of the information disclosed	…	…
Public Consultation / Input	Public consultation or input not considered	…	…
Transparency	Process to release information is not transparent	…	…
Accountability	Lack of accountability for information release	The established policy assigns clear responsibilities for this initiative and the related publication(s) of information	*Proactive Disclosure Policy*

Section D: Privacy Risks and Mitigation Plan

The disclosure of information may impact individuals' privacy. If your initiative does not involve any information about identifiable individuals, you may skip this section. **This table includes sample statements meant only to serve as examples.**

Project Risk	Description	Mitigation Measures for Project	Policy Reference
Unauthorized access to, use, or disclosure of personal information by internal or authorized parties	An unauthorized employee of the entity has access to all the entity's information.	The responsibility to retrieve information is assigned to an authorized employee who is the only one having access to the information	*Proactive Disclosure Policy*
Unauthorized access to, use, or disclosure of personal information by external parties	…	…	…

Project Risk	Description	Mitigation Measures for Project	Policy Reference
Loss of integrity of personal information	…	…	…
Loss, destruction, or loss of use of personal information	…	…	…
Service provider or business partner accesses, uses or discloses personal information in contravention of applicable privacy legislation or our policies	…	…	…
Third party attempts to re-identify information through inference attack	…	…	…
Other risks that you identify	…	…	…

Section E: Policies and Procedures

1. Entity Documentation

Compile appendices such as policies, procedures and other materials that are referenced in your AIA, or are relevant to your initiative.

2. Other Documentation

You may use a simple table to organize and summarize your attachments and provide page references. **This table includes a sample statement only meant to serve as an example.**

Topic	Policy Description	Attachment Title	Page Reference
Privacy policy	*Privacy policy description*	*"Access to Information Policy"*	*Page x*