

Information
and Privacy
Commissioner/
Ontario

Model Access and Privacy Agreement



Ann Cavoukian, Ph.D.
Commissioner
August 1997



**Information and Privacy
Commissioner/Ontario**

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

The Information and Privacy Commissioner/Ontario gratefully acknowledges the work of John Eichmanis in preparing this report.

Cette publication est également disponible en français.

This publication is also available on the IPC website.

Table of Contents

Introduction	1
Considerations for Alternative Service Delivery Contracts or Agreements	1
Transitional Provisions Included in the Agreement	1
1. Custody or control of general records and personal information	1
2. Physical transfer of general records and personal information	2
3. Outstanding Requests and Appeals	2
Model Access and Privacy Agreement	3
I. Purpose	4
II. Definitions	4
III. Policies	5
1. Accountability and Administration	5
2. Protection of Personal Information	6
Collection	6
Individual Access	6
Use and Disclosure	6
Consent	7
Retention	7
Disposal	7
Accuracy	7
Right of Correction	7
Security	8
Complaints	8
Penalties	8
3. Access to Information	8

Introduction

To assist government organizations when contemplating alternative service delivery options, the Office of the Information and Privacy Commissioner/Ontario (the IPC) has prepared a model agreement that could form part of the overall contract or agreement between the government organization and the contracting entity. The model agreement or contract would be appropriate in those circumstances where the government organization does not retain custody or control of its general records or personal information.

While the suggested provisions seek to be inclusive, the specific circumstances of each agreement or contract may require modifications to some provisions.

Considerations for Alternative Service Delivery Contracts or Agreements

The agreement or contract should contain:

1. transitional provisions; and
2. access and privacy provisions attached as a schedule to the agreement or contract (see “Model Access and Privacy Agreement”).

Transitional Provisions Included in the Agreement

1. Custody or control of general records and personal information

The agreement or contract should include reference to whether the government organization will retain custody or control of the general records and personal information in its possession.

The government organization should consider whether it will transfer custody or control of the general records or personal information to the contracting entity, or whether it will retain custody or control, while transferring certain responsibilities for the general records and personal information to the contracting entity. By determining who has custody or control of the records, the government organization is able to decide whether the *Freedom of Information and Protection of Privacy Act* or the *Municipal Freedom of Information and Protection of Privacy Act* (the *Acts*) will continue to apply. For example, if the government organization retains custody or control, the *Acts* will still apply to the records. However, if custody or control is to be passed to the Alternative Service Delivery Provider, then access and privacy provisions need to be considered in the contract or agreement.

2. Physical transfer of general records and personal information

Where the government organization decides to transfer its general records and personal information, all reasonable steps should be taken to protect the security and confidentiality of the information during its storage, transportation, and handling.

3. Outstanding Requests and Appeals

Government organizations should include procedures to deal with outstanding requests and appeals during the transition phase, prior to the contracting entity taking full custody or control of the government organization's general records or personal information.

For your convenience and ease of use the IPC has developed the following template that can be applied in preparing the agreement.

Model Access and Privacy Agreement

Note: This model agreement would be appropriate in those circumstances where a government organization does not retain custody or control of its general records or personal information. However, where the government organization does maintain custody or control of its records, there should be a clause in the agreement which stipulates that the contracting entity agrees to comply with the provisions of the *Freedom of Information and Protection of Privacy Act* or the *Municipal Freedom of Information and Protection of Privacy Act* (the Acts) in the course of providing services. For more information about circumstances where the government organization does retain custody or control of its records, please refer to Management Board's *FIPPA Considerations for Alternative Services Delivery* and the IPC's Investigation Report I97-017P.

AGREEMENT

[Indicate the title of the agreement]

I. Purpose

The purpose of this agreement is to establish policies and procedures regarding public access to general records held by the organization and the protection of personal information including access by individuals to their own personal information.

II. Definitions

‘Access to information’ means access by the public to the organization’s general records.

The **‘Access and Privacy Agreement’** means the policies and procedures dealing with access to information and the protection of privacy affixed to this agreement or contract.

‘Personal Information’ means information about an identifiable individual recorded in any form including:

- a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual;
- b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
- c) any identifying number, symbol or other particular assigned to the individual;
- d) the address, telephone number, fingerprints or blood type of the individual;
- e) the personal opinions or views of the individual except where they relate to another individual;
- f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence;
- g) the views or opinions of another individual about the individual; and
- h) the individual’s name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

For the purpose of collection, 'personal information' includes information that is not recorded and that is otherwise defined as 'personal information' in this agreement.

The 'organization' means... [name of the non-government organization to provide the service].

III. Policies

1. Accountability and Administration

- a) The [organization] shall develop and implement policies and procedures dealing with public access to information and the protection of privacy. The policies and procedures shall be publicly accessible.
- b) The [organization] shall appoint a senior officer who shall have the responsibility of ensuring the organization's compliance with this agreement.
- c) The [organization] shall develop a procedure and time frames for complying with requests for access to information already held by the [organization].
- d) Staff will be required to adhere to strict confidentiality of personal information.
- e) The [organization] shall publish information regarding its policies and procedures relating to the management of personal information and general records. Such information shall include:
 - i) the name of the person responsible for the [organization]'s policies and procedures;
 - ii) the name of the person to whom complaints should be directed;
 - iii) the form such complaints should take;
 - iv) the means of gaining access to personal information held by the [organization];
 - v) a description of the type of personal information held by the [organization]; and
 - vi) brochures or other documentation describing the [organization]'s policies, procedures and codes.
- f) The [organization] shall ensure that the staff of the [organization] are adequately trained in order to ensure that the policies and procedures can be effectively implemented.

2. Protection of Personal Information

Collection

The collection of personal information shall be limited to that which is necessary for the [organization] to comply with the contract, or to meet the obligations of a statute. Wherever possible, personal information shall be collected directly from the individual to whom the information relates by fair and lawful means.

The purpose for which information is collected shall be identified by the [organization] to an individual, at or before the time the information is collected.

Individual Access

- a) Upon request, the [organization] shall provide an individual with information concerning the existence, use and disclosure of his or her personal information and provide the applicable personal information to the individual, except where releasing the personal information would:
 - i) violate another individual's right to privacy, unless that individual consents to the information's release;
 - ii) violate solicitor-client privilege; or
 - iii) compromise security, or legally recognized commercial proprietary concerns.
- b) Personal information shall be made available to requesters at minimal or no cost and shall be provided in a form that is easily understandable.

Use and Disclosure

- a) Personal information shall not be used or disclosed for purposes other than that for which it was collected, except with the consent of the individual or as required by law.
- b) An individual's consent must be obtained before personal information may be disclosed to third parties, except for law enforcement purposes.
- c) The [organization] shall provide personal information to third parties who can demonstrate that they have in place a means to provide protection comparable to that provided by the [organization].
- d) Where personal information is made available to third parties on an ongoing basis, amendments to such information shall regularly be provided to them.

Consent

The knowledge and consent of the individual are required for the use, or disclosure of personal information, except where permitted under freedom of information and privacy legislation, such as law enforcement purposes.

Retention

- a) Personal information shall be retained only as long as necessary for the fulfilment of the purpose for which it was collected.
- b) Guidelines shall be developed to govern the period of time personal information is retained by the [organization].

Disposal

- a) Reasonable steps should be taken to protect the security and confidentiality of personal information that is to be destroyed.
- b) Personal information that is no longer required to fulfil the identified purposes should be permanently erased, rendered anonymous or destroyed in such a way that it cannot be reconstructed or retrieved.
- c) Guidelines shall be developed and procedures implemented to govern the secure destruction of personal information to ensure it cannot be reconstructed or retrieved.

Accuracy

Personal information shall be as accurate, complete, and as up-to-date as possible.

Right of Correction

- a) The individual has the right to ask that information relating to him or her be corrected, and where there is disagreement about the correctness of the information, the [organization] shall attach the individual's statement of disagreement to the personal information.
- b) The individual may require that any third party to whom their personal information was disclosed, within the year before the time the correction was requested or a statement of disagreement required, be notified of the correction or statement of disagreement.

Security

In order to prevent the unauthorized disclosure, copying, use or modification of personal information held by the [organization], access to such information shall be restricted by the use of recognized security mechanisms such as passwords, encryption or other reasonable safeguards.

Complaints

- a) An individual shall be able to file a complaint concerning compliance with the above rules to the designated individual or individuals accountable for the [organization's] compliance with this agreement.
- b) The [organization] shall develop a mechanism to address all complaints about the handling of personal information and the refusal to grant access in response to a request for one's own information.
- c) If a complaint is found to be justified, the [organization] shall take appropriate measures to rectify the problem in a timely manner.
- d) The [organization] shall develop and implement procedures which establish a mechanism to allow any unresolved complaints to be addressed by an independent third party.

Penalties

No person shall willfully use, disclose, or retain personal information obtained under the authority of this agreement or contract, as determined by the [organization]'s enabling legislation.

3. Access to Information

Records of the [organization] shall be made available to the public on request, subject to the following exceptions:

- i) personal information, including medical information, when the personal information is sought by persons other than by the individual to whom the information relates;
- ii) law enforcement information;
- iii) information, the disclosure of which, would violate solicitor-client privilege; and
- iv) a trade secret, commercial, technical, financial, or labour relations information which, if released, would harm the competitive position of the [organization].