

About the Freedom of Information (FOI) and Privacy Manual

The Freedom of Information (FOI) and Privacy Manual is designed to assist Freedom of Information and Privacy Coordinators for organizations covered by the [Freedom of Information and Protection of Privacy Act](#) (FIPPA) or [Municipal Freedom of Information and Protection of Privacy Act](#) (MFIPPA).

The Manual provides an overview of FIPPA and access–and privacy–related practices and procedures to help Coordinators carry out their primary responsibilities — ensuring that the organizations they support:

- process access requests in compliance with the law; and
- collect, use, disclose and dispose of personal information in compliance with the law.

For advice about processing FOI requests and protecting personal information, please contact us.

Chapter 1: Introduction to the Act

Table of Contents

- Purpose of the Act
 - How the Act is Organized
 - Scope of the Act
 - Definitions
 - Custody
 - Control
 - Directory of Institutions
 - Directory of Records
 - Exemptions: Mandatory and Discretionary
 - Frivolous and Vexatious Requests
 - Head
 - Individual
 - Information and Privacy Commissioner (Commissioner)
 - Institution
 - Labour Relations
 - Law Enforcement
 - Person
 - Personal Information
 - Personal Information Bank
 - Public Interest
 - Record
 - Machine Readable Record
 - Third Party
 - Use (of personal information)
 - Waiver of Notice
 - Role of the Responsible Minister and Ministry of Government Services
 - The Annotation
-

Purpose of the Act

s.1 FIPPA / s.1 MFIPPA

The *Freedom of Information and Protection of Privacy Act (FIPPA)* and the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* provide individuals with a right of

access to certain records and personal information under the custody or control of institutions covered by the Acts.

The purposes of the FIPPA/MFIPPA are as follows:

(a) to provide a right of access to information under the control of institutions in accordance with the principles that,

- information should be available to the public,
- necessary exemptions from the right of access should be limited and specific,
- decisions on the disclosure of information should be reviewed independently of the institution controlling the information; and

(b) to protect the privacy of individuals with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information.

How the Act is Organized

FIPPA came into force on January 1, 1988, MFIPPA became law 3 years later on January 1, 1991. FIPPA/MFIPPA are divided into four similar parts. FIPPA has an additional part at the beginning dealing with administrative matters covering both of FIPPA/MFIPPA. The sections are as follows:

FIPPA Part I: Administration covers administrative matters with respect to the Responsible Minister and the Information and Privacy Commissioner, Ontario (IPC).

FIPPA Part II / MFIPPA Part I: Freedom of Information deals with the right of access to records, exemptions to that right, access procedures and information to be published or made available to assist in locating government held records.

FIPPA Part III / MFIPPA Part II: Protection of Individual Privacy concerns the collection, retention, use, disclosure and disposal of personal information and personal information banks. This part also deals with an individual's right of access to his/her own personal information and the right to request correction of that information.

FIPPA Part IV / MFIPPA Part III: Appeal addresses the right to appeal and the procedures for appealing a decision made by an institution.

FIPPA Part V / MFIPPA Part IV: General covers general matters including the charging of fees, offences, regulations and the powers and duties of the IPC.

Scope of the Act

s.10, 63, 64, 65, 69, 70 FIPPA / 4, 50, 51, 52 MFIPPA

s.5 O.Reg.460 /s.5 O.Reg.823, O.Reg.372/91

FIPPA covers all ministries of the Ontario Government and any agency, board, commission, corporation or other body designated as an "institution" in the regulations. MFIPPA covers all municipal corporations, including a metropolitan, district or regional municipality, local boards and commissions. The term institution is defined in s.2 of FIPPA/MFIPPA and is set out in the Definitions segment of this chapter immediately below.

FIPPA/MFIPPA apply to any record in the custody or under the control of an institution, including records created both before and after the laws came into force.

FIPPA binds the Crown.

FIPPA/MFIPPA do not apply to:

- records such as private donations placed in the Archives of Ontario (FIPPA) or the archives of an institution by or on behalf of a person or organization other than the institution (for MFIPPA institutions). This includes private donations of manuscripts and letters;
- records covered by the disclosure scheme in the *Young Offenders Act* (YOA);
- for FIPPA institutions: records of a patient in a psychiatric facility as defined by section 1 of the *Mental Health Act* where the record is a clinical record as defined by subsection 35(1) of the *Mental Health Act*, or contains information on the history, assessment, diagnosis, observation, examination, care or treatment of the patient;
- for FIPPA institutions: wiretap application records covered by the *Criminal Code*;
- for FIPPA institutions: notes for the personal use of a presiding judge (s.65(3));
- for institutions covered by FIPPA/MFIPPA: labour relations or employment-related matters as described in s.65(6 & 7) FIPPA / s.52(3 & 4) MFIPPA.

FIPPA/MFIPPA do not impose any limitation on the information otherwise available by law to a party to litigation. Where an institution is required to produce documentary evidence pursuant to rules of court, the exemptions in FIPPA/MFIPPA do not apply.

FIPPA/MFIPPA is a comprehensive access scheme which must be implemented by all institutions, including administrative tribunals who are listed as "institutions" under the Act. It does not deny access to information through rules of natural justice or legal procedures. For example, it does not affect the power of a court or tribunal to compel a witness to testify or to compel the production of a document.

Not all requests for information need to be made under FIPPA/MFIPPA. Information can be provided in response to an oral request or in the absence of a request, where an institution may give access to that information under FIPPA/MFIPPA. The Acts should not be applied to

preclude access to information (except personal information) that was available by custom or practice before they came into force.

Definitions

s.2 FIPPA / s.2 MFIPPA

The terms that appear in green are taken from the Acts. The remaining terms have been defined in such sources as the IPC orders. The terms defined in the Act appear with the relevant section from the Act.

Control (of a record)

Means the power or authority to make a decision about the use or disclosure of the record.

Custody (of a record)

Means the keeping, care, watch, preservation or security of the record for a legitimate business purpose. While physical possession of a record may not always constitute custody, it is the best evidence of custody.

In Order # P-120 the IPC first outlined 10 factors that could be considered to determine the custody or control of a record. These factors are listed in s.10/4 of the *Annotation* under (Custody or Control).

Directory of Institutions

s.31 FIPPA / s.24 MFIPPA

Is a compilation listing all institutions covered by the Acts, including information on where requests can be made and whether institutions have a library or reading room available to the public and if so, its address.

Directory of Records

s.32, 33, 35, 45 FIPPA / s.25, 34 MFIPPA

Is a publication which lists, for institutions covered by FIPPA,

(a) information on the general classes or types of records and manuals maintained by institutions and

(b) the personal information banks maintained by each institution.

Each MFIPPA institution is required to make available similar information for public inspection.

Exemptions: Mandatory and Discretionary

There are two types of exemptions in FIPPA/MFIPPA.

Mandatory exemptions impose a duty on the head of an institution to refuse to disclose a record. Mandatory exemptions begin with the words: "a head shall refuse to disclose...". There are three mandatory exemptions in FIPPA. They are: s.12 (Cabinet records), s.17 (third party information) and s.21 (personal privacy). The three mandatory exemptions for MFIPPA are: s.9 (relations with other governments), s.10 (third party information) and s.14 (personal privacy). In the case of mandatory exemptions the head must determine whether the facts exist or may exist which bring the record requested within the exemption.

If grounds for a mandatory exemption exist, the head must refuse access unless a compelling public interest outweighs the purpose of the exemption (e.g. s.21 FIPPA / s.14 MFIPPA). The public interest override does not apply to s.12, 14, 16, 19 and 22 FIPPA / s.6, 8, 12, and 15 MFIPPA.

All other exemptions are discretionary exemptions. They permit the head to disclose a record despite the existence of the exemption. Discretionary exemptions are introduced by the words: "(A) head may refuse to disclose...". FIPPA/MFIPPA require a two-stage process in determining whether a discretionary exemption is to be applied. First, the head must determine whether the facts exist or may exist which bring the record requested within the exemption. Second, the head must decide whether he/she is willing to release the record, despite the existence of grounds for the exemption. A decision by a head to disclose information falling within an exemption is an exercise of discretion.

Frivolous and Vexatious (requests)

s.27.1 FIPPA / s.20.1 MFIPPA

s.5.1 O.Reg.460 /s.5.1 O.Reg.823

An institution is not required to proceed with a request it views as frivolous or vexatious. If a requester appeals this decision, the institution is required to present evidence that the request is frivolous and/or vexatious and the IPC will determine if the institution's decision is reasonable.

Under the regulations, a frivolous or vexatious request occurs where the request is part of a pattern of conduct that amounts to an abuse of the right of access or where responding to the request would interfere with the operations of the institution. Examples of the meaning of "abuse" in the legal context include:

- proceedings instituted without any reasonable ground;
- proceedings whose purpose is not legitimate, but is rather designed to harass, or to accomplish some other objective unrelated to the process being used;
- situations where a process is used more than once, for the purpose of revisiting an issue previously addressed.

In addition, the regulations provide that a request meets the definition of frivolous or vexatious if it is made in bad faith. Bad faith is not simply bad judgment or negligence, but rather it implies the conscious doing of a wrong because of dishonest purpose. It contemplates a state of mind which views the access process with contempt and for the nuisance it creates, rather than a valid means of obtaining information.

Head

s.2 FIPPA / s.2 MFIPPA

Under FIPPA, means,

(a) in the case of a ministry, the minister of the Crown who presides over the ministry, and

(b) in the case of any other institution, the person designated as head of that institution in the regulations.

For FIPPA institutions other than ministries (such as agencies listed in the regulations), the minister responsible for that institution shall be deemed to be the head of that institution, unless the regulation designates someone else.

Under MFIPPA, means,

(c) in respect of an institution, means the individual or body determined to be head under section 3;

The selection of a head for MFIPPA institutions is discussed in greater detail in the Administration chapter (Chapter 2) of this manual.

Individual

Means a human being; it does not include a corporation (see also the definition of "Person").

Under s.66 FIPPA / s.54 MFIPPA, **Any right or power conferred on an individual by this Act may be exercised,**

(a) where (FIPPA)/if (MFIPPA) the individual is deceased, by the individual's personal representative if exercise of the right or power relates to the administration of the individual's estate;

(b) by the individual's attorney under a continuing power of attorney, the individual's attorney under a power of attorney for personal care, the individual's guardian of the person, or the individual's guardian of property; and

(c) where (FIPPA)/if (MFIPPA) the individual is less than sixteen years of age, by a person who has lawful custody of the individual.

The personal representative referred to in clause (a) is the executor named in a will or, where there is no will, the administrator appointed by a court to administer the estate of the deceased person. In order for the personal representative of a deceased to exercise a right or power of the deceased, the exercise of the right or power must relate to the administration of the estate. As a result, the rights of the representative are narrower than the rights the deceased could have exercised while alive.

In clause (b), a guardian may be appointed by a court order for a person who is incapable of managing his/her own affairs or who is capable of making decisions about personal care. In addition, the Public Guardian and Trustee may become an individual's statutory guardian as provided by the *Mental Health Act* and the *Substitute Decisions Act*.

In clause (c) the IPC has held that the rights under FIPPA/MFIPPA of an individual with lawful custody of a child are not absolute; for instance the rights cannot be used to access records for personal objectives that are not those of the child.

The rights or powers which may be exercised on behalf of an individual include the right to make a request for access to a record, the right to consent to the use and disclosure of personal information under s.21(1)(a), 41(a) and 42(b) FIPPA/ s.14(1)(a), 31(a) and 32(b) MFIPPA, and the right to authorize personal information to be collected other than directly from the individual under s.39(1)(a) FIPPA / s.29(1)(a) MFIPPA.

Information and Privacy Commissioner(Commissioner)

s.4, 5, 6, 7, 8, 9, 50, 51, 52, 54, 55, 56, 58, 59, 61 FIPPA / s.39, 40, 41, 43, 44, 46, 48 MFIPPA

The Commissioner is appointed by the Lieutenant Governor in Council. The Commissioner is an officer of the Legislature and is independent of the government.

The IPC hears appeals of decisions made by heads of institutions, issues binding orders, conducts privacy investigations, and has certain powers relating to the protection of personal privacy. In the Appeals chapter (Chapter 7) of this manual the role of the Commissioner is discussed in more detail.

Institution

s.2 FIPPA / s.2 MFIPPA

Under FIPPA "**institution**" means,

- (a) a ministry of the Government of Ontario,**
- (b) any agency, board, commission, corporation or other body designated as an institution in the regulations.**

Under MFIPPA there are three parts to the definition of institution:

- (a) a municipal corporation, including a metropolitan, district or regional municipality or the County of Oxford,**

Each municipal corporation (village, town, township, city, county, and district and regional municipality) is a separate institution for the purposes of the Act.

The following bodies are considered to part of a municipal corporation: boards of control, sinking fund committees, fence viewing boards, courts of revision, planning advisory committees, property standards committees, cemetery boards, committees of adjustment, land division committees, parking authorities, parks boards, arena boards and recreation boards, and other bodies where all the members or officers are appointed by council.

For example: A board of management for a Business Improvement Area would be covered as part of the municipal corporation because all of the members of the board are appointed by a municipal council.

Where only some of the members of an agency or board are appointed by the municipal institution, that agency or body is not considered part of the municipality for the purposes of the Act.

For example: A non-profit housing corporation may not be an institution under the Act when some members are appointed by community groups rather than the municipality.

(b) a school board, public utilities commission, hydro-electric commission, transit commission, suburban roads commission, public library board, board of health, police commission, conservation authority, district welfare administration board, local services board, planning board, local roads board, police village or joint committee of management or joint board of management established under the Municipal Act.

These institutions, some of which are closely connected to municipal corporations, are designated separate institutions for the purposes of the Act.

(c) any agency, board, commission, corporation or other body designated as an institution in the regulations.

Other bodies may be prescribed as separate institutions for the purposes of the Act.

For example: A municipality might have a corporation established under a private statute that operates a convention centre. Except for the fact that the centre is owned by the municipality, it operates as an autonomous entity. In this case it may be appropriate that the centre be designated in regulation as a separate institution for the purposes of the Act (e.g., The Hamilton Entertainment and Convention Facilities Inc.)

Labour Relations

Means the collective relationship between an employer and its employees. (see Chapter 5 on Privacy Protection for a further discussion of labour relations and employment-related records).

Law Enforcement

Law enforcement means,

(a) policing,

(b) investigations or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed in those proceedings, and

(c) the conduct of proceedings referred to in clause (b).

There are three parts to the definition. Part (a) encompasses the activities of police forces. These activities include the investigation and prosecution of offences, the collection and analysis of intelligence information, the prevention of crime, the maintenance of law and order and the

provision of security and protective services. This part does not apply to internal employment-related investigations for breach of contract.

Part (b) of the definition includes activities by an institution to enforce compliance with standards, duties and responsibilities set out in a statute or regulation. Many institutions have a branch which is responsible for the enforcement of statutes administered by the institution.

In part (b) the words "lead or could lead" indicate that inspections and investigations may be part of "law enforcement" even if they do not actually result in proceedings in a court or tribunal.

For example: The result of an investigation to determine whether an offence has been committed under the *Environmental Protection Act* or a Municipal By-law may be that there is insufficient evidence of an offence and therefore no charge should be laid. The investigation would still come within the definition of law enforcement.

Part (b) refers to proceedings where a "penalty or sanction" could be imposed in those proceedings. This includes the imposition of imprisonment or a fine, the revocation of a licence and the issuance of an order requiring a person to cease an activity. A civil action for monetary damages or recovery of debt, as well as internal employment-related investigations where a tribunal could hear the matter **only** at the insistence of the employee would **not** be included.

Part (c) of the definition refers to the actual conduct of proceedings before a court or tribunal.

For example: Prosecution of an offence under the *Criminal Code*, and investigations under the *Ontario Human Rights Code* and the conduct of a hearing before a regulatory tribunal such as the Ontario Securities Commission or the Superintendent of Insurance are included.

Person

The term refers to an individual and to organizations such as business entities and associations.

Personal Information

Personal information means recorded information about an identifiable individual, 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 if 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 if it appears with other personal information relating to the individual or where disclosure of the name would reveal other personal information about the individual.**

Personal information must be about an identifiable individual, however an individual's name need not be attached to the information to qualify as personal information. A physical description or a photograph of a person attached to other personal information about that person is personal information although no name is ever indicated. This individual is "identifiable" and all of the kinds of information described above are his/her personal information.

Generally, information about a property or a specific municipal address, such as market value assessment, hydro-electric consumption or building permit information, is not personal information. However, records containing such property-related information may also contain an individual's name and personal information such as a home telephone number. Care should be taken to ensure that any disclosure of that personal information complies with the privacy protection provisions of the Act (see the Privacy chapter (Chapter 5) for a discussion regarding the disclosure of personal information).

An individual's name on its own is not personal information. To be personal information within the meaning of the Act, the name must be associated with other personal information as defined in s.2.

For example: An individual's name kept by a social services department would be personal information because the fact that the name was on a record at the department might indicate that the person was, or is, in receipt of public assistance.

The term "person" when used in legislation may refer to both individuals and to organizations such as business entities and associations. However, an "individual", which is the term related to privacy rights in the context of FIPPA and MFIPPA, does not include sole proprietorships, partnerships, unincorporated associations, corporations, trade unions or law firms or the names of officers of a corporation writing in their official capacity. Nevertheless records of sole proprietorships and other small businesses such as partnerships may contain information about business entities that is also personal information about individuals.

For example: In a sole proprietorship or family business the finances of the individual may be virtually identical to the finances of the business. Where this is the case, the information in the custody or control of an institution would be subject to the Act's privacy provisions.

Correspondence submitted to an institution by a representative of a group or association is not the personal information of the author of the correspondence if: 1) the correspondence submitted to an institution is on the letterhead of the organization and 2) it is signed by an individual in his/her capacity as a spokesperson of the organization.

However, the information about individuals acting in their business or official capacities becomes personal information when they are affected as private individuals.

For example: The witness statements of by-law enforcement officers who were physically assaulted while acting in their official capacity would contain their personal information.

Personal information also includes opinions and views.

For example: If A expresses an opinion about B, that opinion is part B's personal information. Other views or opinions, which are not about an individual are the personal information of the individual who has expressed the opinion.

Personal information does not include information about an individual who has been dead for more than thirty years (s.2(2)).

The definition of personal information under the Act refers to **recorded** information about an identifiable individual. For the purpose of regulating the collection of personal information under the privacy protection provisions of the Act, personal information includes personal information collected orally on behalf of an institution. This is discussed in detail in the chapter dealing with Privacy (Chapter 5).

Personal Information Bank

s.44, 45 FIPPA / s.34 MFIPPA

A Personal Information Bank (PIB) is a **collection of personal information that is organized and capable of being retrieved by an individual's name or other individual identifier.**

A collection of personal information in the custody or control of an institution would be a personal information bank if it has the following characteristics:

- it must contain personal information;
- information contained in the bank must be a collection of like or similar information about individuals;
- information must be linked to an identifiable individual; and

- the information must be capable of being retrieved by the individual's name or identifying symbol (such as a client identification number).

For example: A public library's circulation records that contain the names, addresses and borrowing records of patrons is a personal information bank.

Usually a personal information bank serves an important administrative or operational function and is used in reaching decisions that affect the individuals in the bank. A number of personal information banks can support one function.

Institutions will often have collections of records containing some personal information, but these do not meet the criteria for the definition of a personal information bank (e.g., records of purchase orders or general correspondence). The Act does not require an institution to rearrange its personal information into personal information banks.

Collections of personal information that meet the characteristics of a personal information bank (as set out above) must be identified and described by the institution. Generally, individuals have a right to information about themselves contained in an institution's personal information banks. These descriptions must be made available to assist the public in exercising privacy rights.

Public Interest

Means the interest of the public in general, not of any individual or group of individuals.

The interest may be a pecuniary one or one by which legal rights or liabilities are affected. It may be an interest in public health or safety or an interest in the maintenance of confidence in the conduct of government or in the administration of an institution.

For example: A breach of security occurring within a sensitive government function, might raise serious questions about how and why the breach happened. If information contained in a record could inform the public in some way about the incident by adding to the information they have to express opinion or to make political choices, it could be considered in the public interest to release it.

Record

s.2 FIPPA / s.2 MFIPPA

A record is **any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, and includes:**

(a) correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine-readable record, any other documentary material regardless of physical form or characteristics, and any copy thereof; and

(b) subject to the regulations, any record that is capable of being produced from a machine-readable record under the control of an institution by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution.

The definition of record is very broad and includes virtually every form of information held in some recorded form by an institution. The definition is not restricted to actual physical documents, but includes records that can be created from existing data in a computer bank. Even documents such as electronic mail are considered to be records. For further information on computer records, see the definition of "machine readable records" immediately below.

Handwritten notes or other notations on records form a part of the records. Working copies and drafts of reports and letters are also records.

Machine Readable Record

s.2, 60 FIPPA / s.2, 47 MFIPPA

s.2 O.Reg.460 /s.1 O.Reg.823

In cases where a request is for information that can not currently be extracted in a way that is useful to a requester, but is capable of being produced from a machine readable record, the Act gives the requester the right (subject to the regulations) to the information which would answer all or part of a request.

If the process of producing a record from a machine readable format would unreasonably interfere with the operations of an institution, the machine readable record would not be included in the definition of a record as outlined above. Unreasonable interference with operations could include instances where normal business activities would have to stop or change in order to produce the record. It may also include instances where the cost of producing the record would result in the inability of an institution to meet its other obligations.

See the regulations for further information.

Third Party

Any person whose interests might be affected by disclosure other than the person making a request for access or the institution. Where the third party is an individual, his/her rights may in some cases be exercised by another person. See the definition of "individual" above.

Use

Use (of personal information): to take action, to employ, to put to use.

Waiver of Notice

s.39(2) FIPPA / s.29(3)(b) MFIPPA

This is a letter signed by the Minister responsible for FIPPA/MFIPPA that allows an institution to forego giving a notice of collection in specified circumstances.

Role of the Responsible Minister and Management Board Secretariat

The Responsible Minister: the minister of the Crown who is designated by order of the Lieutenant Governor in Council under section 3 (subsection 2(1) of FIPPA).

The Responsible Minister is the Chair of Management Board of Cabinet.

The Corporate Freedom of Access and Privacy Office of Management Board Secretariat supports the Chair of Management Board of Cabinet as the minister responsible for FIPPA/MFIPPA. The Office assists institutions that are covered by FIPPA/MFIPPA by providing training, policy and operational advice.

Chapter 2: Administration of the Act

Table of Contents

- Introduction
 - Head of An Institution
 - Head in Municipal Corporations
 - Head in Local Boards and Institutions Other than a Municipal Corporation
 - Delegation of Head's Authority
 - Conflict of Interest
 - Responsibilities of the Head
 - Additional Obligations under FIPPA
 - Information Available to the Public
 - Report to Commissioner
 - Responsible Minister
 - Documents Available to the Public in Accessible Locations
 - Freedom of Information and Privacy Coordinators
 - Records Management
 - Accountability
 - Security and Confidentiality of Records
 - Determining Security Requirements
 - Security Measures
 - Information Technology Security
 - Routine Disclosure/Active Dissemination
-

Introduction

Both the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* and the *Freedom of Information and Protection of Privacy Act (FIPPA)* set requirements that must be met by each institution. In many instances, the head of the institution is responsible for fulfilling these requirements. The requirements concern:

- responding to requests for access to records;
- protecting records from inadvertent destruction or damage;
- protecting personal privacy;
- providing specific information to the Information and Privacy Commissioner (Commissioner); and
- making information available to the public.

In addition, Management Board of Cabinet has issued the Freedom of Information and Privacy Directive that specifies mandatory requirements and responsibilities of institutions administering FIPPA.

Some administrative responsibilities such as publishing the Directory of Records are shared between an institution's head and the Responsible Minister. FIPPA outlines how the Responsible Minister, who has overall administrative responsibility for FIPPA/MFIPPA, is to be chosen. Both Acts set out duties of the Responsible Minister (known in MFIPPA as the Minister/Chair of Management Board of Cabinet).

This chapter provides an overview of the administrative responsibilities of the head of an institution, the Responsible Minister and other issues dealing with the administration of FIPPA/MFIPPA.

Head of an Institution

s.2, 62 FIPPA / s.2, 3, 49 MFIPPA

The head of an institution is responsible for decisions made under FIPPA/MFIPPA by the institution and for overseeing the administration of that Act within the institution. This responsibility includes complying with the access provisions of that Act, and ensuring that personal information held by the institution is accurate, up to date and collected, used and disclosed only as authorized. FIPPA/MFIPPA specify those circumstances where information must be disclosed or access refused, and those cases where the head may exercise discretion.

For FIPPA institutions, the head will either be the minister who presides over a ministry or whomever is designated by regulation. For MFIPPA institutions, the head is the council of a municipality or the board of a local board.

Once the head has been determined, the powers or duties of the head can be delegated to an officer or officers of the institution.

Head in Municipal Corporations

s.3(2) MFIPPA

MFIPPA states that the members of a council of a municipal corporation may designate from among themselves an individual or a committee of the council to act as head for the purposes of this Act. This designation must be enacted by by-law. If no person is designated as head under this section, the head shall be the council.

This power gives a council flexibility in designating who will be the head. The designated head could be an individual, such as the mayor, warden, reeve or councillor, or the head could be a committee of council, such as the executive committee or a special freedom of information and privacy committee. Where an individual is designated, the designation could be to a named individual or to a position, as appropriate.

Careful consideration should be given when deciding who will be designated as the head. The Act requires decisions about access to information to be made in a relatively short time, usually within 30 calendar days. Because of this, the head must be available to make those decisions, unless some or all of the head's duties and powers are delegated. Designating a large committee as the head may present some problems if calling the members together to make access decisions within the 30-day time limit is impractical or difficult.

To revoke a designation, a council would have to revoke the by-law that set out the designation.

Appendix I contains a sample by-law municipalities can adapt to designate the head.

Head in Local Boards and Institutions Other Than Municipal Corporations

s. 3(2) MFIPPA

The Act gives powers similar to those of municipalities to boards and other local institutions in that the members elected or appointed to a board, commission or other body that is an institution may designate an individual or a committee of the body to act as head. If there is no designation, the head shall be the members elected or appointed to the board, commission or other body.

The designation, if it occurs, must be in writing.

For example: The board of a public utilities commission could pass a resolution in writing designating the chair of the commission as the head of the institution.

To cancel the designation, a body should do so in writing.

Appendix II contains a sample written resolution local boards can adapt to designate the head.

Delegation of Head's Authority

s.62(1) FIPPA / s.49(1) MFIPPA

The head, once determined, may delegate some or all powers and duties under the Act. However, even if the powers or duties are delegated, the head remains accountable for actions taken and decisions made under the Act.

The head may delegate the powers and duties in writing to an officer or officers of the institution or, under MFIPPA, of another institution. The delegation would usually be to a position, rather than to a named individual. The document that sets out the delegation should make clear the duties and functions being delegated.

The head may also place limitations, restrictions, conditions or requirements on the delegation. A head may wish to delegate only some of the duties and retain certain decision making authority. Institutions must adhere to the delegation of authority. Where circumstances change, the institution must revise the delegation of authority.

For example: The head may wish to delegate routine duties such as sending out notices (e.g., acknowledgment letters, fee estimates), preparing the annual report, and deciding the fees to be charged, but may retain particularly important duties such as the authority to decide if an exemption from disclosure applies.

Employees who issue notices required by the Act (especially decision letters) must ensure they have the delegated authority to do so. Where an employee of an institution denies partial access to records and does not have the written authority to do so, the institution is deemed to have refused complete access to the records.

Appendix III contains some samples of written delegations under the Act, showing all the powers and responsibilities that may be delegated.

It is important to delegate responsibilities to an officer or officers of an institution who, if required, have access to decision makers and who can act quickly within the time periods prescribed in the Act.

Conflict of Interest

A conflict of interest may exist where a public official knows that he/she has a private interest that is sufficiently connected to his/her public duties to influence those public duties. The focus for conflict of interest is frequently financial matters. It may also arise when the head is meeting his/her decision-making responsibilities under the Act.

A head may be in a conflict of interest situation where it is reasonable to assume that he/she is making decisions based on their personal interest rather than the public interest. In some instances, the conflict of interest may be more apparent than real. It is recommended that delegations of the head's powers reflect the possibility of conflict of interest and provide for alternate decision-makers in those instances.

Responsibilities of the Head

s.10, 11, 24, 25, 26, 27, 27.1, 28, 29, 30, 33, 34, 36, 39, 40, 44, 46, 48, 57 FIPPA / s.4, 5, 17, 18, 19, 20, 21, 22, 25, 26, 28, 29, 30, 34, 35, 37, 45 MFIPPA

The head has certain responsibilities pursuant to the legislation, including:

- adhering to time limits and notification requirements;
- considering representations from third parties;
- providing a response to access requests;
- determining the method of disclosure;
- responding to requests for correction of personal information;
- calculating and collecting fees;
- providing access by the public to manuals and guidelines prepared by the institution;
- where necessary, defending decisions made under the Act at an appeal; and
- administering the privacy protection provisions of the Act.

Additional Obligations under FIPPA

s.44, 46(3) FIPPA

Under FIPPA the head also has an obligation to include in a personal information bank all personal information under the institution's control which is organized or intended to be retrieved by an individual's name or by an identifying number or symbol.

When personal information is used/disclosed on a regular basis for a purpose not listed in the FIPPA Directory of Records, the head must ensure that this use/disclosure is included in the next edition of the Directory.

The head must also retain a record of any use by the institution of personal information in a personal information bank and any new use/disclosure not specified in the Directory of Records. This new use/disclosure must be recorded and attached to the personal information.

Each of the above listed duties will be discussed in more detail elsewhere in the Manual. As well, the duties shared with the Responsible Minister and reporting requirements for the Commissioner are discussed further on in this chapter.

Information Available to the Public

s.31, 32, 33, 35, 34, 36, 45 and 46 FIPPA / s.24, 25, 34 and 35 MFIPPA

A head of an institution must prepare and make available descriptions of the institution's records and personal information banks. These descriptions are intended for use by the public to determine the information generally maintained by each institution. Accurate record descriptions enable a requester to submit a more detailed request, thus simplifying the response process.

For institutions covered by FIPPA, s.36 requires heads to provide to the Responsible Minister, upon request, the information that the Responsible Minister needs to prepare the Directory of Records required by s.31, 32 and 45 of the Act.

The records descriptions of MFIPPA institutions should be made available in a publicly accessible place or a variety of places such as at the head office of a board, in the clerk's office of a municipality and/or at a public library. The descriptions of records can be prepared in a number of ways and can take advantage of existing material. For instance, municipalities and local boards can use annual reports or promotional brochures that describe how their institution is structured and organized. An institution's file plan can be used to prepare the record list.

MFIPPA heads must also ensure that the descriptions of records and personal information banks are kept accurate and up to date.

The description of records and personal information banks must include:

- a description of the organization and responsibilities of the institution;
- a listing of the general types or classes of records in the custody or control of the institution;
- an index describing all the personal information banks in the custody or control of an institution including:
 - the name and location of the personal information bank;
 - the legal authority for it;
 - a description of the types of personal information in the bank;
 - how the information is used on a regular basis;
 - to whom the personal information is disclosed on a regular basis;
 - the categories of individuals about whom personal information is maintained;
 - the policies and practices about the retention and disposal of the personal information;
 - the title, address and telephone number of the head; and
 - the address to which a request for access to records should be made.

Institutions covered by FIPPA have some additional requirements to make information available under s.31, 33, and 46:

- the location of manuals, directories and other material available for public use;
- the location of any institution library or reading room available for public use; and
- whenever personal information is used/disclosed on a regular basis for a purpose not listed in the Directory of Records, the head must notify the Responsible Minister forthwith of the use/disclosure.

Report to Commissioner

s.34 FIPPA / s.26 MFIPPA

The head is responsible for providing the Commissioner with an annual report that sets out the following:

- the number of access requests received;
- the number of requests refused, the provisions of the Act relied upon for refusal and the number of times each provision was invoked;
- for each provision of the Act, the number of appeals commenced;
- the number of times personal information was used or disclosed for a purpose which is not included in the statements of uses and purposes set forth under s.45(d) and (e) FIPPA / s.34 (1)(d) and (e) MFIPPA;
- the amount of fees collected under s.57 FIPPA / s.45 MFIPPA; and
- any other information indicating an effort by the institution to put into practice the purposes of the Act.

The IPC will forward to institutions, the instructions and forms for completing this report.

Responsible Minister

s.2, 3, 31, 32, 35, 39(2), 45 FIPPA / s.2, 23, 24, 29(2), 47 MFIPPA

O.Reg.460 / O.Reg.823

The Lieutenant Governor in Council may by order designate a minister of the Crown to be the Responsible Minister. The Responsible Minister administers FIPPA/MFIPPA.

The Responsible Minister is required to:

- publish the Directory of Institutions, a compilation listing all institutions, including information on where requests can be made and whether institutions have a library or reading room available to the public and if so, its address.
- publish annually a Directory of Records, an indexed listing of general records and personal information banks for FIPPA institutions.

The Responsible Minister also prepares training packages and other products including this Manual, to support the proper administration of FIPPA/MFIPPA.

The Lieutenant Governor in Council may make regulations about such matters as: procedures for access to original records or personal information, forms and standards or safeguards for the security and confidentiality of records and personal information under the control of institutions. The regulations are prepared by the Responsible Minister.

The approval of the Responsible Minister is usually required before a head may forego the legal requirement to notify the affected individual when collecting their personal information. This approval document is called a waiver of notice.

Documents Available to the Public in Accessible Locations

s.33, 35 FIPPA

The head of an institution covered by FIPPA and the Responsible Minister must work together to fulfill their responsibilities under the Act. Cooperation is particularly necessary in making documents and records accessible to the public.

The Responsible Minister must make available to the public generally and in the reading room, library or office designated by each institution covered by FIPPA, the following materials:

- the Directory of Institutions
- the Directory of Records.

The head of a FIPPA institution must make available to the public in the institution's reading room or designated office:

- the manuals, directives or guidelines prepared by the institution which are issued to its officers and contain interpretations of the provisions of the enactment or scheme administered by the institution;
- the instructions and guidelines for officers of the institution in the procedures, methods or objectives in administering or enforcing the provisions of any enactment or scheme administered by the institution that affects the public; and
- the annual report to the Commissioner.

The manuals, directives or guidelines that must be made available are those prepared and used by the institution's staff to determine the eligibility of an individual for a program, changes in status or the imposition of new conditions affecting an individual in a program, or the imposition of obligations or liabilities on an individual under a program.

The requirement to make administrative instructions and guidelines available to the public covers virtually every aspect of procedures, methods or objectives of any program affecting the public.

Manuals and other materials relating only to the internal operation and administration of the institution and not affecting the public, need not be included. This covers instruction manuals for operating equipment or procedures to follow when ordering office supplies.

Guidelines and manuals of administration are subject to the same exemptions as other government records. Portions can be severed if they are exempt from disclosure under FIPPA. Any deletion must include a statement that a deletion has been made, the nature of the information deleted and the provision of the Act authorizing the deletion.

For example: A manual that deals with security precautions or protections for a building that is open to the general public (such as a jail or a laboratory) may have some sections or paragraphs severed for many legitimate reasons.

Other materials not required by the Act that might be helpful in a reading room include:

- record retention schedules;
- file plans; and
- listings of publications in the institution's custody.

Freedom of Information and Privacy Coordinator

Each institution should designate an individual to coordinate freedom of information and privacy activities. This is an important function that assists the institution in meeting its statutory obligations.

The coordinating responsibilities will vary depending on an institution's size, mandate and organization. The function may be a full-time responsibility or a part-time responsibility, assigned to an employee with related duties. The Coordinator's responsibilities may include:

- developing and monitoring procedures for administering the Act, including tracking requests, statistical reporting and ensuring adherence to legislative requirements;
- developing policy recommendations on issues related to the legislation;
- staff training and orientation;
- consulting with line and senior management and legal advisors on interpreting and administering the legislation;
- collecting information for the institution's entry in the Directory of Record or for the General Classes of Records and Personal Information Bank indexes;
- liaisons with the Corporate Freedom of Information and Privacy Office, the IPC and other institutions and central agencies;
- making decisions on requests under the Act (on the delegated authority of the head);
- providing consultation and support related to the Act for any agencies related to the institution; and
- designing measures to ensure the privacy requirements of the Act are honoured.

Records Management

Improvement in records management systems throughout institutions is one of the major long-term benefits of the Act. The public has a right to **expect** that each institution knows what records are in its custody or control and where they are located so they can be retrieved.

The IPC has stressed the need for institutions to develop and maintain up-to-date retention schedules. Search time is reduced significantly if an institution can determine that a record has

been destroyed by consulting a records destruction certificate or other such document. Lengthy searches need not be conducted to determine if a record still exists.

Please see the Access chapter (Chapter 3) for further discussion of records management related topics such as custody and control of records, including political and other elected official's records.

Accountability

An important first step in managing an institution's records is to assign responsibility and accountability for the security of the institution's records. This assignment of responsibility and accountability will vary, depending on size and complexity of the institution. Usually, the manager with direct operational responsibility for a program would be assigned responsibility for safeguarding the records generated by that program.

In larger institutions, an internal auditor or other official could coordinate security matters throughout the organization and provide technical support to individual managers. Smaller organizations may wish to assign responsibility for records security to the chief administrative officer or other responsible position.

However an institution assigns responsibility, this assignment should be documented, and appropriate training and awareness should be provided to staff.

Security and Confidentiality of Records

s.60 FIPPA / s.47 MFIPPA

s.3 O.Reg.460 FIPPA / s.3 O.Reg 823

Regulations can be made setting standards for and requiring administrative, technical and physical safeguards to ensure the security and confidentiality of records and personal information under the control of institutions.

O.Reg.460/823, s.3 requires measures to prevent unauthorized access to an institution's records and to protect against inadvertent destruction of records. The regulations are intended to apply to access and security considerations in the day-to-day administration of an institution's records, rather than access to records in response to requests under FIPPA/MFIPPA.

The head of an institution shall ensure that only those individuals who need a record for the performance of their duties shall have access to it. In most cases, the institution would determine

which staff need to have access to a particular class or series of records in the performance of duties, and take steps to ensure that access is limited to those persons.

If records are inadvertently destroyed before their proper disposal date, as specified on a retention schedule, requesters are deprived of their right of access to those records. The head must therefore take all reasonable steps to protect the institution's records from accidental destruction.

In determining what are reasonable steps, the head should consider all relevant factors, including:

- the media of the record (protective measures appropriate for paper records, for instance, may not be appropriate for other media);
- whether copies of the record exist;
- whether the original copy of the record is inherently valuable (such as archival records or signature documents);
- how vital the record is to the functions of the institution;
- the cost of replacing or recreating the record; and
- the cost of available protective measures.

Although measures to protect records from inadvertent destruction will vary among institutions, some common steps that might be considered include:

- making regular back-up copies (disks, photocopies, microfilm), with a copy stored at a site separate from the original or working copy;
- using fire-resistant file cabinets;
- locating record storage/computer operations away from areas where fire or water damage is more likely to occur (for instance away from exposed pipes);
- raising records and records-producing equipment off the floor to prevent flood damage;
- installing smoke detectors and fire-extinguishing equipment (it should be noted that some automatic fire extinguishing systems such as water sprinklers, may themselves pose a hazard to records and computers); and
- ensuring that storage facilities and maintenance practices are appropriate to the record's media (magnetic media, for instance, are especially vulnerable to inadvertent destruction or damage through improper storage). Similarly because magnetic media is often tied to a particular operating system and set of hardware, data stored on that media may not be usable if the operating system or hardware is no longer available.

As with other measures, the institution should document steps to ensure against inadvertent records destruction.

Determining Security Requirements

Before establishing measures protecting records from unauthorized access, an institution should determine the degree to which access to its records should be controlled. Although it may be necessary to determine appropriate levels of access to individual documents or files, usually this

determination would be on the basis of record series. When considering access controls for record series, the level of security should be appropriate for the most sensitive information in the series.

All relevant factors should be taken into account in determining whether access to records should be controlled, and the scope and extent of those controls, including:

- whether or not exemptions are likely to apply to the records;
- the nature of the exemptions (mandatory or discretionary) which may apply;
- the circumstances under which the records were supplied to or created by the institution;
- possible harms which may result from unauthorized access;
- the need to protect the records from tampering; and
- the need to protect unique or original records.

Security Measures

In identifying security measures, the head should balance the cost and complexity of such measures against the possible harms resulting from unauthorized access. Security measures should be appropriate to the nature of the record and to the level of security required.

For paper records, security measures can include:

- clean desk policies, where desks are locked when unattended;
- locking filing cabinets, which are locked when unattended, and where key distribution is limited and documented;
- central file stations, with log-in and log-out procedures for files, accompanied by restriction on the making of copies;
- locked file room with access controlled by file room staff;
- coded file labels, labels using numeric or alpha-numeric codes rather than descriptive texts;
- inclusion of security provisions in contracts with outside suppliers of records storage and disposal services;
- record distribution/circulation policies which limit the production and circulation of records to staff on a need-to-know basis; and
- policies and procedures for using facsimile machines, including policies on types of information which should not be faxed, staff access to and physical placement of the fax machine. Checking procedures such as ensuring that the document is being sent to the correct number prior to sending documents should also be developed. The IPC has prepared guidelines on the use of facsimile machines which may be consulted.

Information Technology Security

For FIPPA Institutions, Management Board of Cabinet, has approved the: "Information Technology Security Directive". The purpose of this directive is:

- To ensure that ministries and agencies safeguard confidential information as well as the integrity and availability of data while it is created, entered, processed, communicated, transported, disseminated, stored or disposed of through information technology.
- To promote and maintain among ministry and agency staff an awareness of the security requirements of information technology resources.
- To define the responsibilities and mandatory requirements for developing, implementing and managing security measures for information technology resources.

This directive applies to all ministries and all Schedule 1 agencies unless exempted in a Memorandum of Understanding.

This directive applies to:

(a) Ministry and agency information in electronic form;

(b) All ministry and agency information in paper form or otherwise not in electric form, when such information is under the operational control of a provider of information technology services.

Note: A guideline entitled "Information Technology Security: A Manager's Guide" has also been published to assist in putting the directive into practice.

Factors for all institutions to consider in determining whether access to records should be controlled, and the scope and extent of those controls, include:

- positioning terminals in such a manner that passers-by cannot read information displayed on screen;
- password protection for computer hardware, with policies in place governing the assignment, use and deletion of user identifications and passwords;
- encryption of transmitted data or developing guidelines for transmitting confidential information, for example, guidelines for the use of electronic mail;
- tracking systems which monitor the use of data, and which identify system user; and
- inclusion of security provisions in contracts with outside suppliers of information technology services.

Routine Disclosure/Active Dissemination (RD/AD)

RD/AD are separate concepts but are both ways of providing greater access to government information. Routine disclosure occurs when a request for a general record can be granted routinely either inside or outside of the formal access process prescribed by FIPPA or MFIPPA. Active dissemination occurs when information or records are periodically released (without any request) pursuant to a specific strategy for release of information.

RD/AD can be an important part of an institution's commitment to easier, faster and more cost-effective access to records. While not specifically mandated in FIPPA/ MFIPPA, s.63(1) FIPPA /

s.50(1) MFIPPA provide for the disclosure of information outside of the formal access process - for example, through oral requests or in the absence of requests.

The IPC and MBS jointly published 2 papers that provide advice and examples on enhancing access to government information through the employment of RD/AD practices. These publications are available through the IPC.

Chapter 3: Access Procedures

Table of Contents

- Introduction
- Right of Access
 - Severability
- Confidentiality Provisions
- Excluded Records
- Existing Information Practices
 - Copyright Act
- Obligations to Disclose
 - Grave Environmental, Health, or Safety Hazard
 - Compelling Public Interest
- Requests Under the Act
 - What is a Request?
 - Clarifying Requests
 - Who Can Make a Request?
- Processing Requests
 - Continuing Access
 - Time Limits
 - Receipt of Request and Opening Request File
 - Do you have the Record?
 - Forwarding/Transferring Requests
 - Forwarding
 - Transferring
 - Records of other Governments
 - Shared Interest in a Request
- Locating and Reviewing Records
 - Search for Records
 - Time Extensions
 - Notices to Affected Third Parties
 - Fee Estimates/Interim Notices
- Granting and Denying Access
 - Access to Original and Copying
 - Granting Access to Records in Whole
 - Denying Access to Records or Parts of Records
 - Refusing to Confirm or Deny the Existence of a Record
- Access to Own Personal Information
 - Identification Required for Access
 - Comprehensible Form
 - Correction of Personal Information
- Checklist of Steps in Processing a Request

Introduction

This chapter addresses the requirements for providing access to a record in accordance with the *Freedom of Information and Protection of Privacy Act* (FIPPA) or the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA). The obligation of the head to disclose a record where there has been no request, the right of access to general information and the procedures for processing requests for personal information under FIPPA/MFIPPA are discussed. The particular requirements that apply to requests for personal information and to requests for correction of personal information are considered. The procedures to be followed in notifying the requester of decisions reached and in notifying third parties are also outlined.

Right of Access

s.10, 47, 63, 65, 69 FIPPA / s.4, 36, 50, 52 MFIPPA

O.Reg.460, s.2, s.5 FIPPA / O.Reg.823, s.1, s.5 MFIPPA

The right of access applies to existing records, in whole or in part, that fall within the custody or control of an institution (for further information on custody and control see the Introduction (Chapter 1) of this manual). Certain limitations on access to records exist in the form of the exemptions, exclusions, confidentiality provisions and the determination that the request is frivolous or vexatious. There is no obligation to create a record in response to a request under FIPPA/MFIPPA, except in certain circumstances involving information maintained on a computer. Despite these limitations to access, denial of access to records should be the exception. While an institution may not have a duty to create a record, it may wish to do so where it is consistent with the spirit of the Act.

In addition, an individual has a legal right of access to personal information about him/herself. The right of access to personal information is subject to the exemptions discussed in the related sections and the exclusions mentioned below.

The Act does not require that records be translated into the language of the requester. The *French Language Services Act* does require any communications with the requester including notifications, be made in the language of the request (French or English) for provincial bodies covered by this legislation. Some municipalities and local boards offer services in a number of different languages as a courtesy. When responding to requests, institutions should follow the policies and practices set by their respective organization.

Other points to note regarding the right of access:

- FIPPA/MFIPPA apply to any record that exists in the institution regardless of whether it was created prior to the Act taking effect. Although different requirements concerning

disclosure of records may have been imposed pursuant to earlier legislation, once FIPPA/MFIPPA came into force, these records were also subject to the Acts.

- Some federal acts such as the *Young Offenders Act* and the *Criminal Code* have disclosure or non-disclosure provisions that serve to exclude specified records from FIPPA and MFIPPA.

For more information on the right of access please see *Who Can Make a Request?* further on in this chapter.

Severability

s.10(2) FIPPA / s.4(2) MFIPPA

When information falls within an exemption and can reasonably be severed from the record, s.10(2) FIPPA / s.4(2) MFIPPA provides the requester with a right of access to the remainder of the record. The process of severing is important in processing a request under the Act.

One method of severing is to blank out the exempt information from a photocopy of the record, using a black marker, and releasing a copy of the severed photocopy to the requester. This second photocopy step is necessary because print can be seen through black marker.

Alternatively, removable white tape could be put over the exempt portions of the record and a photocopy made for release to the requester. A copy should be made and retained by the institution before the tape is removed.

Generally, the smallest unit of information to be disclosed after severing is a sentence. But even where only a sentence remains, some information, such as a name, might be removed and the remainder released.

Severing does not apply where the Act specifically exempts from disclosure an entire class of records such as a Cabinet agenda or the minutes of a qualified in-camera meeting. In all cases, the information in a record must be assessed to determine whether portions are severable.

When information is severed from a record, the notification to the requester must specify the section(s) of the Act under which access to the severed information is refused. One way to accomplish this notification is by inserting the subsection number in the space remaining after the information has been severed from the record or in the margin. As well, where information must be severed from a record, it is not feasible to allow a requester the option of viewing the original.

Confidentiality Provisions

s.67 FIPPA / s.53 MFIPPA

The Acts prevail over confidentiality provisions in any other act unless the other act or FIPPA/MFIPPA specifically provide otherwise.

The confidentiality provisions that prevail over MFIPPA are:

- *Municipal Elections Act, R.S.O. 1990, c.M.53, s.105.*

This subsection deals with the contents of the ballot box in the custody of the Clerk.

The confidentiality provisions that prevail over both FIPPA/MFIPPA are:

- *Assessment Act, R.S.O. 1990, c.A.31, s.53(1).*

This subsection deals with records derived in the course of determining the value of real property and what assessment should be made.

The confidentiality provisions that prevail over FIPPA are:

- The additional confidentiality provisions include *the Child and Family Services Act, Colleges Collective Bargaining Act, Courts of Justice Act, Labour Relations Act, Occupational Health and Safety Act, Pay Equity Act, Public Service Act, Securities Act, Commodity Futures Act, Statistics Act and Vital Statistics Act*. Please refer to s.67 of FIPPA for details.

Excluded Records

s.65 FIPPA / s.52 MFIPPA

Certain categories of records are outside the application of FIPPA or MFIPPA. Access to these records is determined by considerations such as access provisions in other Acts. In order to make a decision on whether an exclusionary provision applies, an institution must first determine that the records in question meet criteria provided in the relevant legislation or developed by the Information and Privacy Commission (IPC). Even if an institution makes a determination that a record is excluded from FIPPA/MFIPPA, it must issue a decision letter to that effect since the decision is still subject to appeal to the IPC.

FIPPA does not apply to:

- clinical records or treatment related records of psychiatric facility patients as defined in the *Mental Health Act*.
- notes prepared by or for a person presiding in a proceeding of a court of Ontario if those notes are prepared for that person's personal use in connection with the proceeding.
- anything contained in a judge's performance evaluation under s.5.11 of the *Courts of Justice Act* or to any information collected in connection with the evaluation

- a record of the Ontario Judicial Council whether in the possession of the Judicial Council or of the Attorney General if certain conditions are present.

FIPPA and MFIPPA do not apply to:

- records in the Archives of Ontario or the municipal archives where the records were provided by private donors or by an organization other than institutions defined in the Act.
- most labour relations related records and to much employment-related information in which the institution has an interest.

The 1995 *Labour Relations Act* (Bill 7) amended FIPPA and MFIPPA to exclude most employment-related and labour relations records from the legislation - see s.65(6) of FIPPA and s.52(3) of MFIPPA. FIPPA/MFIPPA does not apply to:

Records collected, prepared, maintained or used by or on behalf of an institution in relation to any of the following:

- (a) Proceedings or anticipated proceedings before a court, tribunal or other entity relating to labour relations or to the employment of a person by the institution.
- (b) Negotiations or anticipated negotiations relating to labour relations or to the employment of a person by the institution between the institution and a person, bargaining agent or party to a proceeding or an anticipated proceeding.
- (c) Meetings, consultations, discussions or communications about labour relations or employment-related matters in which the institution has an interest.

Nonetheless, under s.65(7) FIPPA / s.52(4) MFIPPA the following records are still covered by the Acts:

- (a) An agreement between an institution and a trade union.
- (b) An agreement between an institution and one or more employees which ends a proceeding before a court, tribunal or other entity relating to labour relations or to employment-related matters.
- (c) An agreement between an institution and one or more employees resulting from negotiations about employment-related matters between the institution and the employee or employees.
- (d) An expense account submitted by an employee of an institution to that institution for the purpose of seeking reimbursement for expenses incurred by the employee in his/her employment. If such orders are released, this chapter, as well as others, will be updated.

Existing Information Practices

s.63 FIPPA / s.50 MFIPPA

A head may provide information without a formal request under the Act. The Act is not intended to replace the normal process of providing information. Providing information in response to informal oral or written inquiries should continue. The Act should only be used by the public in cases where information is not available through the usual channels. However, when a request is made in writing under the Act and the appropriate application fee is paid, the time limits and procedures in the Act for responding must be followed.

The legislation allows the head of an institution to release information voluntarily in the absence of a request, or in response to an oral request, provided that nothing in the Act prohibits the release of that information. Access to information (except personal information) that was available by custom or practice immediately before the Act came into place is preserved. Pre-existing access must be to the public at large not a select group. Access to records by the parties to an action does not constitute access by the public at large.

For example: Section 73 of the *Municipal Act* requires the clerk to maintain certain official records of the municipal corporation. S.74 states that the clerk shall provide access to the records specified in s.73 to any member of the public, subject to MFIPPA. This means that pre-existing access continues except in respect of personal information. Therefore, if a record falls under the pre-existing access provision, a formal request under the Act is not necessary.

The same provision exists in legislation establishing regional municipalities, the District Municipality of Muskoka, and the Restructured County of Oxford.

Personal information cannot be released as part of previously existing information practices.

Copyright Act

Subsection 27(2)(i) of the federal *Copyright Act* provides that the disclosure of a record pursuant to a freedom of information request is not a violation of copyright. Therefore, this provision means that copies of architects' plans, drawings or specifications may be provided in response to a request under FIPPA/ MFIPPA, unless another exemption applies to the record.

The person to whom the record is provided would still be bound by copyright. When providing access to architects' records, an institution should:

- stamp all plans released under the Act with the phrase "Copyright Act applies to use and reproduction"; and
- ensure that the author is associated by name with the document by including the title block or other indication of authorship on copies of documents released.

Freedom of Information and Privacy Coordinators should also note that their own institution may hold a copyright on works it has created. For example, records generated by a Ministry may be protected by Crown Copyright.

Obligations to Disclose

Grave Environmental, Health, or Safety Hazard

s.11 FIPPA / s.5 MFIPPA

The Act requires the head to disclose a record - either to the public or the persons affected - that reveals a grave environmental, health, or safety hazard to the public, and where it is in the public interest to do so. In this provision where the duties and responsibilities belong to the head alone:

- "grave" means serious, likely to produce great harm or danger;
- "public interest" includes the interests of the local community in general and not of any particular individual or group of individuals; and
- the information must be in record form.

This section overrides every other provision of FIPPA/MFIPPA.

If these conditions are met, and the head has reasonable and probable grounds to believe that this hazard exists, the record must be disclosed as soon as possible. There is no requirement that a request under the Act be made before the head is required to act.

For example:

Where the head possesses records indicating that a beach is unsafe because of high levels of pollution, he or she is obliged to alert the public to the danger.

Before disclosing a record, the head must give notice to any person to whom information in the record relates if it is reasonable to do so in the circumstances. A "person to whom the information relates" includes a third party who will be affected by the release. The head must weigh any harm that the delay in disclosure would create against any possible unfairness to the person to whom the information in the record relates. The notice indicates that the head intends to release a record or part of a record that may affect the interests of the person and a description of the record or part relating to the person. The notice also states that the person may make representations forthwith to the head why the record or part should not be disclosed.

Where notice is given, the person may make representations forthwith to the head concerning why the records or part should not be disclosed. "Forthwith" means immediately. Due to the urgency of the circumstances contemplated, the head is not required to wait for any prescribed period before disclosing the record or obtaining any representations. There is no provision for an appeal to the IPC. There are fewer formal requirements in the notification procedure set out in s.28 FIPPA / s.21 MFIPPA.

For example:

The requirement to give notice could be fulfilled by telephoning the person to whom the record relates.

This section applies despite any other provision of the Act.

Compelling Public Interest

s.23 FIPPA / s.16 MFIPPA

Even where certain exemptions apply to a record, disclosure may still be required if a compelling public interest in the disclosure of the records clearly outweighs the purpose of the exemption.

This provision applies to the following exemptions including two of the three mandatory exemptions for FIPPA and all three mandatory exemptions for MFIPPA:

- Advice or recommendations;
- Relations with governments;
- Third party information;
- Economic and other interests;
- Danger to safety or health of an individual; and
- Personal privacy.

This section does not apply to exemptions dealing with records of closed meetings or Cabinet records, law enforcement, solicitor-client privilege, or published information. Both the head of the institution and the IPC can determine if the compelling public interest provision applies to the disclosure of a record.

The interest in disclosure must be compelling, i.e. strong or overwhelming. The public interest must also clearly outweigh the purpose of the exemption. There is a balancing required by weighing the public interest against the purpose of the exemption. The results of that balancing test must be clear and definitive.

In considering whether to release a record in the public interest, a head must first determine whether an exemption applies, that is, whether facts exist which bring the record within the exemption in question. If the head determines that one of the mandatory exemptions applies, he/she must then consider whether the public interest prevails over the interest in confidentiality. Where a discretionary exemption applies and the head decides not to exercise his/her discretion in favour of releasing the record, the head must then consider whether the public interest outweighs the purpose of the exemption.

If the test is met, the record would be released, although certain procedural steps have to be followed by the head (but not by the IPC) for certain exemptions.

For example: Before information which is exempt under s.15 FIPPA / s.9 MFIPPA (relations with other governments) can be released by the head in the public interest, the approval of the Executive Council is required for FIPPA institutions or the approval of the affected government itself is required for MFIPPA institutions.

Before information which is exempt as third party information or as personal information can be released in the public interest, the notification requirements in s.28 FIPPA / s.21 MFIPPA which apply to those two exemptions must be followed.

Where a requester urges the application of "compelling public interest" on an appeal to the IPC, the requester carries the onus of proof, because of the general legal principle that a party asserting a right or duty bears the onus of proof. The IPC has stated however, that this onus cannot be absolute in the case of an appellant who has not had the benefit of reviewing the requested records before making submissions.

Requests Under the Act

s.24, 25, 26, 48, 66 FIPPA / s.17, 18, 19, 37, 54 MFIPPA

O.Reg.460s.5(2) FIPPA / O.Reg.823s.5(1) MFIPPA

What is a Request?

Under the Act, an access request must be made in writing, be accompanied by the \$5.00 application fee and provide sufficient detail to enable an experienced employee of the institution to identify the record(s) requested. If an individual is seeking access to his/her own personal information, the request must also identify the personal information bank or the location of the personal information being requested. If, after a thorough search, the institution cannot locate the requested personal information and the requester cannot provide any credible evidence to support the existence of records, the head may conclude that the institution does not have the records.

Sometimes a request might be in the form of a question. For example, a requester might write, "Does this institution have any information on tenders?" In this situation it is unlikely that the institution could determine what information the requester wants. For this reason, requests in the form of questions are not generally acceptable and should be clarified with the requester before proceeding to process the request.

There is a prescribed form for access requests, however, a letter that makes reference to the Act would be considered a request if accompanied by the required application fee of \$5.00. If an institution is in doubt about whether or not a requester wishes a letter of inquiry to be treated as a request under the Act, the requester should be contacted and clarification of the inquiry obtained.

A request for access to hardcopy records must be for records that exist at the time a request is received. There is no requirement to compile information from a number of records to create a new hardcopy record in response to a request.

For example: A requester might ask to see a copy of an audit report of a planning board. It might be that an audit report was never prepared by the planning board. If this is the case the planning board would not be obliged to prepare one to satisfy the request.

If requested information exists in a group of records it would still be considered a request despite the fact that the original request was for a record in a format that did not exist. In this case the institution must identify and advise the requester of the existence of the related records.

For example: A list of the names and addresses of all non-profit organizations that have applied to operate a charity casino in a municipality may not exist. However, if all non-profit organizations completed an application form in order to obtain this licence, the application forms taken as a group would constitute the requested information in record format.

An institution might get a request for access to a record that was destroyed according to its records retention schedule. In response to a request for the record, the institution would advise the requester that the record does not exist.

A request may also be made for access to records that are capable of being produced from a machine-readable record using the hardware, software and technical expertise normally used by the institution.

For example: An institution may generate a report in a certain format from data in a computer file. A requester under the Act may ask for a different kind of report using the same computer data sorted or presented differently.

According to s.2 FIPPA / s.1 MFIPPA of the regulations, requests for machine readable records are subject to the ability of an institution to produce them without unreasonably affecting its day-to-day operations.

Where the information requested is personal information, the computer record must be made available in comprehensible form i.e., a record which merely shows computer codes rather than information intelligible to the requester would not be in comprehensible form.

Finally, if a formal access request can be better handled by an institution on an informal basis, the institution should contact the requester to determine whether he/she is agreeable to this change. An agreement to request a record on an informal basis generally results in quicker access to the records but removes the opportunity to appeal the institution's decisions at a later date.

Clarifying Requests

A request may not sufficiently describe the record sought and therefore may not be considered a "complete request".

An institution that receives a broadly worded request has three options:

- respond literally to the request, which may involve an institution wide search for the records;
- request further information from the requester in order to narrow its search; or
- narrow the search unilaterally, outlining the limits of search to the requester

Clarifying a request is helpful to both the institution and the requester. The institution should notify (see notification no.1, in Appendix IV, Sample Notification Letters) or telephone the requester and offer assistance in reformulating the request to identify the general class or type of record and the institution with custody or control of the record. After a request has been clarified it should be clear to each party what records are being requested. For an institution this means that an experienced employee will be able to identify the records sought.

For example: A requester might ask to see "all the minutes that the Hydro-Electric Commission has". Does this mean all the board minutes, the committee minutes, or both? For what year?

In the example above, the requester may be interested in only the board minutes for a particular date or date range, not all of the minutes that exist. By clarifying the request the institution could save considerable time searching through records and preparing them for release. It would also save the requester considerable costs if a fee is charged.

The records descriptions and descriptions of personal information banks can be used to help clarify requests.

Who Can Make a Request?

Any person can make a request for access to records. In this instance a person includes individuals and organizations such as corporations, partnerships and sole proprietorships. The right of access is not limited by citizenship or place of residence.

There may be situations where one person represents another individual. The Act provides that any right or power conferred on an individual by the Act may be exercised by:

- the personal representative of a deceased individual only if the exercise of the right or power relates to the administration of the individual's estate. The personal representative would be the executor named in a will or if there is no will, the administrator appointed by a court;
- a guardian for a person if one has been appointed or the person's attorney under power of attorney, or the Public Guardian and Trustee. A guardian can be appointed by a court for an individual who is incapable of managing his/her own affairs. The Public Guardian and

Trustee may become an individual's guardian under the *Mental Health Act* or the *Substitute Decisions Act*;

- the person having lawful custody of a child under the age of sixteen; or
- a person with the written consent of the individual (that has been verified).

The rights and powers which an individual may exercise include the right to make access requests, the right to consent to the collection, use and disclosure of personal information and the right to request correction of personal information. Requests made on behalf of an individual by a person or an organization that has that individual's written consent are considered to be a personal information request.

Processing Requests

s.24, 25, 26, 28 FIPPA / s.17, 18, 19, 21 MFIPPA

Processing requests is an administrative function that requires knowledge about the legal requirements of the Acts and the institution's programs and records management practices.

FIPPA/MFIPPA have specific time restrictions that must be met. The Acts also require that certain statistical records about requests be provided to the IPC on an annual basis. The actions and decisions taken with respect to a request should be documented in case they are later challenged.

A records management system that includes a filing system and storage, retrieval and records retention procedures will help an institution process requests for access to information. It is not acceptable for requesters to be denied access to records that they would otherwise be entitled to receive, solely on the basis that the institution's records management systems are inadequate or deficient.

In order to conform to the request processing time limits set in FIPPA/MFIPPA it is important to record the date that a request is received and to devise a method of tracking individual requests. FOI Coordinators often maintain a descriptive profile of each request that helps them refer back to previous requests for records and reporting requirements for the IPC. A carefully considered descriptive profile of requests or of the type of requests received can also be of internal use when justifying staff and budgets or when examining procedures for handling requests.

For example: Keeping records on the numbers and types of access requests received can help a coordinator determine whether certain records (such as severed building permits) are being requested frequently enough that they might be more efficiently provided outside of the formal request process as a routine disclosure item.

Requests for Continuing Access

Under FIPPA only, a requester may indicate in a request for access to general records that it shall, if granted, continue to have effect for a specified period up to two years. Continued access is based on the existence of the record at the time the request is received by the institution. This does not apply to a request by an individual for personal information about him/herself under sections 47 and 48.

If access to the record is granted, the institution provides the person with a proposed schedule of dates for disclosure. The test for frequency is one of reasonableness. The schedule indicates why the particular dates were selected. The schedule also contains a statement that the requester may ask the IPC to review the schedule.

For example: A requester may be granted access to a report and request any updates to the report over the next year. If the report is quarterly, a quarterly schedule for disclosure would be proposed to the requester.

Continuing access is contemplated for records which are likely to be produced and/or issued in series. It is not intended to provide ongoing access to the kind of records of which only one edition is produced. The discussion to grant access to the original request need not automatically be applied on the subsequent dates in the schedule.

In dealing with this type of "continuing request", the Act applies as if a new request were being made on each of the dates in the schedule therefore an application fee of \$5.00 is required for each of the dates in the schedule. In practical terms, the original request is brought forward on each of the dates listed in the schedule and processed as if it were a request made on that day.

If access to the request is denied, there is no obligation to grant continuing access.

Time Limits

In general, access requests must be responded to within 30 calendar days from the date a complete request is received. A complete request is one which has been clarified or one which provides sufficient detail to allow the institution to understand what information is being requested. The \$5.00 application fee must also have been received. The 30-day time period starts to run the day the institution receives a complete request. If a time limit under the Act expires on a Sunday or statutory holiday, it is extended to the next day which is not a Sunday or statutory holiday. If the time limit expires on a Saturday, the response date becomes the preceding Friday.

Where an institution receives a broad request which is subsequently narrowed by the requester, the 30-day time period begins on the date the original broad request was received. A broad request is deemed to be narrowed, not clarified if it originally provided the institution with sufficient detail regarding the nature of the records being requested and is now simply being reduced in scope.

For example: An individual requests the results of a police investigation, including all correspondence between the police agency and an outside organization relating to a specific case. The requester later limits his request to one specific report regarding the case. This request would be considered narrowed and not clarified. The original request contained sufficient detail for a staff person to identify the records. In this case, the 30-day time limit would begin on the day the first (broad) request was received.

An example of a request that needs clarification can be found earlier in this chapter under the heading Clarifying Requests.

The time limit for responding to a request is automatically extended where notice is given to a third party.

For example: An institution that receives an access request where a third party must be consulted is required to notify that third party within 30 days of receiving the request. This initial time period allows the institution time to gather the records, make a determination that a third party must be consulted and define exactly what the third party must be consulted about. The third party is allowed 20 days to respond to this notice. Upon receipt of the third party's response, the institution has a further 10 days to make its final decision about the requested records. Under normal circumstances then, an institution would have up to 60 days to respond to an access request that involves third party notification.

Institutions that wish to courier materials to requesters and third parties should note that courier companies cannot deliver to a post office box. A street address is required.

All of the above mentioned time limits are maximums; a faster response may be possible. Under certain circumstances time extensions are also possible. These circumstances are discussed in detail later in this chapter.

Receipt of Request and Opening Request File

The first step an institution should take when a request is received is to stamp the date on the request. This is important because of statutory time requirements. Requests arriving at an institution should be routed quickly to the access and privacy coordinator to ensure that time is not wasted in the internal mail process. As a courtesy, a notice should be sent as soon as possible to the requester acknowledging receipt of the request.

Once the person responsible for dealing with access requests receives the request, a file should be opened. The file cover can be printed with information that will help route the file if it must be sent to other divisions of the institution. If return dates are filled in on the folder this will help keep people aware of the time deadlines. The file folder can also serve as a record of the decisions taken with respect to the file. To help track requests for access to records it is a good idea to have a different coloured folder for freedom of information and privacy matters.

A tracking and recording form is useful to record the actions taken to process a request. It allows the institution to know at a glance how a request was processed and what decisions were made with respect to the file. Also, by keeping a recording and tracking form, it is evident what has to be done to complete the file.

Do You Have the Record?

Detailed explanations of the terms "custody" and "control" are provided in Chapter 1 of this manual. These definitions help to establish if an institution has a record subject to the Act, and hence a responsibility for responding to a request. In determining "custody" or "control" an institution must consider all aspects of the creation, maintenance and use of particular records.

For example: Records of the public works department of a municipality would be both in the custody and under the control of the municipality.

Political records belonging to a municipal councilor or elected official of a board or commission or a Minister's staff may come within the custody and control of an institution if these records are integrated with other files held by the institution. When no steps are taken to separate the maintenance and storage of political records from an institution's records and an employee of the institution has responsibility for their care, these records are subject to the Act.

In addition, where a record in the custody or control of an elected official is communicated to an officer or employee of an institution, the record may now be considered to be in the custody and control of the institution.

In the examples above, the Act might apply to the records because the institution would have either custody or control of the records (or both).

The following questions can be used to determine custody or control. This is not an exhaustive list of possible considerations:

- was the record created by an officer or employee of the institution?
- what was the intended use of the record?
- does the institution have possession of the record either because it has been voluntarily provided by the creator or pursuant to a mandatory statutory or employment requirement?
- if the institution does not have possession of the record, is it being held by an officer or employee of the institution for the purpose of his/her duties as an officer or employee?
- does the institution have a right to possession of the record?
- does the content of the record relate to the institution's mandate and functions?
- does the institution have the authority to regulate the use of the record?
- to what extent has the record been relied upon by the institution?
- how closely is the record integrated with other records of the institution?
- does the institution have the authority to dispose of the record?

For example: Records of FIPPA institutions at the Archives of Ontario are in the custody and control of the archives.

Records in the custody of lawyers privately retained by a ministry or agency may still be in the control of the institution.

If an institution has custody or control of the records and will be responding to a request for access to records, it would proceed to gather and review the records to determine what will, or will not, be released.

Institutions may receive requests for records in their custody or control but which would be more properly handled by another institution. The institution receiving such a request should confer with the institution that has the greater interest in the record to determine whether it should transfer the request or answer the request itself.

Forwarding / Transferring Requests

Forwarding

s.25(1) FIPPA / s.18(2) MFIPPA

In some cases access requests will be sent to an institution that does not have the responsive record "in its custody" or "under its control". When such a request is received the institution has an obligation to:

- determine if another institution has either custody or control of the record;
- if so, forward the request to that institution along with the application fee; and
- give written notice to the requester about the new contact.

The term "forward" is used when an institution sends the request to what should have been the proper institution.

An institution has 15 calendar days from the date a "complete request" is received to forward the request. The 30-day time limit begins when the request is received at the first institution. Due to time constraints, institutions forwarding a request should immediately telephone the Freedom of Information Coordinator at the second institution. This will give the second institution more time to locate records that are responsive to the request.

The second institution that receives the request has the remainder of the 30-day period to respond. For this reason, it is important to choose a fast and reliable method of forwarding a request. The time for responding does not stop running while the request is in transit, however the second institution may send a notice to an affected third party, require a time extension, or issue a fee estimate, all of which would change the original deadline.

An institution that does not have a requested record must make "reasonable inquiries" to determine if another institution has the record. Determining what constitutes "reasonable inquiries" depends on the circumstances.

For example: A regional municipality might receive a request for information about a program run by a local municipality in the region. If the region knows that the matter is a local responsibility it would be reasonable to expect that the region would contact the local municipality to see if it is appropriate to forward the request to that local municipality.

Under the Acts a request can be forwarded to an institution covered by either FIPPA or MFIPPA.

To assist institutions in determining where to forward a request, the *Directory of Institutions* lists the institutions covered by both FIPPA and MFIPPA.

If an institution does not know where to forward a request, it should inform the requester of this and indicate what steps were taken to make the inquiries.

Transferring

s.25(2) FIPPA / s.18(3) MFIPPA

In some cases more than one institution will have copies of the requested record(s). An institution might determine that another institution has a greater interest in the record. In that case the request may be "transferred" to the second institution along with the application fee. An institution is under no obligation to transfer the request, but may do so if it wishes.

Another institution has a greater interest in a record than the institution that received the request if:

- the record was originally produced in or for that institution; or
- the record was not originally produced in or for an institution, the other institution was the first institution to receive the record or a copy of it.

For example: Both a municipality and provincial government ministry might have a copy of an environmental impact study that was originally prepared for the provincial government. In such a case the municipality might decide to transfer the request to the provincial ministry.

If an institution believes that the institution that created a record might exempt all or part of a record from disclosure to the record, the first institution might consider transferring the request to the second institution.

When a request is transferred, the same rules regarding time limits apply as with forwarding a request.

Records of Other Governments

An institution cannot forward or transfer a request to a federal department. The requester must be instructed to re-submit the request under the federal *Access to Information Act* or the *Privacy Act*.

For example: All records of indictable criminal convictions, supported by fingerprints are held by the RCMP. While Provincial and Municipal police agencies have access to Criminal History information, an individual requiring an official copy of their own history must be directed to submit such a request to the RCMP, supported by their fingerprints. If the request was made to a Municipal or Provincial police agency, it cannot forward or transfer such a request. The request must be re-submitted to the RCMP.

Shared Interest in a Request

When it is determined that more than one institution has records responsive to a request, the institution that received the request should inform the requester of this fact. The requester should be provided with the names and addresses of contacts in the other institutions.

Locating and Reviewing Records

s.24(4), 26, 27, 28, 57 FIPPA / s.19, 20, 21, 45 MFIPPA

s.6, 6.1, 7 O.Reg 460 / s.6, 6.1, 7 O.Reg 823

When an access request is received, the institution must search for the requested records, examine them and decide what will be released. During the review of the records, an institution may find it necessary to extend the time period to respond to a request, notify affected parties and/or issue a fee estimate. In these instances the time period for processing the request is suspended or extended.

Search for Records

Searches for records responsive to a request should include, where practicable, enquiries of staff responsible for the issue at the time the records were created or might have been created.

The following should also be considered when searching for records:

- identify the specific files and data banks that should be searched;

- ensure that if a requester claims certain records should exist, they have been searched for in the appropriate files; and
- establish whether other files and data banks including e-mails and those of alternative media might contain records responsive to the request.

An institution should be prepared to verify in an affidavit, the steps taken to locate a record.

Time Extensions

A head may extend the time limit set out in s.26 FIPPA / s.19 MFIPPA for a period of time that is reasonable in the circumstances, where:

- the request is for a large number of records or necessitates a search through a large number of records and meeting the time limit would unreasonably interfere with the institution's operations. Note that an interference with operations posed by meeting the time limit is not an independent ground on which to base a time extension. An extension can only be claimed if the request is for a large number of records or necessitates a search through a large number of records and meeting the time limit would be an unreasonable interference.
- consultations that cannot reasonably be completed within the time limit are necessary to comply with the request. Consultations in this context do not include consultations within an institution, but may include consultations between or among institutions.

Examples of time extension are:

An institution receives a request for a large number of records that requires careful review by the individual acquainted with the records and this individual can only be available on a part-time basis.

A municipality might have to consult with the provincial government to determine if s.9 of MFIPPA (relations with governments) applies to the requested records.

An institution should consider all of the potential factors that may contribute to the need for the length of a time extension. The time limit in section 26 FIPPA / s.19 MFIPPA can only be extended once. Further, when assessing the length of time of the extension, the institution must make its decision regarding time required within the initial 30-day time period prescribed in section 26 FIPPA / s.19 MFIPPA.

All requests for extension of time must be reasonable. In order to ascertain the reasonableness of the request for an extension of time, the institution must explain why the consultation will take the amount of time indicated.

There are two legitimate courses of action that an institution might consider when compliance with the time limit set out in the Act places an excessive strain on resources. They are as follows:

- negotiate with the requester who sends in numerous requests as to whether he or she would consent to waive the 30-day limit for each of the requests in favour of a response within 30 days in respect of certain priority requests and a longer response time in respect of others.
- if at all possible, allocate the institution's resources in such a way that, on an emergency basis, additional staff can be assigned to assist those routinely working on freedom of information requests.

The institution's Freedom of Information Coordinator could work on a one-to-one basis with the requester to work out a compromise. Where possible, the coordinator may offer the requester access to the originals, a few at a time, and the requester could then determine which records he or she would like copied.

An institution should consider each request separately and decide on a case-by-case basis, whether a request's volume justifies an extension.

If the head extends the time limit, the head must give the requester a written notice that sets out:

- the length of the extension;
- the reason for the extension; and
- the fact that the requester can ask the IPC to review the decision to extend the time period.

Appendix IV contains a sample of time extension notice. A head may wish to send such a notice once a deposit for the fee estimate is received see Order #M-1071.

Notices to Affected Third Parties

Records sometimes contain information concerning a person other than the requester. In this instance, a person may be another individual or a corporation, partnership or other legal entity considered to be a person. Before granting access to a record affecting a third party, a head must give written notice to the third party to whom the information relates. The information is considered to affect a third party if:

- the head has reason to believe that the record contains third party information referred to in s.17(1) FIPPA / s.10(1) MFIPPA; or
- the record contains personal information that the head has reason to believe might, if released, constitute an unjustified invasion of personal privacy (s.21(1)(f) FIPPA /s.14(1)(f) MFIPPA).

A notice to an affected party gives that party an opportunity to make representations about the proposed disclosure of records that affect him/her.

If the head intends to release the records, then the affected party must be given a notice. The notice must contain:

- a statement that the head intends to disclose a record or part of a record that may affect the interests of the person or organization;
- a description of the contents of the record or the part that relates to the third party; and
- a statement that the person may, within 20 days after the notice is given, make representations to the head as to why the record in whole or in part should not be released.

The notice must be given within the initial 30-day period after a complete request is received or, if there has been an extension of time, within the extended time period.

The third party has 20 days after the notice is given to make representations to the head. Representations are to be in writing unless the head permits them to be made orally. After the representations are made (or after the 20-day period for representations has elapsed), the head must decide within 10 days whether to disclose the record.

If affected third parties have been notified, this will delay the processing of a request. Therefore, the head must notify the requester of the delay. It is advisable to do this at the same time that the affected third party is notified. The notice to the requester must state that the:

- disclosure of the record or part may affect the interests of a third party;
- third party has an opportunity to make representations concerning the disclosure; and
- head will decide within 30 days if the record or part will be released.

If a head decides to release a record in whole or in part that affects a third party and has heard representations from the third party, or the time period for making representations has expired, the head must notify the requester and the affected third party that:

- the person to whom the information relates may appeal the decision to the IPC within 30 days; and
- the requester will be given access to the record or part unless an appeal is filed within the 30 days after the notice is given.

The notice should be very clear that the requester will be given access to the record or part unless the affected third party appeals to the IPC within the 30-day time limit.

Appendix IV contains sample notification letters to third parties and to requesters.

Fee Estimates/Interim Notices

In processing a request, certain costs for time, materials and services will be incurred. Immediately upon receipt of a request, the costs generated in processing a request for access to

general records and, to a limited extent, the costs for processing a request for personal information start to accumulate. If it appears that the costs of processing the request will be over \$25.00, the requester must be given a fee estimate before the head grants access to the records. If the cost estimate is \$100.00 or more, the head may require the requester to pay a deposit equal to 50 per cent of the estimate before taking any further steps to respond to the request.

For example:

An institution receives a request for records that it knows will take more than 3 hours to locate, prepare and copy (this will be roughly equivalent to fees of \$100.00 or more). The institution's first step might be to prepare a cost estimate for processing the request. This cost estimate would likely involve processing a representative sample of the records and estimating probable costs, exemptions applied and expected decisions regarding disclosure. As the request will cost over \$25.00 to process, the institution is required to send a copy of this fee estimate to the requester. In addition, since the expected fee will be over \$100.00, the institution is entitled to ask for a deposit of 50% of expected costs in the letter providing a fee estimate. The institution is not required to complete any further work in responding to the request until it receives the 50% deposit from the requester. If the cost of processing the request was less than \$100.00, the institution would be required to issue a fee estimate and continue processing the request without receiving a deposit.

The head is required to notify the requester of his/her decision regarding access to the requested records within 30 days of receiving the request. Therefore, both the fee estimate notice and a notice of decision on access must be issued within the 30-day period (unless there has been a time extension or a third party notice issued). There are 3 distinct situations with respect to fee estimate notices and final decisions:

- where the access request will cost \$25.00 or less to process, no fee estimate is required.
- where the number of records is not large or unduly expensive to retrieve (i.e. over \$25.00 but under \$100.00 to process), the institution should review the records and provide the requester with both a fee estimate and a decision about disclosure within the 30-day period. The institution is not allowed to stop processing the request once a fee estimate has been sent but may determine the best time to send the fee estimate in the request processing cycle.
- where the processing costs for a request will be over \$100.00, the institution should follow the example provided above where a detailed fee estimate is developed. Work on processing the request stops until the requester provides a 50% deposit.

In the latter case, the head may wish to provide the requester with a notice combining the fee estimate with an interim decision. An interim decision lets the requester know that certain exemptions may apply to the records, although no final determination has been made. Since this is not a final decision, it is not binding on the institution and is not subject to appeal. However, the fee estimate may be appealed.

Both the interim decision and fee estimate are determined using one of the following methods:

- consulting with an employee of the institution who is familiar with the type and contents of the records; or
- basing the interim decision and fee estimate on a representative (as opposed to haphazard) sampling of the records.

In all cases, the fee estimate should be based on an examination of the records and should provide the requester with as much information as possible about the costs that will be incurred in processing the request. The estimate should also indicate that the requester may ask for a fee waiver.

Once the interim notice and fee estimate are sent the 30 day clock stops until the requester indicates willingness to proceed with the request (an institution may request a 50% fee deposit as an indication of the requester's willingness). A time extension notice can then be sent if necessary after a deposit is received.

See Chapter 6 (Fees) for information about chargeable costs, the calculation of fees, deposits and fee waivers.

Granting and Denying Access

s.10, 14(3), 21(5), 24, 26, 28, 29, 30 FIPPA / s.4, 8(3), 14(5)17, 19, 21, 22, 23 MFIPPA

s.3 O.Reg.460 FIPPA / s.2 O.Reg.823 MFIPPA

Once the access decision has been made, written notice of the decision must be provided to the requester and any affected third parties. The notice must be given within the 30-day time period (or within the period of extended time, if any).

However, if third party notices have been given, the notice of a decision concerning disclosure cannot be given until:

- a response from a third party has been received; or
- after the 20-day period in which a third party can respond to a third party notice has elapsed.

If a head does not give the requester notice of his/her decision within the 30 days (or within the time frames extended under the extension of time, or third party notice procedures) the head is deemed to have refused access to the record. The requester may then appeal to the IPC.

Access to Original and Copying

Requesters may ask to view all or part of an original record, rather than being provided with a copy. The head can provide access to original materials if the circumstances make this possible. For instance, it may not be reasonable to provide access to original records if their security would be compromised. An archives, for example, might have records with historical value in original and microfiche form. Access to the microfiche might only be possible because of the age and condition of the original records.

When access is to be granted to an original record, the institution must ensure security of that record. In other words, the institution must then take reasonable steps to ensure that the record is not defaced, changed, destroyed or stolen as a result of granting access. An institution may wish, for example, to have an employee present when access to the record is provided to the requester. In general, the nature of security measures taken should be determined by the nature of the original record requested.

When an institution has several sites such as regional or field offices, the head has the discretion to determine the site where access will be granted to the record.

Factors to consider in exercising this discretion include:

- whether security of the record can be maintained while transporting the record or at a site other than where the record is located;
- whether access at another site would result in undue inconvenience or expense, or would compromise the operation of the institution;
- whether the record is in active use and needed on-site;
- whether there are legal requirements for maintaining the record on-site; and
- the volume, size and fragility of the records.

In exercising this discretion, the head must assess the particular facts of each case before a decision is made.

A requester can ask for copies of all or part of an original record he/she has examined. The requester must be given a copy of what is wanted, unless it would not be reasonable to reproduce the record or part because of its length or nature.

If a photocopy is made of the original severed record, the requester is charged for the cost of photocopying.

Granting Access to Records in Whole

If a record is to be released in its entirety, a requester should be informed of this in a decision letter that outlines any fees that he/she will be required to pay. A copy of the record being provided may be enclosed with the letter if fees are not an issue. If access is to be provided to an original record rather than a copy, the letter should inform the requester of the time and place where the record can be seen.

The institution should confirm the identity of individuals requesting personal information before any personal information is released. Further information about verifying an individual's identity is discussed later in this chapter.

Denying Access to Records or Parts of Records

When access to a record is refused or is only partially granted in the case of a "severed" record, the requester must be notified of the decision and the sections of the Act which justify that decision. The head is required to provide a requester with information about the circumstances which formed the basis for the head's decision to deny access. In the end the requester should be in the position to make an informed decision as to whether or not to seek a review of the head's decision. The requester must also be notified when it is determined that the record sought does not exist,

The notification must contain the following information:

- a statement that the record does not exist; or
- where the record exists, the specific provision of the Act under which access is refused and the reason the provision applies;
- the name and position of the person responsible for the decision; and
- that the requester may appeal the decision to the Commissioner.

The head is required to provide the requester with a clear description of the records responding to the request and a specific reference to the exemption being used. The decision letter should be accompanied by a detailed index of records at issue which describes the contents and subject matter of the records. In the end, the requester should be in the position to make a reasonably informed decision on whether to seek a review of the head's decision by the Commissioner.

An institution must describe the withheld record(s) by providing at least a summary of the categories of the requested records in enough detail to sufficiently allow a requester to make a reasonably informed decision whether or not to appeal. Care should be taken not to disclose any names when describing the withheld record(s).

Appendix IV (Sample Notification Letters) contains a sample notice denying access to records.

Refusing to Confirm or Deny the Existence of a Record

An institution may refuse to confirm or deny the existence of a record if the record relates to law enforcement, or if disclosure of the records would constitute an unjustified invasion of personal privacy.

For example: A social services department that acknowledges that a record about a particular individual exists may invade that individual's personal privacy because the acknowledgment would be a strong indication that the person was, or is, in receipt of social assistance.

The notice of refusal to the requester must state:

- that the head refuses to confirm or deny the existence of the record;
- the provision of the Act (law enforcement or unjustified invasion of personal privacy) on which the refusal is based;
- the name and office of the person responsible for making the decision; and
- that the requester may appeal the decision to the IPC.

A police agency that acknowledges that a record exists about a particular individual may compromise an investigation before a decision is made to lay a charge.

Access to Own Personal Information

s.47, 48 FIPPA / s.36, 37 MFIPPA

FIPPA/MFIPPA provide an individual with a right of access to his/her own personal information, regardless of whether the information is held in a personal information bank or in general records.

A request by an individual must meet the criteria for a "complete request". It must be in writing, must be accompanied by the \$5.00 application fee and must identify the personal information bank where the record is held or the location of the personal information. The institution's *Directory of Records* will assist the requester in locating the specific personal information bank that contains his/her information.

Identification Required for Access

When releasing personal information, an institution must verify and satisfy itself with the requester's identity and ensure that the records are safely transmitted. Verifying an identity can be done in several ways, for example:

- asking for photo identification, e.g. driver's license or a passport;
- spelling of names, address, telephone number, signature, handwriting, etc., should be reviewed and compared with the information that an institution may have on file. Any discrepancies should trigger further inquiry; or
- if the requester wishes to examine the personal information in person, proper identification (such as a drivers licence) should be examined before access to the file is

granted. Since not everyone has a driver's licence, however, the institution should be prepared to accept other appropriate documentation.

If the requester wishes to have a copy of the personal information mailed to him or her, the institution should verify the requester's identity by telephone before forwarding the requested records. This verification could include asking the individual to submit photocopies of his/her identification. Since some individuals may have problems with physical access, requiring personal attendance to view personal information should not be the standard method of verifying identity.

Comprehensible Form

Personal information must be provided to the individual in a comprehensible form and in a manner that indicates the general terms and conditions under which the information is stored and used.

Personal information may be stored in such a manner that it is not readily understood by the individual. For instance, information produced in coded form is meaningless without providing the key to the code. Information provided in response to a request under the Act should be decoded, or the code or key provided, so the information can be understood by the individual.

Correction of Personal Information

Every person who is given access to his/her own information has the right to request correction of the information if he/she believes that it contains errors or omissions.

The right of correction applies only to personal information to which an individual is given access and for which the individual has paid the \$5.00 application fee. The meaning of the word "correction" incorporates three elements:

- the information at issue must be personal information; and
- the information must be inexact, incomplete or ambiguous; and
- the IPC will not order a correction that is a substitution of opinion.

Opinion material obtained from persons other than the individual requesting the correction would not ordinarily be changed. A statement of disagreement is appropriate. The Access/Correction Request form may serve as a statement of disagreement.

An opinion expressed by the individual which has been inaccurately recorded would, in all likelihood, be corrected. However, an opinion which was accurately recorded at the time it was collected but has changed subsequently would not likely be altered.

When the request for correction has been received, the head must determine whether the information submitted for correction can be verified. In some cases, documentary proof should be requested, especially if the information impacts on an individual's financial status or eligibility for a benefit.

If the requested correction of personal information is not made, the individual should be informed of the reasons the correction was not made and that he/she has the right to:

- appeal the decision to the IPC;
- require that a statement of disagreement be attached to the information; or
- have any person or body to whom the personal information was disclosed within the last twelve months notified of the correction or statement of disagreement.

If the correction is made, the requester should be notified with a copy of the corrected record. The requester should also be notified of the right to have any person to whom the personal information was disclosed during the past 12 months notified of the correction.

The Act does not specify the time period within which a response must be provided to a request for correction. The general 30-day period is considered reasonable.

Checklist for Processing a Request

A Request is Received

1. Is the request in writing, does it mention FIPPA/MFIPPA and does it include the \$5.00 application fee?
2. Does it provide sufficient detail to enable an experienced employee to identify the requested record(s)?
 - If not, assist the requester to rewrite the request.
3. Date-stamp the request, open a file and prepare a tracking and recording form.

Do the Requested Records Exist?

1. Do the records exist or are they capable of being reproduced from a machine-readable record?
 - If not, notify the requester that the records do not exist.
2. Does your institution have custody or control of the records?
 - If not, make reasonable inquiries to determine where to forward the request, and forward the request within 15 days of receipt. Notify the requester if the request is forwarded.

- If you do not know where to forward the request, notify the requester that the records do not exist and that the requester can appeal to the IPC.

3. If your institution and another institution have copies of the records, determine which institution has a greater interest in the record and if appropriate, transfer the request to the other institution within 15 days of receiving the request. Notify the requester of the transfer.

Locating and Reviewing the Records

1. Gather the records or a sample of the records and review them.
2. Will some of the exemptions apply?
3. Do you need more time to process the request?
4. Do the records affect the interests of third parties?
5. Will there be a cost for processing the request?
6. Is a time extension required? If so, notify the requester.
7. Does it appear that you will be granting access to records that affect the interests of a third party? If so, send notices and give affected third parties an opportunity to make representations about the disclosure of records that affect them. This will affect the deadline for responding to the request.
8. If the fee will be over \$25.00, the requester must be given a fee estimate. If over \$100.00 a 50% deposit may be requested.

Processing the Request

1. Retrieve the records.
2. Determine what exemptions apply.
3. Determine if the override provisions apply.
4. If required, sever exempt material from the records.
5. Determine what the final fee will be and if the fees will be waived.

Granting or Denying Access to the Records

1. If access to a record or part of a record is granted, determine the method of access (copy or original).

2. If access is granted, give the requester notice regarding access.
3. If an affected third party is involved, give notice regarding access to third party and requester.
 - Note that the affected third party has 30 days in which to appeal your access decision to the IPC. Access is not granted to the record until the 30 days have expired and an appeal has not been filed.
4. Collect fee where applicable, and provide record.

OR

4. Give the requester a *notice of refusal* if:
 - the record does not exist;
 - all or part of the record is exempt from disclosure; or
 - the institution is refusing to confirm or deny the existence of certain records.

Correcting Personal Information

1. If an individual requests the correction of personal information, verify the information to be corrected, correct the personal information or permit a statement of disagreement to be filed.
2. If requested, notify recent users of the personal information of the correction or statement of disagreement.

Complete the File

1. Document the request and all actions taken.
2. Close the file, unless an appeal is commenced.

Chapter 4: Exemptions

Table of Contents

Draft By-Laws, Records of Closed Meetings (s.6 MFIPPA)

- Draft By-laws
- Closed Meetings

Cabinet Records (s.12 FIPPA)

- Substance of Deliberations
 - Agenda and Minutes
 - Policy Options or Recommendations
 - Background Explanations and Analyses
 - Consultations Among Ministers
 - Briefing to Minister
 - Draft Legislation
- Exceptions to Exemptions for Cabinet Records
 - Documents More Than Twenty (20) Years Old
 - Consent of Cabinet

Advice or Recommendations (s.13 FIPPA / s.7 MFIPPA)

- Advice and Recommendations
- Exceptions
 - Factual Material
 - Statistical Survey
 - Valuator's Report
 - Environmental Impact Statement
 - Report on Performance of an Institution
 - Test Report (FIPPA)
 - Feasibility Study
 - Field Research Report
 - Proposal to Change or Establish a Program
 - Interdepartmental Task Force Report (FIPPA)/Committee Report (MFIPPA)
 - Report of a Body Attached to Institution
 - Reasons for a Final Decision of an Officer or Employee
- Record More than 20 Years Old
- Basis for Decision [FIPPA]

Law Enforcement (s.14 FIPPA / s.8 MFIPPA)

- Law Enforcement Matter
- Law Enforcement Investigation
- Reveal Investigative Techniques
- Reveal a Confidential Source
- Safety of a Law Enforcement Officer
- Fair Trial of Impartial Adjudication
- Intelligence Information
- Confiscated Records
- Endanger the Security
- Facilitate Escape
- Centre for Lawful Detention
- Unlawful Act
- Other Law Enforcement Exemptions
 - Law Enforcement Report
 - Act of Parliament
 - Civil Liability
 - Correctional Authority
- Refusal to Confirm or Deny the Existence of a Record
- Exceptions to Exemption for Law Enforcement
 - Routine Inspections
 - Degree of Success in a Law Enforcement Program

Relations with Other Governments (s.15 FIPPA / s.9 MFIPPA)

- Differences Between FIPPA and MFIPPA
- Prejudice to Intergovernmental Relations
- Confidential Information

Defence (s.16 FIPPA)

Third Party Information (s.17 FIPPA / s.10 MFIPPA)

- Threshold Tests
 - Test #1: Categories of Third Party Information
 - Test #2: Supplied in Confidence
 - Test #3: Harms Test
- Competitive Position or Negotiations
- Impede Supply of Similar Information
- Undue Loss or Gain
- Labour Relations Information
- Tax Information (FIPPA)
- Exception to Exemption for Third Party Information (includes Tax Information (FIPPA))

Economic and Other Interests (s.18 FIPPA / s.11 MFIPPA)

- Commercial Information
- Employee Research
- Economic Interests
- Financial Interests
- Negotiating Strategy
- Personnel or Administration Plans
- Policy Decisions / Unfair Advantage
- Examination or Test Questions
- Submissions Under the Municipal Boundary Negotiations Act
- Exception (FIPPA)

Solicitor-Client Privilege (s.19 FIPPA / s.12 MFIPPA)

- Application to Legal Advice
- Application to Litigation Records
- Waiver

Danger to Safety or Health (s.20 FIPPA / s.13 MFIPPA)

Personal Privacy (s.21 FIPPA / s.14 MFIPPA)

- Personal Privacy
- The Exceptions
 - Consent
 - Compelling Circumstances
 - Public Records
 - Disclosure Expressly Authorized By Statute
 - Research Agreements
 - Unjustified Invasion of Personal Privacy
- Factors to be Considered
 - Public Scrutiny
 - Public Health and Safety
 - Informed Choice
 - Fair Determination of Rights
 - Unfair Exposure to Harm
 - Highly Sensitive Information
 - Information Inaccurate or Reliable
 - Information Supplied in Confidence
 - Damage to Reputation
- Presumed Invasion of Privacy
 - Health Record
 - Violation of Law
 - Eligibility for Social Programs
 - Employment or Educational History
 - Tax Return
 - Financial History

- Personal Recommendations and Evaluations
- Race, Ethnic Origin, Religion or Sexual Orientation
- Exceptions to the Exemption
 - Salary Range and Benefits of Employees
 - Personal Services Contracts
 - Licences or Permits
- Refusal to Confirm or Deny
- Public Appointments

Published Information (s.22 FIPPA / s.15 MFIPPA)

Limitations on Access to One's Own Personal Information (s.49 FIPPA / s.38 MFIPPA)

- General Exemptions
 - Unjustified Invasion of Another's Personal Privacy
 - Revealing a Confidential Source
 - Medical Information
 - Correctional Record (FIPPA)
 - Research or Statistical Record
-

Draft By-Laws, Records of Closed Meetings (s.6 MFIPPA)

Section 6 of the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) is a discretionary exemption. There is no comparable section in Freedom of Information and Protection of Privacy Act (FIPPA). It is intended to protect the free discussion of sensitive subjects where legislation allows a municipality or local board to discuss those subjects in camera. This exemption cannot be relied on if the records are over 20 years old. The compelling public interest override in s.16 does not apply to this exemption.

Draft By-laws

s.6(1)(a)

This exemption permits the head to deny access to a draft by-law or private bill, unless the draft has been considered in an open meeting. The term "considered" involves examination or deliberation. Only the draft by-law itself would be exempt as this provision does not exempt from disclosure records that would reveal the contents of drafts.

For example: Disclosing background records used in preparing the draft by-law may allow an accurate inference to be drawn about the nature of the draft by-law but this exemption can not be applied to prevent their release.

Closed Meetings

s.6(1)(b)

This subsection permits the head to prevent disclosure of a record which reveals the substance of deliberations of a closed meeting of a council, board, commission or other body or a committee of one of them. In order to qualify for this exemption, the institution must establish:

- (a) that a meeting was held in the absence of the public, and
- (b) that a statute authorizes the holding of the meeting in the absence of the public, and
- (c) that disclosing the record would reveal the actual substance of deliberations of the meeting.

The term "substance of deliberations" has been interpreted to mean the theme or subject matter that has been considered through discussion. If the subject matter of the deliberations is later considered in an open meeting, this exemption no longer applies to the record. However, a distinction has to be made between the results of the deliberations and the subject matter. A mere disclosure or reporting of a decision made at an in-camera meeting cannot be characterized as a "consideration" of the subject matter of the in-camera deliberations. As well, a discussion of the product or results of deliberations does not necessarily reveal details about subject matter discussed in-camera.

For example: A consolidated budget which was deliberated in an in-camera meeting was formally adopted at a public meeting. Because the line items of that budget were not discussed at the public meeting, their substance would not have been revealed.

Cabinet Records (s.12 FIPPA)

Section 12 of Freedom of Information and Protection of Privacy Act (FIPPA) is a mandatory exemption. There is no comparable section in Municipal Freedom of Information and Protection of Privacy Act (MFIPPA). Its purpose is to prohibit disclosure of records where disclosure "would reveal the substance of deliberations of an Executive Council or its committees". The right to claim this exemption is not restricted when the record has been disclosed without the knowledge of the institution.

"Executive Council" means Cabinet.

The exemption applies to:

- Cabinet and committees of Cabinet including: Policy and Priorities Board, Management Board, Legislation and Regulations, and Cabinet committees established for various policy areas or that are constituted from time to time.
- Records not sent to Cabinet or its committees, if disclosure of the record would permit an accurate inference concerning the substance of deliberations of Cabinet or its committees.

The exemption does not apply to:

- Records sent to Cabinet in a manner that is outside the normal Cabinet submission process. For example, the exemption does not apply where a non-governmental third party sends a proposal directly to Cabinet.

It is not necessary to show that any injury would result from disclosure in order to claim the exemption.

The compelling public interest override in s.23 does not apply to this exemption.

Substance of Deliberations

s.12(1) A head shall refuse to disclose a record where the disclosure would reveal the substance of deliberation of Cabinet or its committees, including certain records referred to in clauses (a) through (f). The use of the word "including" indicates an expanded definition of the types of records which are deemed to qualify as subject to the exemption, regardless of whether their disclosure would reveal the substance of deliberations of Cabinet. At the same time, the types of records listed in clauses (a) through (f) are not the only ones eligible for the exemption. Any record whose disclosure would reveal the substance of deliberations of Cabinet or its committees qualifies for the exemption in s.12(1). Only in rare circumstances would a record which has never been placed before Cabinet reveal the "substance of deliberations" of Cabinet.

Agendas and Minutes

s.12(1)(a)

An agenda, minute or other record of the deliberations or decisions of the Cabinet or its committees is exempt. "Other records" have to be of the same nature as an agenda or minute.

Policy Options and Recommendations

s.12(1)(b)

A record containing policy options or recommendations submitted or prepared for submission, to Cabinet or its committees is exempt. This includes a Cabinet submission (or policy submission) that proposes alternative courses of action to resolve a problem, provides discussion of the merits of the alternatives and makes recommendations.

There must be evidence that the record either was sent to Cabinet for consideration or was prepared with the specific intention of presenting it to Cabinet.

Background Explanations and Analyses

s.12(1)(c)

This subsection provides an exemption for records that do not contain policy options or recommendations referred to in s.12(1)(b), but that do contain background explanations or analyses of problems submitted or prepared for submission to Cabinet or its committees for consideration in making decisions before those decisions are implemented. For this exemption to apply, it is not enough for the issues to have been considered, but rather the record itself must have been submitted or prepared for submission to Cabinet for its consideration.

A Cabinet submission is sometimes accompanied by a record which provides a background explanation or analysis of the problem which the Cabinet submission is intended to address. Such accompanying material is only exempt from disclosure under this subsection until Cabinet has decided the course of action it will take in relation to the issue and the decision has been implemented. A decision has been implemented when steps have been taken to give effect to the decision.

For example: Cabinet may decide to introduce legislation, but the decision is not implemented until the legislation is tabled in the Legislative Assembly.

Even though not exempt under this subsection, background explanations and analyses may be exempt if these records would reveal the "substance of deliberations" of Cabinet.

Consultation Among Ministers

s.12(1)(d)

This subsection provides an exemption for records used for or reflecting consultation among Cabinet Ministers on matters relating to making government decisions or formulating government policy. Such records would usually be memoranda to and from ministers and minutes of meetings of ministers. Records not exempt would include those used for consultations among public servants.

Briefing to Minister

s.12(1)(e)

This subsection provides an exemption for a record to brief a Cabinet Minister on matters that currently are, or are proposed to be, brought before Cabinet or its committees, or that are the subject of consultation among ministers relating to government decisions or formulating government policy. Such records are ordinarily prepared by the institution's staff or the minister's political advisors and would typically contain information that would inform the minister of the essential facts and circumstances respecting a matter. An index or list of topics or briefings considered by a minister would not contain sufficient information to fall within the subsection.

Briefing notes should include information on why the note was prepared. This is particularly important if the issue is before Cabinet or its committees (e.g. Management Board of Cabinet) and a claim is made that the record should be exempt under s.12.

Draft Legislation

s.12(1)(f)

Draft legislation (including regulations) is exempt from disclosure. However, this subsection only applies where disclosure of the record would reveal the substance of deliberations of Cabinet. The exemption does not, therefore, inhibit the practice followed by many ministries of distributing legislation for comment to interested parties when the draft legislation is under development by a ministry but has not yet been submitted to Cabinet. Where the draft has been considered by Cabinet, Cabinet may consent to distribution of the draft for comment.

Exceptions to Exemption for Cabinet Records

Documents More Than Twenty (20) Years Old

s.12(2)(a)

A head shall not refuse to disclose a record under s.12(1) where the record is more than 20 years old. This subsection does not place an obligation on an institution to retain a record for 20 years. Record retention schedules will be followed in determining the appropriate disposition of Cabinet records.

Consent of Cabinet

s.12(2)(b)

The Cabinet for which, or in respect of which, the record has been prepared can consent to access being given to a Cabinet record before the 20-year period has expired. Consent will normally be reflected in a Cabinet minute.

This exception to the exemption only applies to the Cabinet for which the record was prepared. One Cabinet cannot consent to the release of another's records. A Cabinet is considered to have changed where there has been, for example, an election or a change of government.

Subsection 12(2)(b) does not impose a mandatory requirement but rather provides the head with discretion to seek Cabinet consent where he/she feels a record could be released and where a reasonable expectation may exist that Cabinet will not withhold its consent.

The following are factors that the head might consider in deciding whether to seek the consent of Cabinet to the disclosure of a record:

- the subject matter;
- whether or not the government policy contained in the record has been announced or implemented;
- whether the record would reveal the nature of Cabinet discussion on the position of the institution;
- whether the record has, in fact been considered by Cabinet.

The head has a duty in every case to consider whether to seek Cabinet consent. On an appeal, the institution must be able to present evidence that the head has considered the seeking of consent. Generally, however, where a body such as the Cabinet of a previous government no longer exists it will not be practical to seek its consent to disclosure.

Advice or Recommendations (s.13 FIPPA / s.7 MFIPPA)

Subsection 13(1) Freedom of Information and Protection of Privacy Act (FIPPA)/s.7(1) Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) provides a discretionary exemption for records where disclosure would reveal the advice or recommendations of officers or employees of institutions or of consultants retained by an institution. Officers or employees include those persons who work for an institution or who perform duties under a contract of employment. The advice of an officer or employee of another institution cannot be exempted under this section, nor can advice of a volunteer.

The compelling public interest provision in s.23 FIPPA / s.16 MFIPPA applies to this exemption, except for the records over 20 year old that would qualify for the subsection 3 exception.

Advice and Recommendations

s.13(1) FIPPA / s.7(1) MFIPPA

Please note: the wording of FIPPA/ MFIPPA differs somewhat for this section

The exemption is for advice or recommendations. There is some overlap between the terms advice and recommendations. Recommendations refers to formal recommendations about courses of action to be followed which are usually specific in nature and are proposed mainly in connection with a particular decision. Advice refers to less formal suggestions about particular approaches to take or courses of action to follow. The advice or recommendations must be communicated between individuals employed by or in the service of the institution, and must be made in the course of the deliberative process of decision-making and policy-making. If an accurate inference concerning the advice given may be drawn from a record, it would be exempt. An employee's memo to file on the other hand, has not been communicated and would therefore not be included in this exemption.

For example: A draft letter containing advice which is communicated to another person may be advisory, but where there is no communication of the draft letter (such as with a letter never sent but simply filed), it does not fall under the exemption.

Advice must contain more than mere information. Advice and recommendations, however, do not cover the whole range of activities carried out by employees of institutions in the course of policy development, administration of programs, operation of facilities and adjudication. Advice pertains to the submission of a suggested course of action which will be accepted or rejected during the deliberative process.

For example: Draft reports or briefing materials not intended for Cabinet or not qualifying for the closed meeting exemption available to local institutions, would normally fall within this exemption.

This exemption is not time limited. A record may continue to be exempt under this exemption, even though an institution may have completed its decision-making on a matter. However, the fact that a decision on the subject-matter of the advice has been made is one of the factors that the head should consider in exercising his/her discretion to disclose the record.

The Exceptions

Section 13(2) FIPPA / s.7(2) MFIPPA requires that the head shall not refuse, under s.13(1) FIPPA / s.7(1) MFIPPA, to disclose specified types of records and information despite the exemption contained in s.13(1) FIPPA / s.7(1) MFIPPA. These "exceptions" are intended to insure that factual or statistical information is publicly available. Where factual or statistical information and advice and recommendations are contained in the same record, the advice and recommendations may be severed and withheld. However, severing may not be possible and the

document withheld in whole, where the factual information is so intertwined with the advice and recommendations that it is not possible to disclose factual information without disclosing exempt information.

In addition, subsection 13(2) FIPPA / s.7(2) MFIPPA requires that certain reports, studies, plans and reasons for final decisions be released, even though they may contain advice or recommendations.

It should be noted that subsection 13(2) FIPPA / s.7(2) MFIPPA is an exception only to s.13(1) FIPPA / s.7(1) MFIPPA. Therefore, a record such as an environmental impact statement which contains advice or recommendations cannot be exempt under subsection s.13(1) FIPPA / s.7(1) MFIPPA. It may, however, be covered by other exemptions.

A "report" or "study" within subsection 13(2) FIPPA / s.7(2) MFIPPA means a completed document ready for presentation and would not include working papers used in preparation such as notes and preliminary drafts.

Factual Material

s.13(2)(a) FIPPA / s.7(2)(a) MFIPPA

Records or parts of records containing factual material must be disclosed.

"Factual material" means a coherent body of facts which can be separated from the rest of the advice or recommendations, for example, an appendix of factual information supporting a policy document. Where factual material and advice or recommendations are contained in the same record, the advice or recommendations may be severed and withheld. However, it may not be possible to sever advice and recommendations and still leave meaningful factual information. In this circumstance, severing may not be appropriate, and the information should not be disclosed.

Statistical Survey

s.13(2)(b) FIPPA / s.7(2)(b) MFIPPA

A statistical survey must be disclosed unless another exemption applies.

A statistical survey is a record showing the collection, analysis, interpretation and presentation of aggregate data in relation to a topic or issue which is the object of study, for example, a poll. Any information identifying individuals must be removed before the record is disclosed.

Valuator's Report

s.13(2)(c) FIPPA / s.7(2)(c) MFIPPA

A valuator is someone with specific expertise appointed to determine or estimate the value, price or merit of an article. He or she need not be an officer of the institution. A valuator's report would include an appraisal of the value of real property.

Environmental Impact Statement

s.13(2)(d) FIPPA / s.7(2)(d) MFIPPA

An environmental impact statement or similar record must be disclosed.

An environmental impact statement is a record containing a technical assessment, including findings and conclusions respecting the social, cultural, economic and environmental consequences of projects such as buildings and highways.

Test Report

s.13(2)(e) FIPPA

An institution cannot under subsection 13(1) refuse to disclose a report of a test carried out on a product for the purpose of government equipment testing or a consumer test report.

In this subsection, "government" includes ministries and all the agencies and other bodies designated as institutions. Product and environmental testing is discussed under subsection 18(2) FIPPA.

Report on Performance

s.13(2)(f) FIPPA / s.7(2)(e) MFIPPA

A report or study on the performance or efficiency of an institution is not exempt under s.13(1) FIPPA / s.7(1) MFIPPA. The report or study may be of a general nature or about a particular program or policy.

For example: a final audit report, including its findings and conclusions would not be exempt.

Feasibility Study

s.13(2)(g) FIPPA / s.7(2)(f) MFIPPA

A feasibility or other technical study, including a cost estimate, relating to an institution's policy or project must be disclosed unless another exemption applies.

A feasibility or other technical study is prepared by experts in the relevant discipline to determine whether a proposed policy or project can be accomplished within certain given assumptions and constraints. If the study is classified as a feasibility study, the record will be fully disclosed, including cost estimate information.

For example: a feasibility study for a micrographics program would not be exempt from disclosure under this subsection.

Field Research Report

s.13(2)(h) FIPPA / s.7(2)(g) MFIPPA

The exemption in s13(1) FIPPA/ s.7(1) MFIPPA does not apply to a report setting out the findings and conclusions of field research on an issue or problem which is undertaken before the formulation of a policy proposal.

Proposal to Change or Establish a Program

s.13(2)(i) FIPPA / s.7(2)(h) MFIPPA

This subsection requires disclosure of a final plan or proposal to change or establish a program, including a budgetary estimate, or, in the case of FIPPA, whether or not the plan or proposal is subject to approval.

This section must be considered in relation to the exemption in s.18(1)(f) FIPPA / s.11(f) MFIPPA, and refers to a final plan or proposal to alter or establish a program which provides a service to the public and which is developed or implemented to carry out the institution's responsibilities. Subsection 18(1)(f) FIPPA / s.11(f) MFIPPA covers internal administrative arrangements relating to personnel which do not fundamentally alter the nature and content of the programs being delivered to the public.

If the plan or proposal is one that is to be presented to Cabinet or its committees, this section does not apply and s.12 FIPPA must be considered.

Interdepartmental Task Force Report (FIPPA)/Committee Report (MFIPPA)

s.13(2)(j) FIPPA / s.7(2)(i) MFIPPA

A report of a committee within an institution must be disclosed unless another exemption applies to the record.

Unless another exemption applies, this subsection requires disclosure of a report of an interdepartmental task force or similar body, or of a committee within an institution that has been established for the purpose of preparing a report. The word "interdepartmental" in this subsection means "inter institutional" in the sense of involving representatives of more than one institution designated under the Act.

For example: A report of a task force that included members from the Ministry of the Environment and Ontario Hydro is subject to this subsection.

Report of a Body Attached to Institution

s.13(2)(k) FIPPA / s.7(2)(j) MFIPPA

The type of body referred to in this subsection is one that consists primarily of representatives from outside the institution, and that undertakes inquiries and make reports or recommendations to the institution. The phrase "attached to an institution" indicates that the body has been appointed or invited to meet and deliberate by someone in an institution with appropriate authority. A local grants committee established to make recommendations regarding the awarding of grants is an example of one such body.

Reasons For a Final Decision

s.13(2)(l) FIPPA / s.7(2)(k) MFIPPA

Unless another exemption applies, this exception requires disclosure of the reasons for a final decision, order or ruling of an officer of the institution made during or at the conclusion of the exercise of a discretionary power under an enactment or scheme administered by the institution.

This exception covers a wide range of decisions made within an institution. It applies regardless of appeal rights and whether the reasons are recorded in internal memoranda, external correspondence, or given by the deciding officer or subsequently incorporated in a decision, order or ruling. Names and other features identifying individuals mentioned in the record may be subject to the personal information exemption.

Record More Than 20 Years Old

s.13(3) FIPPA / s.7(3) MFIPPA

Unless another exemption applies, an institution must release a record that is more than 20 years old. This subsection does not place an obligation on an institution to retain a record for 20 years. Retention schedules will be followed in determining the disposition of records.

Basis for Decision or Policy(FIPPA)

s.13(3) FIPPA Under FIPPA a head shall not refuse to disclose a record under subsection 13(1) where he/she has publicly cited the record as the basis for making a decision or formulating a policy.

For example: This subsection applies where portions of a record have been disclosed to the media to explain a decision.

Law Enforcement (s.14 FIPPA / s.8 MFIPPA)

This section provides a discretionary exemption for records relating to police and by-law enforcement investigations and certain other investigative, adjudicative and protective functions.

- Subsection (1) provides an exemption where disclosure could reasonably be expected to interfere with law enforcement and certain other activities.
- Subsection (2) exempts certain types of law enforcement records.
- Subsection (3) provides that a head may refuse to confirm or deny the existence of records in subsections (1) and (2).
- Subsections (4) and (5) set out exceptions to the exemption.

Law enforcement is defined in s.2(1) of the Act. The phrase not only includes policing activities and prosecutions, but also investigations, or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed. This definition encompasses the enforcement of federal and provincial statutes and municipal by-laws. Law enforcement investigations do not include internal employment-related investigations for other than violations of the law.

For example: The enforcement of property standards by-laws by a municipality or the enforcement of a no-smoking by-law by a transit authority would constitute a law enforcement activity.

The term "could reasonably be expected to" as used in this section requires that the expectation of the harm coming to pass should the record be disclosed, not be fanciful, imaginary or contrived, but based on reason. An institution must establish a clear linkage between the disclosure of the information and the harm alleged.

The compelling public interest override in s.23 Freedom of Information and Protection of Privacy Act (FIPPA) / s.16 Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) does not apply to this exemption.

Law Enforcement Matter

s.14(1)(a) FIPPA / s.8(1)(a) MFIPPA

This exemption applies if disclosure could reasonably be expected to interfere with a law enforcement matter. To interfere with a law enforcement matter means that the disclosure would have the effect of hindering or impeding the conduct of a proceeding or the carrying out of a law enforcement activity.

Law enforcement matter refers to a proceeding or an activity that is within the scope of law enforcement as defined in s.2(1) of the Act.

Law Enforcement Investigation

s.14(1)(b) FIPPA / s.8(1)(b) MFIPPA

An institution may refuse to disclose a record where the disclosure could reasonably be expected to interfere with an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result. An "investigation" is the methodical determination of facts and gathering of evidence. In some cases, the evidence gathered in an investigation will be insufficient to support the commencement of a proceeding in a court or tribunal. A record of the investigation could still be exempt, however, since it is undertaken with a view to a law enforcement proceeding.

To "interfere" with an investigation does not mean that disclosure would altogether prevent a law enforcement investigation from taking place, but rather that disclosure would frustrate or impede the carrying out of an investigation.

For example: Disclosure to an individual that he/she is the subject of a current law enforcement investigation would probably not prevent the investigation from continuing, but in many cases would hamper or impede it. In these circumstances, records relating to the investigation would be exempt.

"In Ontario (Minister of Labour), the Court of Appeal for Ontario drew a distinction between the requirements for establishing "health or safety" harms under sections 14(1)(e) and 20, and harms under other exemptions. The court stated (at p. 6): The expectation of harm must be reasonable, but it need not be probable. Section 14(1)(e) requires a determination of whether there is a reasonable basis for concluding that disclosure could be expected to endanger the life or physical

safety of a person. In other words, the party resisting disclosure must demonstrate that the reasons for resisting disclosure is not a frivolous or exaggerated expectation of endangerment to safety. Similarly [section] 20 calls for a demonstration that disclosure could reasonably be expected to seriously threaten the safety or health of an individual, as opposed to there being a groundless or exaggerated expectation of a threat to safety. Introducing the element of probability in this assessment is not appropriate considering the interests that are at stake, particularly the very significant interest of bodily integrity. It is difficult, if not impossible, to establish as a matter of probabilities that a person's life or safety will be endangered by the release of a potentially inflammatory record. Where there is a reasonable basis for believing that a person's safety will be endangered by disclosing a record, the holder of that record properly invokes [sections] 14(1)(e) or 20 to refuse disclosure.

Reveal Investigative Techniques

s.14(1)(c) FIPPA / s.8(1)(c) MFIPPA

This subsection applies where disclosure could reasonably be expected to reveal investigative techniques and procedures in use or likely to be used in law enforcement. The IPC has found that successful application of this exemption requires the institution to demonstrate that disclosure of the technique or procedure to the public would hinder or compromise its effective utilization. If the technique or procedure is generally known, or such that a lay person would expect, reliance on this exemption would not be successful.

For example: This exemption applied to records containing strategies, procedures and specific drug industry investigation targets, as well as other courses of action currently in use or likely to be used in law enforcement.

Reveal a Confidential Source

s.14(1)(d) FIPPA / s.8(1)(d) MFIPPA

Disclosure may be refused where it would reveal the identity of a confidential source of information in respect of a law enforcement matter, or disclose information furnished only by the confidential source.

For example: A person who complains against his/her neighbour in respect of a municipal by-law infraction is a source protected under the exemption. A police informant is a source protected under the exemption. A family member who provides information in confidence about a violation of law by another family member would also be protected.

Safety of a Law Enforcement Officer

s.14(1)(e) FIPPA / s.8(1)(e) MFIPPA

Disclosure may be refused where it would endanger the safety of a law enforcement officer or any other person. Section 20 FIPPA / s.13 MFIPPA also apply where disclosure of a record could reasonably be expected to seriously threaten an individual's health or safety.

Fair Trial or Impartial Adjudication

s.14(1)(f) FIPPA / s.8(1)(f) MFIPPA

This exemption prevents premature disclosure of information that could deprive a person of a fair trial or impartial adjudication. Once the proceeding has been completely disposed of (including appeals), the exemption no longer applies. In order to demonstrate unfairness under this subsection, the institution must produce more evidence than the mere commencement of a legal action. The institution must present specific arguments as to how or why disclosure of specific parts of the record could reasonably be expected to deprive a person of a fair trial.

This subsection does not contain a reference to law enforcement and, accordingly, the exemption applies to proceedings that do not fall within the definition of law enforcement such as tribunals established by law to adjudicate individual or collective rights. An example of such a tribunal would be the Social Assistance Review Board. To rely on this exemption, however, there must be evidence that the disclosure of the records would result in unfairness.

Intelligence Information

s.14(1)(g) FIPPA / s.8(1)(g) MFIPPA

This subsection exempts from disclosure records where the disclosure could reasonably be expected to interfere with the gathering of or reveal law enforcement intelligence information respecting organizations or persons.

"Intelligence information" is gathered because it may be useful for future investigations. It may also be used for activities aimed at preventing the commission of an offence and for the purpose of ensuring the security of individuals or organizations including institutions covered by the Act. Intelligence information may be derived from previous investigations which may or may not have resulted in the commencement of proceedings against a person or organization. It may also be gathered through observing the conduct of associates of known criminals and through other activities.

Confiscated Records

s.14(1)(h) FIPPA / s.8(1)(h) MFIPPA

This exemption applies where disclosure could reasonably be expected to reveal records confiscated by a peace officer in accordance with an act or regulation.

Endanger the Security

s.14(1)(i) FIPPA / s.8(1)(i) MFIPPA

Disclosure may be refused where it could reasonably be expected to endanger the security of a building or the security of a vehicle carrying items (e.g., things or articles), or of a system or procedure established for the protection of items, for which protection is reasonably required. The exemption is qualified by the requirements that the protection be reasonably required.

For example: A security audit was found to be a record which if disclosed would endanger the security of a system or procedure established for the protection of items.

Facilitate Escape

s.14(1)(j) FIPPA / s.8(1)(j) MFIPPA

Records are exempt where the disclosure could reasonably be expected to facilitate escape from custody of a person who is under lawful detention. Custody indicates that an individual is not free to leave a place of confinement without restriction. In general, any person held in custody pursuant to a valid warrant or other authorized order is under lawful detention.

The term "facilitate" means make easier or less difficult. The exemption applies to construction plans and specifications regarding a maximum security facility. It is not necessary that the plans be extremely detailed.

The fact that the plans for the secured facility were available to the public in the past does not mean that this section requires that they continue to be available. It is appropriate to limit access to records for security reasons.

Centre for Lawful Detention

s.14(1)(k) FIPPA / s.8(1)(k) MFIPPA

This provision exempts records where disclosure could reasonably be expected to jeopardize the security of a centre for lawful detention. This includes records containing details of previous investigations of escape attempts and details of security measures in place.

Unlawful Act

s.14(1)(l) FIPPA / s.8(1)(l) MFIPPA

Records are exempt where the disclosure could reasonably be expected to facilitate the planning or committing of an unlawful act or hamper the control of a crime. "Unlawful act" means a contravention of a statute or regulation or of a municipal by-law.

Other Law Enforcement Exemptions s.14(2) FIPPA / s.8(2) MFIPPA

Subsection (2) specifies certain records that the institution may refuse to disclose in response to a request. These records are described immediately below. This subsection deals with the confidentiality that necessarily surrounds law enforcement investigations in order that institutions charged with external regulatory activities can carry out their duties.

Law Enforcement Report

s.14(2)(a) and 14(4) FIPPA / s.8(2)(a) and 8(4) MFIPPA

This subsection exempts from disclosure a report prepared in the course of law enforcement inspections or investigations by an agency responsible for enforcing and regulating compliance with a law. A "report" must consist of a formal statement or account of the results of the collation and consideration of information. Generally speaking, reports would not include mere observations or recordings of fact. "Agency" includes organizations acting on behalf of or as agents for law enforcement agencies.

The exemption in s.14(2)(a) FIPPA / s.8(2)(a) MFIPPA is modified by subsection 4.

Subsection 14(4) FIPPA / s.8(4) MFIPPA does not allow the head to exempt from disclosure a report containing the results of a routine inspection by an agency with statutory authority to enforce and regulate compliance with standards (e.g., the enforcement or compliance branch of an institution). "Routine inspections" are inspections that are carried out where there are no specific allegations that standards have been breached.

Material relating to routine inspections in areas such as health and safety legislation, fair trade practices laws, environmental protection schemes and many other regulatory schemes administered by government are to be open to public scrutiny.

For example: The *Fire Marshals Act* authorizes the Fire Chief to enforce compliance with fire safety standards through routine inspections. These standards are set out in the *Fire Marshals Act* and the *Ontario Fire Code*. These inspections need not take place as a result of a complaint. The records of these routine inspections would not be exempt under s.14(2)(a) FIPPA /s.8(2)(a) MFIPPA.

Act of Parliament

s.14(2)(b) FIPPA / s.8(2)(b) MFIPPA

This subsection exempts a law enforcement record where disclosure would be an offence under an Act of Parliament.

For example: Section 46 of the *Young Offenders Act* makes it an offence to knowingly disclose certain court, police and government records relating to young offenders, except as authorized by that Act.

Civil Liability

s.14(2)(c) FIPPA / s.8(2)(c) MFIPPA

This subsection exempts a law enforcement record where disclosure could reasonably be expected to expose the author of the record, or any person who had been quoted or paraphrased in the record, to civil liability.

The purpose of this exemption is to provide protection for law enforcement officials and witnesses/informants who might be sued for defamation as a result of disclosure of records made while carrying out their duties.

Correctional Authority

s.14(2)(d) FIPPA / s.8(2)(d) MFIPPA

This subsection exempts records that contain information relating to an individual's correctional history while the individual is under the control or supervision of a correctional authority.

This exemption applies to individuals on parole, probation, a temporary absence permit, under bail supervision or performing community service work.

Refusal to Confirm or Deny the Existence of a Record

Subsection (3) provides that a head may refuse to confirm or deny the existence of a record to which subsections (1) or (2) apply. Situations may arise in which merely disclosing the existence of an investigation or intelligence file will communicate information to the requester which may impede ongoing investigation or intelligence-gathering.

Exceptions to Exemption for Law Enforcement

Routine Inspections

s.14(4) FIPPA / s.8(4) MFIPPA

This subsection requires an institution to disclose a record that is a report prepared in the course of routine inspections by an agency that is authorized to enforce and regulate compliance with a particular statute of Ontario.

For further discussion on routine inspections, see the section above pertaining to law enforcement reports.(s.14(2)(a) FIPPA/ s.8(2)(a) MFIPPA).

Degree of Success in a Law Enforcement Program

s.14(5) FIPPA / s.8(5) MFIPPA

This subsection provides that the exemptions in subsections (1) and (2) do not apply to a record regarding the degree of success achieved in a law enforcement program, unless the disclosure of such a record would prejudice, interfere with, or adversely affect any of the matters referred to in (1) or (2).

Relations with Other Governments (s.15 FIPPA / s.9 MFIPPA)

This section provides a discretionary exemption where disclosure of a record could reasonably be expected to prejudice the conduct of intergovernmental relations or reveal information received in confidence from another government.

"Other governments" include the:

- Government of Canada;
- Government of Ontario (for MFIPPA institutions);
- Another provincial or territorial government;
- A government of a foreign country or state; or
- An international organization of states (e.g. United Nations).

This section also applies to records received in confidence from agencies or boards of these governments. For example, the Royal Canadian Mounted Police is an agency of the federal government. Municipal and regional police services are law enforcement agencies of the Government of Ontario, because the *Police Services Act* (PSA) is the governing legislation with respect to police services in Ontario and the PSA is administered by the Solicitor General of Ontario. Further, this subsection requires the relations in question to be intergovernmental rather than relations among agencies of the same government.

For this exemption to apply, a three-part test must be met: 1) the records must reveal information received from another government or its agencies; 2) the information must have been received by an institution; and 3) the information must have been received in confidence.

This exemption requires that there be a reasonable expectation of harm and the institution is expected to establish a clear and direct linkage between the disclosure of the information and the harm alleged. The expectation that disclosure of a record could prejudice the conduct of intergovernmental relations or reveal information received in confidence by the institution from another government or its agencies, must not be fanciful, imaginary or contrived, but rather one that is based on reason.

The compelling public interest provision in s.23 FIPPA / s.16 MFIPPA applies to this exemption. However, FIPPA institutions must obtain the approval of the Executive Council (Cabinet) before disclosing any information to which this exemption applies.

Differences Between FIPPA and MFIPPA

There are some differences in the wording and provisions of this exemption between the Freedom of Information and Protection of Privacy Act (FIPPA) and the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

For example: Section 9 (2) MFIPPA explicitly states that local institutions shall disclose a record to which the exemption applies if the government, agency or organization from which the record was received consents to the disclosure. There is no similar expressed provision in s. 15 FIPPA.

This exemption does not apply to records received in confidence by one municipality/local board from another municipality/local board. The Act provides that an access request can be transferred to the originating municipality or local board if that institution has a greater interest in the records Chapter 3 (Access Procedures) for a discussion on this transfer provision.

Prejudice to Intergovernmental Relations

s.15 (a) FIPPA

This exemption applies if there is a reasonable expectation of prejudice to the conduct of intergovernmental relations. "Intergovernmental" extends to the relationship that the Government of Ontario or an institution has with other governments. The term "relations" includes not only current negotiations, but general and ongoing exchanges with other governments.

Confidential Information

s.15 (b) and (c) FIPPA / s.9(1) MFIPPA

The purpose of this exemption is to ensure that governments under MFIPPA/FIPPA will continue to obtain access to records which other governments could otherwise be unwilling to supply without having this protection from disclosure. In order for this provision to apply, the case for confidentiality must be made by the supplying government, not the receiving government.

Defence (s.16 FIPPA)

This section provides a discretionary exemption for a record where disclosure could reasonably be expected to prejudice (or injure) the defence of Canada or any foreign state allied or associated with Canada.

The "defence of Canada or any foreign state allied or associated with Canada" includes the prevention of attack and other acts of aggression.

An "allied state" is one with which Canada has concluded formal alliances or treaties. An "associated state" is a state with which Canada may be linked for trade or other purposes outside the scope of a formal alliance.

The section also exempts records whose disclosure could reasonably be expected to be injurious to the detection, prevention or suppression of espionage, sabotage or terrorism.

If the head proposes to disclose the information despite the exemption, prior approval of Cabinet is required. The compelling public interest override in s.23 Freedom of Information and Protection of Privacy Act (FIPPA) does not apply to this exemption.

Third Party Information (s.17 FIPPA / s.10 MFIPPA)

Institutions subject to the Freedom of Information and Protection of Privacy Act (FIPPA)/Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) often acquire information about the activities of private sector organizations. Some of this information may constitute a valuable asset to the organization, and disclosure would impair its ability to compete effectively. S.17(1) FIPPA / s.10(1) MFIPPA provides a mandatory exemption from disclosure for certain third party information where disclosure could reasonably be expected to cause certain harms. This exemption is not limited to commercial third parties, but may also apply to any supplier of information which meets the tests specified below, including another institution.

Section 28 FIPPA /s.21 MFIPPA provides that before access is granted to a record that might contain information referred to in s.17(1) FIPPA / s.10(1) MFIPPA affecting the interests of a third party, that party must be notified and given the opportunity to make representations before a final access decision is made. If a third party claims in its representations that the record is exempt, the burden of establishing that the record falls within this section rests with that third party. Similarly, where an institution asserts that this provision applies, the burden of proof is on the institution. Notification procedures are discussed in Chapter 3 (Access Procedures).

The compelling public interest provision in s.23 FIPPA / s.16 MFIPPA applies to this exemption.

Threshold Tests

Before this exemption can be applied, all of the following three tests must be met:

- the information must fit within one of the specified categories of third party information;
- the information must have been "supplied" by the third party "in confidence", implicitly or explicitly; and
- the disclosure of the information could reasonably be expected to cause certain harms specified in this section.

The three tests are discussed in more detail immediately below.

Test #1: Categories of Third Party Information

In order for this exemption apply, the record in question must contain one or more of the following types of information:

Trade secret: Means information including, but not limited to, a formula, pattern, compilation, program, method, technique, or process or information contained or embodied in a product, device or mechanism which (i) is, or may be used in a trade or business, (ii) is not generally known in that trade or business, (iii) has economic value from not being generally known, and (iv) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Scientific information: Means information belonging to an organized field of knowledge in either the natural, biological or social sciences or mathematics. It must also relate to observing and testing specific hypotheses or conclusions and be undertaken by an expert in the field. Finally, scientific information must be given a meaning separate from "technical" information in this provision.

Technical information: Means information belonging to an organized field of knowledge that would fall under the general categories of applied sciences or mechanical arts. Examples of these fields would include architecture, engineering or electronics. It will usually involve information prepared by a professional in the field and describe the construction, operation or maintenance of a structure, process, equipment or thing. "Technical" information is distinct from "scientific" information.

Commercial information: Means information that relates solely to the buying, selling or exchange of merchandise or services. The term "commercial" information can apply to both profit-making and non-profit organizations, and has equal application to both large and small enterprises. Commercial information is distinct from "financial" information

Financial information: Refers to specific data and is information that relates to finance or money matters. For example, the IPC has found that the price paid for land, tax information, conversion rates, default consequences and interest incentives regarding loans qualifies as financial information.

Labour relations: Means information concerning the collective relationship between an employer and its employees. This includes information compiled in the course of negotiating pay equity plans which, when implemented, would effect the collective relationship between the employer and its employees.

Test #2: Supplied in Confidence

The second test for this exemption is that the information must have been supplied in confidence to the institution by a third party. The IPC's findings on this test include the following:

- Information that is created or gathered by the institution is not "supplied" by a third party. For example, information deriving from an institutions' negotiations with a third party is not "supplied" by the third party. However, the exemption is applicable to records developed by the institution where disclosure of those records would permit the drawing of accurate inference with respect to supplied by the third party and meeting other parts of the test.
- The intention to maintain confidentiality may be expressed or may be implied from the circumstances (or conduct of the parties). For example, confidentiality may be implied where there is evidence that the information was consistently treated in confidence.
- The expectation of confidence must be reasonable and have an objective basis. The following factors may be considered: 1. was it communicated that the information was to be kept confidential; 2. was it treated consistently in a manner that shows concern for its protection prior to being communicated to the institution; 3. is it otherwise available to the public; and 4. was the record prepared for a purpose that would not entail disclosure.

Test #3: Harms Test

For this exemption to apply, it must be demonstrated that disclosure of the record could reasonably be expected to yield one of the three results discussed below.

Competitive Position or Negotiations

s.17(1)(a) FIPPA / s.10(1)(a) MFIPPA

The subsection applies where the disclosure could reasonably be expected to prejudice significantly the competitive position or interfere significantly with the contractual or other negotiations of a person, group of persons or organization.

This involves significant injury to competitive position, or significant interference with contractual or other negotiations. It requires some measure of the injury. The particular circumstances must be evaluated in each case. The institution or third party must present evidence that is detailed and convincing and must describe a set of facts and circumstances that would lead to a reasonable expectation that harm would occur if the information were released. Generalized assertions of fact without sufficient evidence do not meet the test.

Where this exemption is considered concerning contracts, it is unlikely that the harms test will be met by disclosure of standard clauses found in all or most contracts of a similar nature. If the exemption is applied to the contract, such clauses may be disclosed by release of a severed copy.

The "competitive position" could be prejudiced without resulting in any immediate or direct loss. There must be a competitive community where another's knowledge of the relevant information could affect the competitive position.

The "negotiations" for which the exemption may be claimed are contractual negotiations or some similar type, such as negotiations relating, to the settlement of a lawsuit or negotiations regarding the funding of a non-profit agency.

The injury contemplated may be either to the third party submitting the information, or to any person, or group of persons, or to an organization other than an institution.

Impede Supply of Similar Information

s.17(1)(b) FIPPA / s.10(1)(b) MFIPPA

This subsection applies where disclosure could reasonably be expected to result in similar information no longer being supplied to an institution where it is in the public interest that similar information continue to be supplied.

Release of the information would deter the voluntary supply of similar information from the same or another source. The consideration here is whether a third party requires assurance of confidentiality prior to voluntarily supplying information. The test is whether the third party or another source would entrust similar information to the institution in the future if the information were disclosed. If not, this subsection applies.

A further necessary test is that it is in the public interest that the institution continue to receive the information. At issue is the public interest, not necessarily the institution's interest.

Undue Loss or Gain

s.17(1)(c) FIPPA / s.10(1)(c) MFIPPA

This subsection applies when the disclosure could reasonably be expected to result in undue loss or gain to any person, group, committee or financial institution or agency.

The loss or gain referred to in this subsection could be of any character, but must be "undue". "Undue" means more than necessary, improper, or unwarranted. The loss or gain need not be attributable to the third party submitting the information, but to "any person, group, committee or financial institution or agency".

Labour Relations Information

s.17(1)(d) FIPPA / s.10(1)(d) MFIPPA

This subsection applies where disclosure could reasonably be expected to reveal a report or information supplied to a conciliation officer, mediator, labour relations officer or other person appointed to resolve labour relations dispute.

Tax Information (FIPPA)

s.17(2) FIPPA

This subsection also provides a mandatory exemption for records which reveal information obtained on a tax return for records which are gathered to collect a tax or determine tax liability. The injury tests in subsection 17(1) do not apply to subsection 17(2).

Exception to Exemption for Third Party Information

s.17(3) FIPPA / s.10(2) MFIPPA

This subsection gives the head discretion to release information described in s.17 FIPPA / s.10 MFIPPA if the person to whom the information relates consents. The person to whom the information relates could be the third party who submitted it, or any other person who is a subject of the information.

For example: Where a contractor supplies information about itself and about the sub-trades on a particular project, both the contractor and the subtrades could be persons "to whom the information relates", and each would have to give consent to disclosure.

Economic and Other Interests (s.18 FIPPA / s.11 MFIPPA)

This section provides a discretionary exemption for certain proprietary information of institutions and the premature disclosure of certain plans or negotiating strategies. Information affecting the interests of third parties is covered by s.17 Freedom of Information and Protection of Privacy Act (FIPPA) / s.10 Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

Subsections 18(1)(a) through (g) FIPPA / s.11(a) through (g) MFIPPA set out the types of information and circumstances covered by this exemption. Subsection 18(2) FIPPA contains an exception to the exemption.

The compelling public interest provision in s.23 FIPPA / s.16 MFIPPA applies to this exemption. Where the head exercises his/her discretion to withhold the record, the head must consider whether the public interest in disclosure outweighs the need for confidentiality.

Commercial Information

s.18(1)(a) FIPPA / s.11(a) MFIPPA

This subsection allows the institution to refuse access to trade secrets, or financial, commercial, scientific or technical information belonging to an institution that has monetary value or potential

monetary value. The terms trade secrets, or financial, commercial, scientific or technical information have the same meaning as in s. 17 FIPPA / s. 10 MFIPPA. Having monetary value or potential monetary value means that the trade secret or information is or is potentially marketable. The information may belong to the institution with custody of the record or another institution. This exemption may not apply where the information in the record is in the public domain through a bona fide publication or court record.

Employee Research

s.18(1)(b) FIPPA / s.11(b) MFIPPA

This subsection exempts information obtained through research by an employee of an institution where the disclosure could reasonably be expected to deprive the employee of priority of publication. The employee must be able to establish his/her intention to publish the information.

Economic Interests

s.18(1)(c) FIPPA / s.11(c) MFIPPA

This subsection exempts information where the disclosure could reasonably be expected to prejudice the economic interests or competitive position of an institution.

"Economic interests" concern the production, distribution and consumption of goods and services. If it can be reasonably expected, for instance, that disclosure of certain information would cause an institution to pay a higher price for goods and services, that information may be exempt under this provision.

"Competitive position" applies only to those institutions engaged in the supply of goods and services on a competitive basis.

In applying this exemption, the institution must present evidence that is detailed and convincing and must describe a set of facts and circumstances that would lead to a reasonable expectation that harm would occur if the information were released. Generalized assertions of fact without sufficient evidence do not meet the test.

Financial Interests

s.18(1)(d) FIPPA / s.11(d) MFIPPA

This subsection exempts information where the disclosure could reasonably be expected to be injurious to an institution's financial interests (MFIPPA) or the Ontario Government's ability to manage the economy of Ontario. Financial interests refers to an institution's financial position, its ability to collect taxes and generate revenues, and its ability to protect its own interests in financial transactions with third parties, including other governments.

An institution's belief that it may be sued if records are disclosed is not sufficient to invoke this exemption. The exemption is based on reasonable expectations of injury and evidence is required to substantiate the assertion of injury.

Negotiating Strategy

s.18(1)(e) FIPPA / s.11(e) MFIPPA

An institution may refuse to disclose positions, plans, procedures, criteria, or instructions to be applied to any negotiations carried on, or to be carried on, by or on behalf of an institution. This exemption is intended to protect an institution's ability to negotiate effectively with other parties. It extends to options, fall-back positions and tactics developed as part of the negotiating process. It also applies to on-going or future negotiations.

"Negotiations" in this context means discussions and communications where the intent is to arrive at a settlement or agreement.

Personnel or Administration Plans

s.18(1)(f) FIPPA / s.11(f) MFIPPA A head may refuse to disclose a record that contains plans relating to managing personnel or the administration of an institution that have not yet been put into operation or been made public. This exemption does not apply once a plan has been put into effect or publicly disclosed. The exemption is intended to cover an institution's internal management plans such as a reorganization, relocation, or creation of an agency prior to implementation. Typically, this exemption would apply to records containing detailed methods,

schemes or designs that are characteristic of a plan, rather than records with advice for developing a plan, to resolve issues.

See also s.13(2)(i) and s.65(6)(3) FIPPA / s.7(2)(h) and s.52(3)(3) MFIPPA concerning proposals to change or establish a public program.

Policy Decisions/Unfair Advantage

s.18(1)(g) FIPPA / s.11(g) MFIPPA

This subsection exempts information such as proposed plans, policies or projects where disclosure could reasonably be expected to result in:

- premature disclosure of a pending policy decision, or
- undue financial benefit or loss to a person.

"Undue" means more than necessary, improper or unwarranted.

This is a time limited exemption in that it covers only proposed plans, policies or projects. It applies when one of the two specified results can reasonably be expected to occur due to the disclosure. There must be evidence to substantiate the assertion that one of the results would occur.

Examination or Test Questions

s.18(1)(h) FIPPA / s.11(h) MFIPPA

An institution may refuse to disclose questions that are to be used in an examination or test for an educational purpose. Once the question is no longer to be used in an exam or test, the exemption does not apply.

Questions for a job competition are not included in this exemption.

Submissions Under the Municipal Boundary Negotiations Act

s.18(1)(i) FIPPA / s.11(i) MFIPPA

This subsection exempts records containing submissions made under the *Municipal Boundary Negotiations Act*, by a party municipality or other body. This exemption is time limited and may

be only be invoked until the matter, to which these submissions relate has been resolved under the *Act*.

Exception to Exemption for Economic and Other Interests (FIPPA)

S.18(2) FIPPA

This subsection is an exception to the subsection 18(1) exemption. It requires the disclosure of a record that contains the results of certain product or environmental testing. The testing can be carried out either by or for the institution (by another institution or person). The two circumstances when the head is not required to disclose are when:

- the testing was done as a service to a person, a group of persons or an organization other than an institution for a fee (e.g., a commercial product test); or
- the testing was preliminary or experimental for the purpose of developing methods of testing.

Disclosure of a report of a test carried out on a product for the purpose of the government equipment testing or consumer test report is discussed under subsection 13(2)(e).

Solicitor-Client Privilege (s.19 FIPPA / s.12 MFIPPA)

This discretionary exemption covers records subject to the common-law solicitor-client privilege (Branch 1) or those records prepared by or for Crown counsel or counsel employed or retained by an institution, for use in giving legal advice or in contemplation of or for use in litigation (Branch 2). Branch 2 can apply regardless of whether the common-law privilege applies.

Under FIPPA, "Crown counsel" includes any person acting in the capacity of legal advisor to an institution.

"Legal advice" includes a legal opinion about a legal issue and a recommended course of action based on legal considerations. It does not include information which was provided about a matter having legal implications where no legal opinion was expressed or where no course of action based on legal considerations was recommended. The fact that a lawyer reviewed a record does not of itself mean that the record falls within the exemption.

The opinion of an institution's legal advisors should always be sought before this exemption is used. Institutions must take care to ensure that that legal opinions are not released to another party as the solicitor-client privilege might be jeopardized.

The public interest override in s.23 Freedom of Information and Protection of Privacy Act (FIPPA) / s.16 Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) does not apply.

Application to Legal Advice (Branch 1)

The common law privilege (Branch 1) applies to: 1) all communications, verbal or written, of a confidential character, between a client, or his or her agent, and a legal advisor directly related to seeking, formulating or giving of legal advice or legal assistance (including the legal advisor's working papers directly related thereto); and 2) papers and materials created or obtained especially for a lawyer's brief for litigation, whether existing or contemplated.

For solicitor-client privilege to apply, four criteria must be met:

- there must be a written or oral communication;
- the communication must be of a confidential nature;
- the communication must be between an institution and a legal advisor; and
- the communication must be directly related to seeking, formulating or giving legal advice.

Application to Litigation Records (Branch 2)

Branch 2 of the section provides an exemption for all materials prepared for the purpose of obtaining legal advice whether in contemplation or litigation or not, as well as for all documents prepared in contemplation of or for use in litigation. This means that any communication, even of a non-confidential nature, between a lawyer and client or between a lawyer and third parties which is conducted for the purpose of litigation is privileged.

For a document to be "prepared... in contemplation of litigation", two criteria must be met:

- (a) contemplated litigation must be the dominant purpose for preparing the record, and
- (b) there must be a reasonable prospect of such litigation at the time the document was prepared; the litigation must be more than just a vague or theoretical possibility.

Waiver

Only the client is entitled to waive the solicitor-client privilege and thereby authorizing disclosure of the record. For such a waiver to be effective, there must be specific evidence of the client's waiver of the privilege. The client's waiver will not be implied from the fact that

individuals or institutions other than the solicitor or client have possession of the record. However, the IPC has found instances where there was an implied waiver of privilege and the record was ordered disclosed. In one instance, a client disclosed an opinion to a specific party, intentionally and without any restrictions on its use, and the IPC found that this release constituted a waiver of the solicitor-client privilege. In another instance, an institution was found to have implicitly waived solicitor-client privilege with respect to a letter that was located in a land development file. The file was available for review by the public and had been seen by the requester in that way. Two additional facts were important to the outcome of the case: the institution did not remove the record from the file once it was aware of the problem and it did not make any representations on the issue of waiver during the appeal process.

Institutions must take care to ensure that legal opinions are not released to a specific party as the solicitor-client privilege may be jeopardized. If an institution wishes to release privileged information to a specific party, it should place restrictions on its use if it wishes to retain the solicitor-client privilege.

Danger to Safety or Health (s.20 FIPPA / s.13 MFIPPA)

This section of the Freedom of Information and Protection of Privacy Act (FIPPA)/Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) provides a discretionary exemption relating to records, the disclosure of which could reasonably be expected to seriously threaten the safety or health of any individual. The wording "reasonable expectation of harm" requires an institution to establish a clear and direct linkage between disclosure of information and the harm alleged.

This exemption is not intended to restrict an individual's right of access to his/her own personal information, except where disclosure could threaten the safety or health of another individual. Where there is an exemption and the head has exercised his/her discretion against disclosure, the head should also consider whether disclosure of the record could reasonably be expected to endanger the life or physical safety of a law enforcement officer or any other person under s.14(1)(e) FIPPA / s.8(1)(e) MFIPPA.

The public interest override in s.23 FIPPA / s.16 MFIPPA applies to this exemption but not to the exemption provided by s.14 (1)(e) FIPPA / s.8 (1)(e) MFIPPA.

"In Ontario (Minister of Labour), the Court of Appeal for Ontario drew a distinction between the requirements for establishing "health or safety" harms under sections 14(1)(e) and 20, and harms under other exemptions. The court stated (at p. 6): The expectation of harm must be reasonable, but it need not be probable. Section 14(1)(e) requires a determination of whether there is a reasonable basis for concluding that disclosure could be expected to endanger the life or physical safety of a person. In other words, the party resisting disclosure must demonstrate that the reasons for resisting disclosure is not a frivolous or exaggerated expectation of endangerment to safety. Similarly [section] 20 calls for a demonstration that disclosure could reasonably be expected to seriously threaten the safety or health of an individual, as opposed to there being a

groundless or exaggerated expectation of a threat to safety. Introducing the element of probability in this assessment is not appropriate considering the interests that are at stake, particularly the very significant interest of bodily integrity. It is difficult, if not impossible, to establish as a matter of probabilities that a person's life or safety will be endangered by the release of a potentially inflammatory record. Where there is a reasonable basis for believing that a person's safety will be endangered by disclosing a record, the holder of that record properly invokes [sections] 14(1)(e) or 20 to refuse disclosure. [D]espite this distinction, the party with the burden of proof under section 20 still must provide 'detailed and convincing evidence' of a reasonable expectation of harm to discharge its burden. This evidence must demonstrate that there is a reasonable basis for believing that endangerment will result from disclosure or, in other words, that the reasons for resisting disclosure are not frivolous or exaggerated." (Order #s MO-1262, PO-1747 and PO-1861)

Personal Privacy (s.21 FIPPA / s.14 MFIPPA)

Section 21 FIPPA / s.14 MFIPPA

This section of the Freedom of Information and Protection of Privacy Act (FIPPA)/Municipal Freedom of Information and Protection of Privacy Act (MFIPPA):

- provides a mandatory exemption relating to the disclosure of personal information to an individual other than the individual to whom the information relates, except in the circumstances specified in this section. It provides an exemption from the disclosure of personal information in response to a formal request under the Act.
- is one of the keystone provisions of the Act. It balances the public's right of access to records and the individual's right of privacy respecting personal information.
- requires the institution to refuse to disclose personal information, unless one of the circumstances listed in 21(1)(a) through (f) FIPPA / s.14(1)(a) through (f) MFIPPA apply.

Subsections 21(2)(a) through (i) FIPPA / s.14(2)(a) through (i) MFIPPA:

- lists circumstances which should be considered in determining whether a disclosure of personal information constitutes an unjustified invasion of personal privacy.

Subsection 21(3) FIPPA / s.14(3) MFIPPA:

- sets out circumstances where disclosure is presumed to be an unjustified invasion of personal privacy.

Subsection 21(4) FIPPA / s.14(4) MFIPPA:

- lists when disclosure does not constitute an unjustified invasion of personal privacy.

Subsection 21(5) FIPPA / s.14(5) MFIPPA:

- permits an institution to refuse to confirm or deny the existence of a record if its disclosure would constitute an unjustified invasion of privacy.

Where an institution has reason to believe that a disclosure might constitute an unjustified invasion of personal privacy, s.21 FIPPA / s.14 MFIPPA directs an institution to give notice to the person to whom the personal information relates disclosing the record. This person must be given the opportunity to make representations about the disclosure. See Notices to Affected Third Parties in Chapter 3 (Access Procedures).

This exemption is subject to the public interest override in s.23 FIPPA/ s.16 MFIPPA. Where this exemption applies, the head must consider whether or not the public interest outweighs the interest in privacy. Prior to releasing information in the public interest, the head must follow the notification requirements in s.28 FIPPA/ s.21 MFIPPA.

Section 49 FIPPA/ s.38 MFIPPA is the relevant section when deciding the disclosure of personal information to the person to whom it pertains.

Note that certain records containing labour relations and employment-related information are excluded from FIPPA/MFIPPA. (See Exclusionary Provisions in Chapter 3 of this Manual)

Personal Privacy

s.21(1) FIPPA / s.14(1) MFIPPA

This subsection requires the institution to refuse to disclose personal information to someone other than the person to whom the information relates, unless one of the circumstances or exceptions listed in 21(1)(a) through (f) FIPPA / s.14(1)(a) through (f) MFIPPA applies.

Consent

s.21(1)(a) FIPPA / s.14(1)(a) MFIPPA

Personal information may be disclosed to someone other than the individual to whom the information relates with the prior request or consent of the individual. The record must be one to which the individual is entitled to have access.

The request or consent should be in writing and be received before the personal information is disclosed. It is good practice to confirm the identity of the person giving consent.

Compelling Circumstances

s.21(1)(b) FIPPA / s.14(1)(b) MFIPPA

Personal information may be disclosed to someone other than the individual to whom the information relates in compelling circumstances affecting the health or safety of an individual, not necessarily the individual to whom the information relates.

Circumstances are "compelling" when either there is no other way to obtain personal information affecting health or safety, or there is an emergency situation where the delay in obtaining the information would be injurious to someone's health or safety. The determination of when compelling circumstances exist is left to the discretion of the head.

Where personal information is released under this subsection, upon disclosure, notification must be mailed to the last known address of the individual to whom the information relates. If the institution does not have the address, it should attempt to find out the address of the individual from the person who made the request.

Public Records

s.21(1)(c) FIPPA / s.14(1)(c) MFIPPA

Personal information may be disclosed to someone other than the individual to whom the information relates if the personal information is collected and maintained specifically for the purpose of creating a record available to the general public.

A public record refers to a collection of personal information to which all members of the public have equal access. In order to satisfy this exception, it must be shown that the personal information was collected and maintained "specifically" for the purpose of making it available to the general public. See Chapter 5 (Privacy Protection) for further discussion of public records.

Public records are created to allow the public, in specific circumstances, access to personal information which would not normally be available. The public's "need to know" must outweigh the privacy protection rights of the individuals to whom the information relates.

Personal information is usually maintained in public records for the following reasons:

- To allow for the proper administration of programs, activities and services, (e.g. list of electors, assessment roll).
- To promote government accountability, by providing information relating to the issuance of licences, permits, government contracts, etc.
- To promote informed choice and consumer protection, (e.g. by making available records such as land registry records, assessment rolls, bills of sales registration, personal property security registration system, records of holders of specific licences and permits etc.).
- To allow for the fair determination of rights.

Key Features of Public Records

- (a) The record must be equally available to all members of the public. A collection of personal information to which only some people have access while others do not, would not qualify as a public record as contemplated in the Act.
- (b) Public availability does not mean the information is necessarily accessible free of charge. There are a number of existing public records which require the payment of fees for access.
- (c) When a public record of personal information is created or maintained, public availability does not have to be the only purpose for collecting and maintaining the information. For example, the land tax register is used for the administration of the property taxing program, but the information contained in these records is also needed by individuals for a number of business-related purposes.
- (d) Access to a public record does not necessarily mean it is readily available without some identifying information. There are situations where an individual must provide the institution with specific details or identifiers to allow the institution to retrieve the record. The fact that existing systems for access are not as convenient or as cost effective to a requester does not mean that the records are not publicly available.
- (e) Personal information appearing in a public record in one context does not necessarily render the information public in another context. For example, personal information relating to criminal convictions may be publicly available through court records, but a record of criminal convictions in a personnel or security file would not thereby be a public record.
- (f) There can be instances where only certain elements of a collection of personal information are maintained as a public record, while other parts are not available to the public.

How Public Records Are Created

In many jurisdictions, public records of personal information are created and maintained through specific statutes or regulations. However, in Ontario, public records can be created either by:

- (a) Statute; or
- (b) Policy Decisions by Institutions.

(a) Statute

Statutes, regulations or by-laws designating public records generally contain terms and conditions regarding the administration of the information. Often, the authority to charge fees, times and location of access, are prescribed in the legislation.

(b) Policy Decisions by Institutions

There are situations where public records exist without a legislative basis. The institution, through its dealings with the public, may determine that there is a legitimate "public need to know" which outweighs the privacy rights of the individuals to whom the information relates. In such cases, the institution may establish a policy designating the record public. The major factors

in this decision would be the privacy protection rights of individuals and whether or not release of the information can be treated as a "justified" invasion of personal privacy.

Factors to Consider

The following are some of the factors to consider in the creation and maintenance of public records:

- Does the public "need to know" outweigh the privacy rights of the individuals concerned?
- Will the release of the information foster informed choice?
- Will the information be accessible to everyone?
- Does the public need the information to assist in the conduct of business?
- Would the public availability of the information constitute an unjustified invasion of personal privacy?
- Is the personal information particularly sensitive?
- Is the information relevant to the fair determination of a requester's rights?

While the Act is silent on statutory requirements governing the creation and maintenance of public records, the balance between the need for disclosure and the right of individuals to privacy must be carefully weighed. In such circumstance the balancing test (see personal privacy section of the Act) outlining the criteria in determining whether a disclosure of personal information constitutes an unjustified invasion of personal privacy, can play an important role in helping an institution decide if a collection of personal information will, or will not, be available as a public record.

Disclosure Expressly Authorized by Statute

s.21(1)(d) FIPPA / s.14(1)(d) MFIPPA

Personal information may be disclosed to a person other than the individual to whom it relates where a statute of Ontario or Canada expressly authorizes the disclosure.

The authority to disclose must be stated in the statute and not simply be an administrative policy of the institution.

For example: Section 14 of the *Business Practice Act* permits information gained during an inspection or investigation to be disclosed to inform a consumer of an unfair business practice and any information relevant to the consumer's rights.

Research Agreements

s.21(1)(e) FIPPA / s.14(1)(e) MFIPPA

When certain conditions are met, personal information may be disclosed to someone other than the individual to whom the information relates if the disclosure is for a research purpose. "Research purposes" are distinct from administrative, operational or regulatory uses of personal information in that research uses do not directly affect the individual to whom the information relates and do not relate to the usual administration of a program. Program audits, evaluations and operational reviews are not research for the purposes of this section. "Research" means a systematic investigation into and study of materials and sources in order to establish facts and reach new conclusions and an endeavour to discover new or to collate old facts by the scientific study or by a course of critical investigation.

This provision covers disclosures in response to access requests from researchers receiving grants, consultants conducting contractual research and independent researchers. Access to personal information by researchers who are employees of an institution is not covered by this subsection but rather by s.41 FIPPA / s.31 MFIPPA and s.42(d) FIPPA / s.32(d) MFIPPA.

The institution must determine that conditions are appropriate for the disclosure of personal information for a research purpose. The following conditions must be met:

- the disclosure must be consistent with the conditions or reasonable expectations of disclosure under which the personal information was provided, collected or obtained. If the information was provided with a reasonable expectation of confidentiality, access should not be granted without the consent of the individual;
- the research purpose for which the disclosure is to be made cannot be reasonably achieved unless the information is provided in a form which allows individuals to be identified. The head must be satisfied that the objective necessitates individual identification;
- the researcher must comply with conditions relating to security and confidentiality prescribed by regulation.

See Appendix VIII for a sample research agreement.

Unjustified Invasion of Personal Privacy

s.21(1)(f) FIPPA / s.14(1)(f) MFIPPA

Personal information may be disclosed to someone other than the individual to whom the information relates where the disclosure does not constitute an unjustified invasion of personal privacy. This provision is an exception to the mandatory exemption. Sections 21(2)(3) and (4) FIPPA / s.14(2)(3) and (4) MFIPPA provide guidance in determining whether disclosure of personal information would constitute an unjustified invasion of personal privacy. Where one of the presumptions in s.21(3) FIPPA / s.14(3) MFIPPA applies to the personal information found in a record, the only way such a presumption against disclosure can be overcome is if the personal information falls under s.21(4) FIPPA / s.14(4) MFIPPA or where a finding is made that s.23 FIPPA / s.16 MFIPPA applies to the personal information.

If none of the presumptions in s.21(3) FIPPA / s.14(3) MFIPPA apply, the head must consider the application of the factors listed in s.21(2) FIPPA / s.14(2) MFIPPA, as well as all other relevant circumstances in the case.

Factors to be Considered

s.21(2) FIPPA / s.14(2) MFIPPA

If none of the presumptions in s.21(3) FIPPA / s.14(3) MFIPPA apply, the head must consider the factors listed in s.21(2) FIPPA / s.14(2) MFIPPA. This list of factors is not exhaustive. Any other relevant circumstances should be considered by the institution before a decision on disclosure is made. For example, one unlisted factor favouring disclosure of personal information may be ensuring or restoring public confidence in an institution.

Public Scrutiny

s.21(2)(a) FIPPA / s.14(2)(a) MFIPPA

One factor in determining whether disclosure of personal information constitutes an unjustified invasion of privacy is whether disclosure is desirable for subjecting the activities of government institutions to public scrutiny. In such cases, access to information and internal scrutiny of the internal workings of government will prevail over the protection of individual privacy. When invoking this provision, institutions should consider the broader interests of public accountability. There must be a public demand for scrutiny of the institution, not one person's personal view or opinion. The requester must demonstrate that the activities of the institution to which the record relates have been publicly called into question.

Public Health and Safety

s.21(2)(b) FIPPA / s.14(2)(b) MFIPPA

In determining whether disclosure constitutes an unjustified invasion of personal privacy, the head must consider whether access to the personal information may promote public health and safety.

For example: The identification of the location of a discharge or emission or some other potential danger to the environment may necessitate the disclosure of personal information.

Informed Choice

s.21(2)(c) FIPPA / s.14(2)(c) MFIPPA

In determining whether disclosure of the personal information constitutes an unjustified invasion of personal privacy, the head must consider whether the disclosure will promote informed choice in the purchase of goods and services.

For example: Disclosure of an evaluation of a supplier's or consultant's performance could disclose personal information.

Fair Determination of Rights

s.21(2)(d) FIPPA / s.14(2)(d) MFIPPA In determining whether the disclosure constitutes an unjustified invasion of personal privacy, the head must consider whether the personal information is relevant to a fair determination of rights affecting the requester. There may be instances where the requester requires access to personal information about his / her own rights.

In order for this section to be relevant, the following factors must be established: 1. the right in question is a legal right, which is based in common law or statute; 2. the right is related to a proceeding which is either existing or contemplated; 3. the personal information which the appellant is seeking access to has some bearing on or is significant to the determination of the right in question; and 4. the personal information is required in order to prepare for the proceeding or to ensure an impartial hearing.

Unfair Exposure to Harm

s.21(2)(e) FIPPA / s.14(2)(e) MFIPPA

The head must consider whether the individual to whom the information relates will be exposed unfairly to pecuniary or other harm. Other provisions of the Act exempt records on the basis that disclosure may threaten someone's life, health or safety (s. 14(1)(e) FIPPA/ s.8(1)(e) MFIPPA). The words "other harm" should therefore be interpreted narrowly to mean injury of a similar nature to pecuniary harm, such as harm to business interest.

This consideration is relevant only where there is evidence that unfair pecuniary or other harm will result from the disclosure.

Highly Sensitive Information

s.21(2)(f) FIPPA / s.14(2)(f) MFIPPA

The head must consider whether the personal information is highly sensitive to the individual to whom it relates. In order for information to be "highly sensitive", the institution must establish that release of the information would cause excessive personal distress to persons other than the requester, this includes the violation of personal security. The fact that an individual may be embarrassed by a disclosure of personal information is not sufficient to make this factor a relevant consideration.

Information Inaccurate or Unreliable

s.21(2)(g) FIPPA / s.14(2)(g) MFIPPA

In this circumstance, the head must consider whether the personal information is unlikely to be accurate or reliable. This factor weighs against disclosure of personal information. Where there is sufficient reason to question the accuracy or reliability of the records, it may be an unjustified invasion of personal privacy to release it. For this factor to be relevant, it must be shown in specific ways that the information received is inaccurate or unreliable.

Subsection 40(2) FIPPA / s.30(2) MFIPPA requires institutions to take reasonable steps to ensure that personal information is not used unless it is accurate and up to date.

Information Supplied in Confidence

s.21(2)(h) FIPPA / s.14(2)(h) MFIPPA The head must consider whether the personal information has been supplied to the institution in confidence by the person to whom it relates. This section does not apply to personal information supplied in confidence by one individual about another.

For example: Complaint information was sent by concerned citizens regarding an alleged trespass to property was expected to be kept confidential and as a result, this provision was a relevant factor.

Damage to Reputation

s.21(2)(i) FIPPA / s.14(2)(i) MFIPPA

The head must consider whether disclosure of the personal information may unfairly damage the reputation of any person referred to in the record. Damage to a reputation may not always be considered unfair.

For example: The IPC found that releasing an investigation which probed the appropriateness of a senior official's foreign currency trading activities, would not "unfairly" damage the official's reputation.

Presumed Invasion of Privacy

Subsection 21(3) FIPPA / s.14(3) MFIPPA provides that disclosure of certain types of personal information is presumed to be an unjustified invasion of personal privacy. The main characteristics of these types or classes of personal information are that they concern intimate, sensitive details of personal life or they give rise to a strong expectation that privacy will be protected. Where one of the presumptions in this subsection applies to the personal information found in a record, the only way the presumption against disclosure can be overcome is if the personal information falls under s.21(4) FIPPA / s.14(4) MFIPPA or where a finding is made that s.23 FIPPA / s.16 MFIPPA applies to the personal information.

Health Record

s.21(3)(a) FIPPA / s.14(3)(a) MFIPPA

Disclosure of information that relates to a medical, psychiatric or psychological history, diagnosis, condition, treatment or evaluation is presumed to constitute an unjustified invasion of personal privacy.

Violation of Law

s.21(3)(b) FIPPA / s.14(3)(b) MFIPPA

Disclosure of personal information compiled as part of an investigation into a possible violation of law is presumed to constitute an unjustified invasion of personal privacy. The phrase "violation of law" includes offences under federal or provincial statutes and regulations and municipal by-laws.

For example: Personal information relating to discrimination investigations compiled by, or on behalf of, the Ontario Human Rights Commission are records compiled as part of an investigation into a possible violation of law.

The presumption applies to investigations into possible violations of law; as a result, there is no need for criminal charges to be laid or for proceedings to have been commenced for the presumption to apply. This exemption does not apply where disclosure is necessary to prosecute the violation or to continue the investigation. Disclosure of personal information qualifying for

this exemption may take place in the absence of an access request under the conditions found in s.42 (f) & (g) FIPPA / s.32 (f) & (g) MFIPPA.

Section 14 FIPPA/ s.8 MFIPPA provides an exemption for records relating to law enforcement activities. That section is complemented by this subsection, which protects the privacy of an individual who has been investigated for a possible violation of law but whose case has not yet been disposed of by a court. This section may also protect the privacy of individuals interviewed with respect to an investigation.

Eligibility for Social Programs

s.21(3)(c) FIPPA / s.14(3)(c) MFIPPA

Disclosure of information that relates to eligibility for social service or welfare benefits is presumed to constitute an unjustified invasion of personal privacy.

Employment or Educational History

s.21(3)(d) FIPPA / s.14(3)(d) MFIPPA

Disclosure of information that relates to an individual's employment or educational history is presumed to constitute an unjustified invasion of personal privacy. This presumption does not apply to employee expense claims. See also s.65(6) FIPPA / s.52(3) MFIPPA.

Tax Return

s.21(3)(e) FIPPA / s.14(3)(e) MFIPPA

Disclosure of personal information obtained on a tax return or gathered for the purpose of collecting a tax is presumed to constitute an unjustified invasion of personal privacy.

Financial History

s.21(3)(f) FIPPA / s.14(3)(f) MFIPPA

Disclosure of most types of personal information describing an individual's finances, income, assets, liabilities, net worth, bank balances, financial history or creditworthiness is presumed to constitute an unjustified invasion of personal privacy.

Personal Recommendations and Evaluations

s.21(3)(g) FIPPA / s.14(3)(g) MFIPPA

Disclosure of personal information consisting of personal recommendations or evaluations, character references, personnel evaluations is presumed to constitute an unjustified invasion of personal privacy.

Race, Ethnic Origin, Religion or Sexual Orientation

s.21(3)(h) FIPPA / s.14(3)(h) MFIPPA

Disclosure of personal information which reveals an individual's racial or ethnic origin, sexual orientation, religious or political beliefs or is presumed to constitute an unjustified invasion of personal privacy.

Exceptions to the Exemption

Section 21(4) FIPPA/ s.14(4) MFIPPA places certain limits on the presumption of invasion of personal privacy created by s.21(3) FIPPA/ s.14(3) MFIPPA. Disclosure of the types of personal information mentioned in s.21(4)(a) through (c) FIPPA/ s.14(4)(a) and (b) MFIPPA does not constitute an unjustified invasion of personal privacy. Therefore, a record that fits within those subsections must be disclosed under s.21(1)(f) FIPPA/ s.14(1)(f) MFIPPA.

Salary Range and Benefits of Employees

s.21(4)(a) FIPPA / s.14(4)(a) MFIPPA

Disclosure of the classification, salary range and benefits, or employment responsibilities of an officer or employee of an institution, or a member of the Minister's staff, is not an unjustified invasion of personal privacy. Note that the provision refers to "salary range", not specific salary.

Officer or employee includes appointed officials and those persons who work for an institution, or who perform their duties under a contract of employment.

Note that the *Public Sector Salary Disclosure Act* provides for public disclosure of salaries and benefits of employees who earn a salary of \$100, 000 or more. See s.21(4)(b) FIPPA / s.14(4)(b) MFIPPA below for factors to consider when determining if an individual is an employee or independent contractor.

Personal Service Contracts

s.21(4)(b) FIPPA / s.14(4)(b) MFIPPA

Disclosure of the financial or other details of a contract for personal services between an individual and an institution is not an unjustified invasion of privacy. A contract in which an individual, not a company, is hired to perform professional services in respect of a particular problem or project would be included.

For example: A contract in which an individual is hired to perform professional services for an institution in respect of a particular problem or project would be included.

Usually, the more control an institution exercises over an individual with respect to such matters as place of work, hours of work and vacation entitlements, the more likely a relationship is one of employer and employee. In order to determine whether a contract is a contract for personal services as opposed to an employment contract, the following factors must be considered:

1. the level of control and supervision exercised by the employer with respect to a) how the work is performed, b) where the work is performed, c) the hours of work and d) what is produced;
2. the ownership and provision of the equipment used for the job;
3. the economic dependence of the worker on the employer;
4. whether the worker is entitled to undertake alternative work while engaged by the employer;
5. whether the worker is obliged to follow the employer's organizational policies;
6. whether the worker bears any risk of loss by entering into the agreement;
7. whether the work which the individual performs is a necessary and integral component of the employer's operations.

Licences or Permits

s.21(4)(c) FIPPA

Disclosure of details of a licence or permit or a similar discretionary financial benefit conferred on an individual by an institution or a head is not an unjustified invasion of privacy under certain circumstances.

The purpose of this limitation on the presumed invasion of privacy is to ensure that the public has access to information about licensing or the granting of benefits where the licensee or recipient of the benefit represents a significant proportion of the total number of persons in Ontario who are similarly licensed or who have received a similar benefit.

The granting of a licence or permit or a financial benefit, at an institution's discretion, may give a significant economic advantage to one individual over others who are in the same business or other activity.

Where an individual represents one per cent or more of all persons and organizations who have received this type of economic advantage, and if the value of the benefit to an individual is one per cent or more of the total value of similar benefits to other persons and organizations, disclosure of details of the benefit is not an invasion of the individual's privacy.

The "value of the benefit" and the "total value of similar benefits" would be determined by dollar value where feasible.

Refusal to Confirm or Deny

s.21(5) FIPPA / s.14(5) MFIPPA

Where the head refuses to give access to a record on the grounds of an unjustified invasion of privacy, the head may also refuse to confirm or deny the existence of the record. Where the head refuses to confirm or deny the existence of a record in response to a request, notification to the requester under s.29(2) FIPPA /s.22(2) MFIPPA is required.

For example: Confirmation that an institution was in possession of a record relating to the treatment of an individual for an illness could be an unjustified invasion of privacy, even if access to the record itself was refused.

In order to use this provision, an institution must provide detailed and convincing evidence that disclosure of the mere existence of the requested records would convey information to the requester, and that the disclosure of this information would constitute an unjustified invasion of personal privacy.

This subsection is similar to s.14(3) FIPPA/ s.8(3) MFIPPA relating to law enforcement records. Notification to the requester under s.29(2) FIPPA/ s.22(2) MFIPPA would be required.

Public Appointments

The IPC has found that members of the public often wish to know some information about elected officials and appointees to public positions on boards and committees. Thus, institutions are encouraged to prepare brief biographies and make them available to the public upon request. Institutions should alert the elected official or appointee concerned before publishing the biography. Please see Appendix V for a sample biography.

Published Information (s.22 FIPPA / s.15 MFIPPA)

In the Freedom of Information and Protection of Privacy Act (FIPPA)/Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) this discretionary exemption allows an institution to refuse disclosure of a record where:

- the record or the information contained in the record has been published or is currently available to the public; or
- there are reasonable grounds to believe that the record or information will be published by the institution within 90 days of the request, or within a further period of time needed for printing the material or for translating it before printing.

This exemption is not limited to information published only by the institution. An institution has a duty to inform a requester where the record or information in question is available. Where an institution invokes this exemption, it must consider the convenience of the requester compared to the convenience of the institution.

Where an institution is dealing with an issue, which is the subject of numerous requests over a long period of time, and the institution will grant access to these records, it may be advantageous for the institution to put together a package of information and have it published. The institution could set a reasonable fee for the package.

The compelling public interest exemption in s.23 FIPPA / s.16 MFIPPA does not apply to this exemption.

Limitations on Access to One's Own Personal Information (s.49 FIPPA / s.38 MFIPPA)

Section 49 Freedom of Information and Protection of Privacy Act (FIPPA) / s. 38 Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) set out the grounds for refusing to disclose personal information to the individual to whom it pertains. The grounds are enumerated in subsections 49(a) through (f) FIPPA / 38(a) through (f) MFIPPA. When an individual seeks access to his/her personal information this section of the Act applies, not the part of the Act dealing with general exemptions or a request by a third party for access to another person's information.

The decision to refuse to disclose personal information to the individual to whom it relates is a discretionary exemption. Where this section applies, it is the record as a whole that is considered not only those parts containing the individual's own information. Individuals have greater access to their own personal information than do third parties under s.21 FIPPA / s.14 MFIPPA.

The principle of severability applies to disclosure of personal information, as it does to general information. Subsection 48(2) FIPPA / 37(2) MFIPPA allows the information which is not be disclosed to be severed pursuant to subsection 10(2) FIPPA / 4(2) MFIPPA.

General Exemptions

s.49(a) FIPPA / s.38(a) MFIPPA

An individual's right of access to his/her own personal information is subject to all the exemptions applying to general records found in Part II of FIPPA / Part I MFIPPA, except for the personal information exemption (s. 21 FIPPA / s.14 MFIPPA). That exemption applies to the disclosure of an individual's personal information to a third party.

Unjustified Invasion of Another's Personal Privacy

s.49(b) FIPPA / s.38(b) MFIPPA

An individual may be refused access to his/her own personal information if disclosure would constitute an unjustified invasion of another individual's personal privacy. Subsections 21(2) and (3) FIPPA / s.14(2) and (3) MFIPPA provide the test for determining an unjustified invasion of personal privacy and guidance in interpreting this subsection.

There may be personal information about more than one individual in the same record and severing may not be feasible because the information is so intertwined. For example, severing may not be feasible because close family or business ties would allow individuals other than the requester to be identified despite the severing. In such a case, disclosure would not be possible because it would invade the privacy of individuals other than the requester.

This is a discretionary exemption and even if disclosure of personal information would be an unjustified invasion of another person's privacy, discretion can be exercised in favour of disclosure. Section 28 FIPPA / s.21 MFIPPA requires the head to notify the individual whose personal privacy may be invaded as a result of disclosure of the records. (See Notices to Affected Third Parties in Chapter 3 (Access Procedures)).

Revealing a Confidential Source

s.49(c) FIPPA / s.38(c) MFIPPA

An individual may be refused access to his/her own personal information when:

- 1) the personal information is evaluative or opinion material;

2) the personal information was compiled solely for the purpose of determining suitability, eligibility or qualifications for employment or for the awarding of government contracts and other benefits;

3) the information was supplied to the institution in circumstances where it may reasonably have been assumed that the identity of the source would be held in confidence;

4) the disclosure of the record would reveal the identity of the source of the information.

Each element of the four-part test must be satisfied in order for the exemption to apply. Further, the exemption only applies to information that would reveal the identity of the source.

"Evaluative" and "opinion" means a personal or subjective interpretation of objective facts (e.g. test scores, ratings and grades). The phrase "information furnished to the institution" may indicate a source within as well as outside the institution. "Other benefits" includes the conferring of awards, grants or similar benefits.

Medical Information

s.49(d) FIPPA / s.38(d) MFIPPA

The institution may refuse to disclose to an individual his/her own personal information where the disclosure could reasonably be expected to prejudice the individual's mental or physical health. It is intended that this provision only be applied in circumstances when disclosure could cause injury or prove detrimental to the individual's mental or physical health. It is not intended as a general provision for withholding access to medical information. Wherever possible, an individual should be granted access to his/her medical information.

Consultation with an appropriate health care professional may be advised to determine whether there is a reasonable expectation of prejudice to the individual's mental or physical health. When the information is disclosed to the requester, the institution may also wish to have the health care professional present to provide explanations and answer questions.

Correctional Record (FIPPA)

s.49(e) FIPPA

The head may refuse to disclose personal information in a correctional record to the individual where disclosure could reasonably be expected to reveal information received in confidence.

Correctional records, such as those of inmates in correctional facilities, may contain personal information that identifies informants or may contain information related to active law

enforcement investigations. The head may refuse to disclose the individual's personal information if it would reveal the identity of a source or reveal investigative or other information supplied in confidence.

Subsection 14(1)(d) FIPPA provides a similar exemption for law enforcement records. Subsection 14(2)(d) provides an exemption for records containing information about persons under the control or supervision of a correctional authority.

Research or Statistical Record

s.49(f) FIPPA / s.38(e) MFIPPA

An individual may be refused access to his/her own personal information if the information was collected and used exclusively for a research or statistical purpose not directly affecting the individual. If the information is used or disclosed for any other purpose, this exemption can not be relied on to withhold it from the person to whom it pertains.

Chapter 5: Privacy Protection

Table of Contents

- Introduction
- Public Records
- Labour Relations and Employment-Related Records
- Collection of Personal Information
 - Expanded Definition of Personal Information
 - Authority to Collect
 - Manner of Collection
 - Individual Authorization
 - Disclosure Under s.42 FIPPA / s.32 MFIPPA
 - Authority of the Commissioner
 - Consumer Reporting Act
 - Honour or Award
 - Courts and Tribunals
 - Law Enforcement
 - Statutory Authority
 - Notification Requirements
 - Exception to Notice Requirements
- Retention of Records
- Accuracy of Records
 - Exception to Accuracy Requirement
- Disposal of Records
- Use of Personal Information
 - Individual Consent
 - Purpose for Which Information Collected
 - For the Purpose Disclosed
- Disclosure of Personal Information
 - Disclosure in Accordance with Part II FIPPA / Part I MFIPPA
 - Consent to Disclosure
 - Consistent Purpose
 - In Performance of Duties
 - Act of Legislature or Parliament
 - Disclosure to Law Enforcement Agency
 - Aid in Law Enforcement
 - Compelling Circumstances
 - Compassionate Circumstances
 - To a Member of the Legislature
 - To a Member of the Bargaining Agent
 - Disclosure to Responsible Minister

- Disclosure to Information and Privacy Commissioner
 - Government of Canada or Government of Ontario
 - Consistent Purpose
 - New Use/Disclosure of Personal Information
 - Role of Information and Privacy Commissioner
-

Introduction

The protection of personal privacy is one of the key principles of the Freedom of Information and Protection of Privacy Act (FIPPA) / Municipal Freedom of Information and Protection of Privacy Act (MFIPPA). The personal privacy requirements, set out in Part III FIPPA/ Part II MFIPPA, deal with privacy protection in the day-to-day operations of institutions. These parts reflect internationally accepted principles of fair information practices, and are based on two key principles:

- that an individual has the right to control his or her own personal information; and
- that the privacy rules governing the collection, use, disclosure, retention and disposal of personal information are necessary.

These privacy rules apply to all personal information in the custody or control of institutions, with the exception of public records and certain employment-related and labour relations records.

Public Records

s.37 FIPPA / s.27 MFIPPA

The privacy requirements do not apply to personal information maintained for the purpose of creating a record that is available to the general public.

Public records of personal information are records to which all members of the public have equal access. Personal information to which some members of the public have access, while others do not, is not a public record.

For example: A public record is a list of electors as required by the *Municipal Elections Act*. Assessment rolls, as required by s.39 of the *Assessment Act*, are public records. Records of court proceedings that are publicly available by virtue of the *Courts of Justice Act* are not subject to the privacy rules.

The Information and Privacy Commissioner has stated in a number of privacy investigation reports that the public records exception applies "only if the information in question is held by

the institution maintaining it for the express purpose of creating a record available to the general public. Other institutions cannot claim the benefit of the public records exception for the same personal information unless they, too, maintain the personal information for the purpose of making it available to the general public" (e.g. (Privacy Investigation Report #I94-011P).

As a result, institutions should consider the privacy implications of their business practices even when they are handling otherwise "public" information. For example, it is not appropriate for institutions to maintain profiles or dossiers on individuals even when the personal information has been gathered from public sources such as newspaper clippings. (This would not apply when the personal information in question relates to information about individuals acting in a representative or professional capacity such as politicians, lobbyists or representatives of groups or organizations).

Labour Relations and Employment-Related Records

s.65(6), (7) FIPPA / s.52(3), (4) MFIPPA

FIPPA/MFIPPA does not apply to most employment-related and labour relations information in which an institution has an interest. Nonetheless, certain records such as employee expense accounts, and agreements arising out of negotiations about employment-related matters between an institution and an employee(s) continue to be covered by FIPPA/MFIPPA. For further discussion regarding this category of excluded records refer to Chapter 3 (Access Procedures) or the Annotation of Commissioner's Orders.

Collection of Personal Information

s.38, 39 FIPPA / s.28, 29 MFIPPA

Expanded Definition of Personal Information

s.38(1) FIPPA / s.28(1) MFIPPA

The privacy provisions dealing with the collection of personal information apply to both recorded and non-recorded personal information - that is, to personal information which is collected verbally.

All other privacy provisions in the Act, dealing with use, disclosure, retention, disposal and access to personal information apply only to recorded personal information about an individual.

Authority to Collect

s.38(2) FIPPA / s.28(2) MFIPPA

This section sets out the conditions under which personal information may be collected. Personal information is collected when the institution actively acquires the information or invites an individual or others to send personal information to the institution. An individual may submit personal information on his/her own initiative without the information being requested by the institution. Receipt of this information is not considered a collection unless the institution keeps or uses the information.

One of three conditions must exist in order for personal information to be collected:

- the collection of personal information is expressly authorized by a statute. The authority to collect must be in a statute rather than in a regulation; or
- the information collected is used for the purposes of law enforcement; or
- the collection is necessary for the proper administration of a lawfully authorized activity (provincial institutions may have this activity authorized by statute, regulation or order-in-council; local governments by statute, regulation or by-law).

By implication, this authority to collect personal information is limited to the collection of necessary information.

For example: It was necessary to the proper administration of a lawfully authorized activity for the Family Support Plan to collect health plan numbers and photographs of individuals who have support or custody orders existing against them. This information was necessary in order to trace individuals, assist in enforcing orders and serve documents personally. (**Privacy Investigation Report #I92-38P**)

Further, the phrase "expressly authorized by statute" requires either that the specific types of personal information collected be expressly described in the statute or a general reference to the activity be set out in the statute, together with a specific reference to the personal information to be collected in a regulation made under the statute, i.e., in the form or in the text of the regulation.

Manner of Collection

s.39(1) FIPPA / s.29(1) MFIPPA

This section requires that personal information be collected directly from the individual to whom it relates, unless certain circumstances described in subsections (a) through (h) permit an indirect collection, - that is, from a source other than the individual to whom the information relates.

Individual Authorization

s.39(1)(a) FIPPA / s.29(1)(a) MFIPPA

An individual may authorize an indirect collection of his/her own personal information. Such authorization should generally include:

- the identification of the personal information to be collected;
- the source from which the personal information may be collected; and
- the name of the institution that is to collect the personal information.

A record should be kept with the date and the details of the authorization.

Disclosure Under Section 42 FIPPA / Section 32 MFIPPA

s.39(1)(b) FIPPA / s.29(1)(b) MFIPPA

Personal information may be collected by one institution from another institution where the disclosing institution has authority to disclose under s.42 FIPPA / s.32 MFIPPA.

For example: When a welfare recipient moves to another municipality, the municipality originally providing benefits may disclose certain personal information about the recipient to the second municipality, so that the client's eligibility for welfare may be determined.

The disclosure is authorized by s.32(c) of MFIPPA, as the disclosure to the second municipality is for the same or similar purpose for which the information was originally collected, namely, determining eligibility for welfare benefits. The second municipality, therefore, may collect the information since it has been properly disclosed to it under s.32(c) of MFIPPA.

Authority of the Commissioner

s.39(1)(a), 39(1)(c), 59(c) FIPPA / s.29(1)(a), 29(1)(c), 46(c) MFIPPA

The Commissioner may authorize a collection from a source other than the individual. The Commissioner's authorization may be sought because the indirect collection is not specifically allowed under this section or where the institution believes it is not possible or practical to collect the personal information directly or to obtain authorization directly from the individual concerned.

The Information and Privacy Commissioner has prepared guidelines to assist institutions in making an application for making an indirect collection authority. See Appendix X (Guidelines on applications for authorization of indirect collection).

Consumer Reporting Act

s.39(1)(d) FIPPA / s.29(1)(d) MFIPPA

This subsection authorizes an institution to collect personal information contained in a consumer report that is prepared in accordance with the *Consumer Reporting Act*. A complete list of information which may be included in such a report is contained in s.8(1)(d) of the *Consumer Reporting Act*.

Honour or Award

s.39(1)(e) FIPPA / s.29(1)(e) MFIPPA

This subsection authorizes an institution to collect personal information indirectly for the purpose of determining suitability for an honour or award to recognize outstanding achievement or distinguished service.

For example: Personal information can be collected to determine which of a number of candidates should receive a Citizen of the Year award.

Courts and Tribunals

s.39(1)(f) FIPPA / s.29(1)(f) MFIPPA

This subsection authorizes an institution to collect personal information indirectly for the conduct of a proceeding or a possible proceeding before a court or judicial or quasi-judicial tribunal.

A judicial or quasi-judicial tribunal is a body constituted under a statute with power to decide the legal rights of a person or the eligibility of a person for a benefit or licence. Such tribunals are required to adhere to standards of procedural fairness similar to the procedures of courts.

Examples of this type of tribunal include the Ontario Municipal Board, Property Standards Committee, Assessment Review Court, Social Assistance Review Board, Courts of Revision, and Committees of Adjustment.

In some cases, after personal information has been collected, no proceeding takes place because, for example, there is insufficient evidence. Even though the tribunal may never hear the matter, this subsection applies as long as the purpose of the collection is to determine whether a proceeding can be commenced before a court or tribunal.

Law Enforcement

s.39(1)(g) FIPPA / s.29(1)(g) MFIPPA

Personal information which is collected for the purpose of law enforcement may be collected from a source other than the individual about whom the information relates.

The IPC has found that collection authorized by this subsection must be directly relevant to the law enforcement activity. Only the minimal amount of personal information that is necessary should be collected.

Law enforcement is defined in Chapter 1 (Introduction to the Act) of this manual.

Statutory Authority

s.39(1)(h) FIPPA / s.29(1)(h) MFIPPA

A statute, regulation or by-law may authorize a collection of personal information from a source other than the individual.

For example: Under s.6(4) of the *Municipal Health Services Act*, a municipal assessment commissioner may require any employer to furnish a list of employees residing in the municipality, and the dates upon which the employees are paid their salary or wages.

Subsection 10(1) of the *Assessment Act* authorizes an assessor to indirectly collect specific personal information about an individual from any person "present on land " visited by an assessor under the Act.

Subsection 61(3) of the *Family Responsibility and Support Arrears Enforcement Act* authorized indirect collection of specific types of personal information.

Notification Requirements

s.39(2) FIPPA / s.29(2) MFIPPA

When personal information is collected on behalf of an institution, either directly from the person about whom the information relates or indirectly from another source, the institution must inform the individual that the collection has occurred.

The notice to the individual must state:

- the legal authority for the collection;

- the principal purpose(s) for which the personal information will be used;
- the title, business address and telephone number of an official of the institution who can answer the individual's questions about the collection.

The notice of legal authority should include a reference to the specific act (or regulation) and section, or by-law which authorized the collection. Where an act or by-law does not specifically refer to the collection, then the notice should refer to the specific section of the act or by-law which establishes the activity or program under which the information is collected.

For example: Subsection 58(2) of the *Education Act* provides for the establishment of Boards of Education. Even though the *Education Act* may not specifically authorize each collection of personal information undertaken by a Board of Education, nonetheless s.58(2) of the *Education Act* would provide sufficient statutory authority to undertake collections of personal information that are necessary to the functioning of a board.

The statement regarding the principal purpose(s) for which the information will be used should be consistent with the allowable uses of personal information. The principal purpose(s) for which the information will be used should also be consistent with the statement in the index of personal information banks which describes the use and disclosure of personal information in each bank.

The IPC has found that a notice of collection should contain each of the three elements described in the subsection. Discussion of matters other than collection (e.g., anticipated disclosure of the information) should be included in a separate paragraph from the notice.

Where the personal information is collected directly from the individual, notice should be given to the individual at the time of the collection. Where the personal information is collected on a form, the notice may be provided on the form itself.

A notification should be included on a form where the principal purpose of the form is to collect personal information and the information is used for the purpose of making a decision affecting the individual.

Further, where a variety of personal information data has been collected, the notice of collection must relate to all of the data that has been collected. Where different personal information data on the form is used for different purposes, or is collected under different legal authority, the various purposes and authority must be included in the notice.

For example: Where a particular use of the social insurance number was not indicated in the notice, the notice of collection was found inadequate by the IPC.

Forms which are prescribed by a provincial regulation are not controlled by a municipality or local board. In cases where personal information is collected on a prescribed form, it is the responsibility of the provincial ministry controlling the form to include a notice on the form.

Alternative ways of providing collection notices could include:

- notifying the public through advertisements in the press (e.g., where a public advertisement solicits the collection);
- orally informing the individual in the course of an in-person or telephone interview (and noting this in the individual's file); or
- including the notice in correspondence or as an insert with other mailed material.

Where personal information is collected and will be used by or disclosed to another institution, the individual should be given notice of:

- the legal authority that the first institution has for collecting the information;
- the principal purposes for which the personal information will be used by that institution;
- the address and telephone number of an official in that institution who can answer questions; and
- the fact that the information will be used by a second institution and the name of that institution.

If the individual is not informed at the time of collection that the information will be used by another institution, then the second institution must provide notice to the individual.

Notice must be provided each time personal information is collected. A notice of collection may notify of specific collections occurring in the future when this can be predicted with certainty. Whenever there is ambiguity regarding the sufficiency of the notice, a new notice of collection should be provided. (**Privacy Investigation Report #I95-030P**)

Where indirect collection is permitted under subsection 1, notice to the individual is still required.

Exception to Notice Requirements

Minister's Waiver

s.39(2) FIPPA / s.29(3)(b) MFIPPA

The requirement to provide a notice of collection may be waived by the Minister responsible for FIPPA/MFIPPA. Each request for waiver is considered on its merits. Waivers will normally be requested for a class or group of individuals rather than one individual.

For example: The Chair of Management Board has granted waivers of notice under s.29(3)(b) MFIPPA in respect of indirect collection of personal information on Alzheimer patients for the creation of Wandering Patient Registries by various Police Services in the province.

Some of the criteria for consideration in determining whether to grant a waiver of notice are as follows:

- *Notice Frustrates Purpose of Indirect Collection:* In some cases, to give notice to the individual where information is collected indirectly for certain programs, or of investigations which do not qualify as law enforcement, would undermine the objectives or frustrate the purpose of those programs and investigations. The circumstances which necessitate indirect collection may be considered in determining whether a waiver will be granted.
- *Statutory Authority for Indirect Collection:* Where there is statutory authority for indirect collection, the circumstances that make indirect collection necessary may be considered in determining whether the notice requirements will be waived.
- *Administrative Burden and Cost:* A heavy administrative burden coupled with high costs may justify a waiver in certain circumstances. The administrative burden and the costs would be excessive when weighed against the requirement or need for notice in the particular case. An alternative, however, such as posting a notice or publishing a notice in the newspaper, might be appropriate in these circumstances.
- *Impossibility/Difficulty:* There can be circumstances where it is impossible or very difficult to provide notice. Those circumstances may be considered in determining whether the notice requirements will be waived.
- *Authorization of Information an Privacy Commissioner:* Where the Commissioner has authorized collection of personal information other than directly from the individual, the circumstances which the Commissioner considered in authorizing indirect collection may be considered in determining whether a waiver of notice will be granted.
- *Subsequent Collection by Another Institution:* Where personal information is collected and will be disclosed to another institution in accordance with s.42 FIPPA/ s.32 MFIPPA, the individual is to be given the required notice by the first institution and a statement the information will be disclosed to the second institution. No waiver is required in these circumstances since the first institution has complied with s.39(2) FIPPA/ s.29(2) MFIPPA for both institutions.

Where the first institution does not advise the individual of the disclosure to the second institution, notice will usually be required. There may, however, be circumstances where to provide notice would be inconsistent with the disclosure in s.42 FIPPA/ s.32 MFIPPA. In such circumstances, waiver may be appropriate.

Therefore, when a institution obtains the information, and the individual was already notified in respect to the first collection, it may be appropriate to waive further notification requirements.

This list is not exhaustive and other criteria may be considered in determining whether a waiver of notice will be granted. To request a waiver of notification, complete the Request for Waiver of Notice the Individual of Collection of Personal Information (see Appendix IX).

Further information on the procedure can be obtained from the Corporate Freedom of Access and Privacy Office, Ministry of Government Services.

Other Exceptions to Notice

s.39(3) FIPPA / s.29(3) MFIPPA

Notice of collection of personal information is not required if:

- the type of information being collected would be exempt from access under s.14(1) or 14(2) FIPPA / s.8(1) or 8(2) MFIPPA (law enforcement);
- the Minister (Chair of the Management Board of Cabinet) waives the notice. Each request for a waiver is considered on its own merits. Waivers will normally be requested for a class or group of individuals rather than one individual; or
- the regulations provide that the notice is not required.

For MFIPPA institutions, O.Reg.823 s.4 outlines circumstances where notice of collection is not required. The following circumstances apply only to institutions governed by MFIPPA:

- *Notice Frustrates Purpose of the Collection:* Providing notice to the individual when personal information is collected may undermine the purpose for which the personal information is collected. An institution might collect personal information to determine the whereabouts of someone who is indebted to the institution and who has absconded to avoid paying the debt. In such circumstances, providing notice would frustrate the purpose of collecting the personal information, since notifying the debtor could result in the debtor taking further steps to avoid payment.
- *Unjustified Invasion of Another Individual's Personal Privacy:* Under the Act a notice of collection of personal information must describe how the information will be used. When the use touches upon sensitive personal matters involving another person, the notice may reveal personal information about another individual.

For example: An individual who applies for social assistance benefits from a municipality may be required to furnish the names and routine biographical details of the applicant's dependents or co-habitators. Providing notice to the dependents or co-habitator that personal information about them has been collected for the purpose of assessing the applicant's application would reveal sensitive personal information, namely that the individual has applied for assistance.

- *Suitability or Eligibility for Award or Honour:* An institution may collect the names and biographical details of persons who are being considered for an award or honour. Where personal information is collected for this purpose, a notice of collection is not required.

The head of the institution must make available to the public, a statement describing the purpose of the collection of personal information and the reason that notice has not been given. The statement should:

- identify the program or activity for which the personal information is collected;
- describe in general terms the type of personal information collected, and how the information will be used;
- state the time period during which the notice would not be given, for example, whether the notice is being dispensed with for a one-time only collection or for collections occurring regularly over an indefinite time period;
- explain under which of the circumstances provided for by the regulations the notice has been dispensed with; and

- advise that any concerns regarding the dispensing of notice may be brought to the attention of the IPC.

The public statement should not disclose any personal information about an identifiable individual.

Retention of Records

s.40(1) FIPPA / s.30(1) MFIPPA

The Act includes the power to make regulations relating to the retention period for personal information.

The regulations prescribe a minimum one year retention period for personal information following the last date of use of the information. This is a minimum period, and other operational or legal considerations may require a longer retention period.

The purpose of the minimum retention period is to ensure that the individual to whom the information relates has a reasonable opportunity to obtain access to the personal information (s.40(1) FIPPA / s.30(1) MFIPPA).

When information is updated the outdated information must be retained in some form so that the it is available for the prescribed retention period of one year. The back up documentation does not necessarily need to be stored in the same location as the current information.

Provincial institutions

The Management Board Directive on Recorded Information Management provides ministries and certain agencies with policies and procedures for scheduling the retention and disposal of records.

Local Institutions

The one year minimum retention period can be shortened in two circumstances: first, where the individual to whom the information relates consents to an earlier disposal, the records need not be kept for one year. Individuals, however, cannot compel the destruction of records. Second, where a by-law or resolution stipulates a retention period for the personal information, shorter than the statutory one year period.

This is a minimum retention period, and other operational and legal considerations may require a longer retention period.

Accuracy of Records

s.40(2) FIPPA / s.30(2) MFIPPA

Subsection 40(2) FIPPA / s.30(2) MFIPPA requires that reasonable steps be taken to ensure that personal information is not used unless it is accurate and up to date.

Reasonable steps include checking for accuracy, including errors or omissions, at the time the personal information is collected. Any verification of information should be documented. Although personal information may be accurate and up-to-date when collected, it may become outdated and, therefore, inaccurate. Before personal information is used, the following questions may be useful in assessing its accuracy:

- When was the information collected?
- Was the information collected directly from the individual to whom it relates?
- Was the accuracy of the information verified at the time it was collected? (e.g., Was a birth certificate viewed to verify age?)
- Is the proposed use of the information consistent with the purpose for which it was collected? Information collected for one purpose may be misleading when used for a different purpose.
- How relevant is the personal information to the current use? (e.g., If the information is used to determine eligibility for benefits based on age, the date of birth may be the most relevant piece of information.)
- Is the information likely to be outdated?

Exception to Accuracy Requirement

s.40(3) FIPPA / s.30(4) MFIPPA

These subsections do not apply to information collected for law enforcement purposes.

Disposal of Records

s.40(4) FIPPA / s.30(4) MFIPPA

For FIPPA institutions, O.Reg.459 governs the disposal of personal information. There is no comparable regulation for MFIPPA institutions.

Regulation 459 establishes certain requirements that must be followed by provincial institutions when disposing of personal information.

These requirements can be summarized as follows:

- *Transfer to the Archives of Ontario or destruction:* An institution may dispose of personal information only by (1) transferring it to the Archives of Ontario or (2) by destroying it in such a manner that the information cannot be reconstructed or retrieved.

Records from ministries and certain agencies are transferred to the Archives of Ontario for permanent retention if the Archivist determines that the records have long-term, historical value. Where these records contain personal information, the head disposes of the personal information by transferring it to the custody of the Archives of Ontario.

Where the personal information does not have archival value, or where the personal information is in the custody or control of an institution which does not transfer records to the Archives of Ontario, the personal information is disposed of by destruction.

Transferring personal information to an internal archives other than the Archives of Ontario is not a "disposal" for the purposes of the regulation.

Personal information that is disposed of by destruction should be destroyed in such a way that it cannot be reconstructed or retrieved. Paper and other hard copy records such as microfiche for instance, should be burned, pulped, or shredded rather than discarded or disposed of as garbage.

Personal information on magnetic media such as tape or disk should be disposed of by magnetic erasure or by destruction of the medium, when the medium is released from the processing environment. Where the medium is retained and re-used within a secure processing environment, however, personal information may be disposed of by writing-over during re-use.

- *Authorization of head:* Where personal information is in the custody or under the control of an institution, no person shall destroy it without the authorization of the head. The head may delegate this responsibility.
The authorization may apply to specific data or to general classes or categories of records, and must be consistent with any retention or other management requirement which may apply to the record of personal information through legislation or policy.
- *Protecting security and confidentiality:* The head shall ensure that all reasonable steps are taken to protect the security and confidentiality of personal information that is to be disposed of, including protecting its security and confidentiality during its storage, transportation, handling and destruction or transfer to the Archives of Ontario. In determining whether all reasonable steps are taken, the head shall consider the nature of the personal information to be disposed of.
- Measures which may be considered include:
 - - ensuring that personal information is not left unattended or outside of secure areas during interim storage;
 - ensuring that storage rooms are locked and secure, with controlled distribution of keys or lock combinations;
 - ensuring that access to information during temporary storage is limited to authorized personnel and that such access is documented;

- labelling record storage containers in such a manner that the nature of the contents is not revealed;
- requiring outside suppliers of transportation and disposal services to be bonded, with security provision included in the service contract.

The nature of these measures should be consistent with the sensitivity of the personal information involved. In all cases, however, the minimum requirement is that the confidentiality of the personal information be maintained during disposal.

- *Record of disposal:* Each institution shall maintain a disposal record setting out what personal information has been destroyed or transferred to the Archives of Ontario and the date of that destruction or transfer. This disposal record must not contain personal information.

The record of disposal would describe the "class" of record involved (e.g., "Licence Application Forms", "ABC Program Closed Case Files") rather than containing information about an identifiable individual, and would include the date or date range of the records, and the disposal date. The authority for the disposal and the means of the disposal may also be included.

Where the disposal is undertaken by an outside supplier, the institution may require the supplier to provide a "certification of destruction" signed by an officer of the company. This certificate would then be linked to the disposal record maintained by the institution.

Use of Personal Information

s.41 FIPPA / s.31 MFIPPA

This section establishes general rules governing the use of personal information in the custody or under the control of institutions. It recognizes that an individual's right to privacy includes the right to know how his/her personal information is being used. Personal information may be used within the institution where any one of the following circumstances exists.

Individual Consent

s.41(a) FIPPA / s.31(a) MFIPPA

An institution may use personal information where the individual to whom the information relates has consented to the use proposed by the institution.

This consent should be in writing and indicate:

- the particular personal information to be used;
- the use for which consent is given;
- the date of the consent; and
- the institution to which consent is given.

Consent of the individual is required where none of the other circumstances described below exists.

Purpose for Which Information Collected

s.41(b) FIPPA / s.31(b) MFIPPA

The institution may use personal information for the purpose for which the information was originally obtained or compiled, or for a consistent purpose.

Usually, an institution may use personal information under its custody or control for the purposes indicated in the collection notice and in the personal information bank descriptions it provides in its directory of records.

The institution may also use personal information for a purpose which is consistent with the purpose(s) listed in the collection notice. For an explanation of a consistent purpose, see the discussion of s.43 FIPPA / s.33 MFIPPA later in this chapter.

For the Purpose Disclosed

s.41(c) FIPPA / s.31(c) MFIPPA

An institution may have personal information disclosed to it by another institution under s.42 FIPPA / s.32 MFIPPA. The receiving institution may use this personal information only for the purpose for which it was disclosed by the first institution.

For example: If personal information is disclosed from one institution to another in compassionate circumstances to assist in locating a family member, that information is to be used by the receiving institution only to locate the family member and for no other purpose.

Disclosure of Personal Information

s.42 FIPPA / s.32 MFIPPA

Institutions covered by FIPPA/ MFIPPA have rules governing the two separate sets of circumstances under which personal information may be disclosed to another party:

- Part II/I. The first set of rules appear under s.21 FIPPA / s.14 MFIPPA. These mandatory rules apply whenever anyone makes an access request for another's personal information. Detailed discussion of these rules can be found in the Chapter 4 (Exemptions).
- Part III/II. The second set of rules appear under s.42 FIPPA / s.32 MFIPPA. These rules govern an institution's disclosure of personal information during the conduct of its day-

to-day activities. An institution may disclose personal information in the absence of a formal access request if the disclosure is permitted under part III/II.

Disclosure in Accordance with Part II/I

s.42(a) FIPPA / s.32(a) MFIPPA

Subsection 42(a) FIPPA / s.32(a) MFIPPA permits an institution to disclose personal information in circumstances where such disclosure would have been permitted under s.21 FIPPA / s.14 MFIPPA, even though the institution has not received an access request. This subsection should be read in conjunction with s.63(1) FIPPA /s.50(1) MFIPPA which permits a head to disclose information even though an access request has not been received.

Consent to Disclosure

s.42(b) FIPPA / s.32(b) MFIPPA

Personal information may be disclosed where the individual has consented to the disclosure. Where consent to disclose personal information has been given by an individual, the specific information for which consent has been given must be identified.

Where this consent is not obtained in writing it should be documented and should indicate:

- the particular personal information to be disclosed;
- to whom the information may be disclosed and for what purpose it is to be used; and
- the date of the consent; and the institution to which consent is given.

Where an individual purports to act as an agent, the institution has an obligation under s.3(3) of Regulation 460 FIPPA / s.2(3) Regulation 823 MFIPPA to verify the identity of an individual seeking access to his/her personal information and whether or not the agent is properly authorized to obtain such information. If proper authorization cannot be obtained, the institution may either notify the individual whose personal information is at issue and provide him/her with an opportunity to provide representations prior to any decision regarding disclosure of the records or may deal with the validity of the authorizations as a preliminary matter. The following factors are relevant for the institution in determining reasonably whether to refuse or accept certain authorizations:

- whether the personal information is very sensitive,
- whether the authorizations preclude the institution from verifying the consent, and
- whether or not the individuals who have allegedly consented have responded to the request for verification made by the institution.

Special care should be taken where personal information is being requested about the treatment of vulnerable individuals. Institutions should not assume that requests for personal information

by agents are invalid; rather, they should discuss the matter with the individuals involved before determining whether or not to accept the authorizations.

Consistent Purpose

s.42(c), 43 FIPPA / s.32(c), 33 MFIPPA

Personal information may be disclosed for the purpose(s) for which it was originally collected, or for a consistent purpose. A purpose is a consistent purpose only if the individual from whom the information was directly collected might reasonably have expected such a disclosure of the information.

For example: A public utility commission may disclose personal information to a debt collection agency to recover monies owed to the commission for utility bills in arrears. Such disclosures would reasonably be expected by persons who have not discharged their debts to the commission.

The IPC has found that where personal information has been collected indirectly, a consistent purpose is one in which the use or disclosure is "reasonably compatible" with the purpose for which it was collected.

An institution may also disclose personal information for a purpose which is consistent with the purpose(s) listed in the collection notice.

For example: Disclosure of personal information such as payments received, social insurance number, date of birth and address regarding an application for a government loan to credit reporting agencies was in compliance with this provision. This personal information was disclosed for the purposes of updating or making the necessary credit investigations or credit reporting as stated in the notice of collection of personal information.

Where an administrative or policy manual provided guidelines for the subsequent use or disclosure of personal information by an institution, disclosure in accordance with the guidelines was found to have been for a consistent purpose.

In Performance of Duties

s.42(d) FIPPA / s.32(d) MFIPPA

Personal information may be disclosed to an employee or officer of the institution who needs the record in the performance of his/her duties, and where disclosure is necessary and proper in the discharge of the institution's functions.

Before an officer or employee of an institution is granted access to personal information under this provision, both of the following conditions must be satisfied:

- the employee or officer must need the personal information for the performance of his/her duties; and
- disclosure of the personal information must be necessary and proper in discharging the institution's functions.

For example: A municipal council resolution that authorized the disclosure of a list of welfare recipients from the Welfare Administrator to the council to address the councillors' "previously expressed interest and concern" regarding social assistance expenditures was insufficient to satisfy the requirements of this subsection. This provision required that the sharing of personal information within an institution be based on more than an interest or concern; it required evidence that the disclosure was needed and necessary. Since it failed to comply with this provision, the council's resolution was illegal and need not be obeyed. (**H.(J) v. Hastings (County)**, (1993) 12 M.P.L.R. (2d) 40 (Ont.Ct.Gen. Div.))

Disclosures that are merely convenient or desirable are not allowed under this section.

It is important to note that the identity of an access requester should not be disclosed within an institution unless such disclosure is necessary in order to respond to the request. Further, names and addresses of individuals who have made requests for general records under the Act should not be communicated within an institution other than to staff of the Freedom of Information and Privacy office.

An institution's functions would include the administration of by-laws, statutory programs, and activities necessary to the overall operation of the institution.

Act of Legislature or Parliament

s.42(e) FIPPA / s.32(e) MFIPPA

This subsection permits disclosure of personal information for the purpose of complying with an act of the Legislature or of Parliament, or an agreement or arrangement thereunder, or a treaty. The agreement or arrangement must result from or be sanctioned by a federal or Ontario statute. Disclosure of personal information for the purposes of complying with a regulation or a by-law would be included.

For example: Section 14 of the *Immunization of School Pupils Act* requires a medical officer of health to transfer a child's immunization records to another medical officer of health when that child moves to a school under the jurisdiction of the latter health unit.

Subsection 72(3) of the *Child and Family Services Act* requires a person (for example, a school teacher or principal, social worker, family counsellor) to report suspicions of child abuse and to report the information on which the suspicion is based.

Subsection 199(3) of the *Highway Traffic Act* requires a police officer to forward accident reports to the Ministry of Transportation.

The *Ombudsman Act* provides authority for the disclosure of personal information to the Office of the Ombudsman from governmental institutions in accordance with this provision.

Disclosure to Law Enforcement Agency

s.42(f) FIPPA / s.32(f) MFIPPA

A law enforcement institution may disclose personal information to a law enforcement agency in Canada, or to a law enforcement agency in a foreign country under an arrangement, a written agreement or treaty, or under legislative authority.

Under this section, disclosure may only be made by a "law enforcement institution". An institution engaged in "law enforcement" is discussed in the Definitions section in Chapter 1 (Introduction to the Act).

For example: The Ministry of the Solicitor General and Correctional Services is a law enforcement institution which is engaged through the Ontario Provincial Police and other programs. It is also responsible for the enforcement of probation and parole orders, another law enforcement activity. The Ministry of Community and Social Services and the Ministry of Consumer and Commercial Relations are also institutions engaged in law enforcement through their departments which are responsible for compliance with statutes. Similarly, municipalities are law enforcement institutions through their enforcement of by-laws.

Disclosure may only be made to a law enforcement agency. A "law enforcement agency" includes a national, state, or local police force, or a municipal or provincial police force in Canada, the RCMP and some special police forces.

For example: The IPC has determined that the Canadian National Railways (CNR) police is a "law enforcement agency" for the purpose of this section. The Ontario Provincial Police were authorized to disclose to CNR police personal information concerning a criminal offence that had been laid against a CNR employee.

In exchanges of personal information with foreign countries, written agreements or treaties should be established. Where this is not possible or practical, an arrangement may be made. An "arrangement" is an unwritten agreement for the exchange of personal information.

When a law enforcement institution discloses personal information to a police agency or other law enforcement agencies in Canada, an agreement or arrangement is not required. It is understood that the purpose of the disclosure is law enforcement.

Aid in Law Enforcement

s.42(g) FIPPA / s.32(g) MFIPPA

An institution may disclose personal information to another institution covered by FIPPA/MFIPPA or to a law enforcement agency in Canada to aid an investigation leading or likely to lead to a law enforcement proceeding. For this section to apply, the disclosure must be in aid of the investigation undertaken.

For example: Disclosure of personal information to an eligibility review officer is for a law enforcement purpose if it is to aid in an investigation into social services benefits eligibility where a person has received benefits. Such an investigation could lead to sanctions such as an assessment of overpayment or withholding of benefits.

Although this subsection permits an institution to release personal information, the institution may choose to require a search warrant before access to personal information is granted.

For example: The *Education Act* states that the Ontario Student Record is privileged for the information and use of supervisory officers and the principal and teachers of the school. A school may require a police agency to provide a search warrant before disclosing such a record.

Compelling Circumstances

s.42(h) FIPPA / s.32(h) MFIPPA

An institution may disclose personal information in compelling circumstances affecting the health or safety of an individual. In compelling circumstances, there may be no other way to obtain the personal information, or there may be an emergency where the delay in obtaining the information would be injurious to someone's health or safety. Before personal information is released under this subsection, both of the following conditions must be satisfied:

- the circumstances in which the release of personal information is contemplated must be compelling; and
- the compelling circumstances must affect the health or safety of an individual.

For example: A mentally unstable social services benefits client convinces his case worker that he is going to kill his roommate.

Where personal information is disclosed under this subsection, notification of the disclosure must be mailed to the last known address of the individual to whom the information relates. This means the most recent address known to the institution which disclosed the personal information. If no address is known, the institution should attempt to obtain it from the person who made the request for the information.

Compassionate Circumstances

s.42(i) FIPPA / s.32(i) MFIPPA

An institution may disclose personal information in compassionate circumstances to facilitate contact with the next-of-kin, or a friend of an individual who is injured, ill or deceased.

"Compassionate circumstances" are those where there is a need to make contact with a friend or next-of-kin to inform them of an individual's injury, illness, or death. The personal information to be disclosed may relate either to the injured or deceased person, or to the relative or friend who is to be contacted.

Only the personal information necessary to facilitate contact should be disclosed.

This provision is not relevant in deciding whether personal information may be disclosed as a result of an access request.

To a Member of the Legislature

s.42(j) FIPPA

Disclosure is permitted to a member of the Legislative Assembly (MLA) who has been authorized by a constituent to whom the information relates to make an enquiry on his/her behalf. Where the constituent is incapacitated, the member may be authorized by the next of kin or legal representative of the constituent.

This subsection applies to situations in which the assistance of a MLA is sought in resolving a problem, and the individual or his/her representative has consented to the disclosure of personal information to the member in the course of his/her enquiry.

Whether the member is making a written or oral inquiry, the member must indicate that he/she is acting with the constituent's authority. This disclosure will be recorded in or linked to the individual/s record. Where the personal information is particularly sensitive (e.g., medical records), the institution may have additional consent requirements specific to the situation, such as written authorization.

To a Member of the Bargaining Agent

s.42(k) FIPPA

Disclosure is permitted to a member of the bargaining agent who has been authorized by an employee to whom the information relates to make an enquiry on the employee's behalf. Where the employee is incapacitated, the bargaining agent may be authorized by the next of kin or legal representative of the employee.

As in s.42(j), reasonable steps should be taken to ensure the authority exists.

Disclosure to Responsible Minister

s.42(l) FIPPA / s.32(j) MFIPPA

Personal information may be disclosed to the Chair of Management Board of Cabinet as minister responsible for the Act.

For example: A request for waiver of notification of personal information may require the disclosure of personal information to the Minister.

Disclosure to Information and Privacy Commissioner

s.42(m) FIPPA / s.32(k) MFIPPA

Personal information may be disclosed to the IPC. This subsection is intended to facilitate the IPC's access to records in order to carry out its decision making and investigation responsibilities. Under s.52(4) FIPPA / s.41(4) MFIPPA, the Commissioner has the authority to examine any record in the custody or control of an institution during the course of an inquiry regarding an appeal of an access decision made by an institution.

Government of Canada or Government of Ontario

s.42(n) FIPPA / s.32(l) MFIPPA

Disclosure of personal information is permitted to the Government of Canada or to the Government of Ontario in order to facilitate the auditing of shared-cost programs.

For example: Personal information contained in general welfare case files established under the *General Welfare Assistance Act* may be audited by the Province of Ontario.

Consistent Purpose

s.43 FIPPA / s.33 MFIPPA

This section provides that when personal information is collected directly from the individual to whom it relates, the purpose of its use/disclosure is a consistent purpose only if the individual might reasonably have expected such a use/disclosure.

Subsection 41(b) FIPPA / s.31(b) MFIPPA permits the use of personal information for the purpose for which it was obtained or for a consistent purpose.

Section 42(c) FIPPA / s.32(c) MFIPPA permits disclosure of personal information for the purpose for which it was collected or for a consistent purpose.

A consistent purpose must be compatible with the purpose stated to the individual at the time the information was collected. The individual could therefore reasonably expect this use/disclosure

of his/her personal information.

Where personal is collected other than directly from the individual, the question of whether use/disclosure is for a consistent purpose is not determined by considering the individual's reasonable expectations. It is determined by considering whether the institution's proposed use/disclosure of information is reasonably compatible with the purpose for which it was collected.

New Use/Disclosure of Personal Information

s.46(1)(a)and(b) FIPPA / s.35(1)(a)and(b) MFIPPA

The personal information banks maintained by institutions include a statement of the regular uses of the personal information and the regular users to whom the information is disclosed.

There may be instances where the institution uses or discloses personal information for a purpose allowed by the Act, but where that use/purpose has not been listed in the personal information bank descriptions. Where such a new use or disclosure has occurred, the institution is required to:

- make a record of that new use or disclosure; and
- attach or link the record of use/disclosure to the personal information, so that when the personal information is accessed, the record of use/disclosure is accessed as well. In other words, the record of the new use/disclosure of the personal information becomes part of the personal information itself (s.46(2) FIPPA/ s.35(2) MFIPPA).

If the new use or disclosure becomes a regular occurrence, the institution should update its personal information bank description to include the new regular use/disclosure. Once the description has been updated, s.46 FIPPA/ s.35 MFIPPA ceases to apply.

The requirement to create and attach a record of use/disclosure only applies to personal information which is part of a personal information bank. It does not apply to personal information contained within a general record.

Role of Information and Privacy Commissioner

s.59 FIPPA / s.46 MFIPPA

This section establishes the powers of the Commissioner relating to the protection of personal privacy.

Subsection (a) of FIPPA/ MFIPPA permits the Commissioner to offer comment on the privacy protection implications of proposed programs of institutions.

Subsection (b) enables the Commissioner to, after hearing representations from a head, order an institution to cease a collection practice and to destroy collections of personal information that contravene this Act.

Subsection (c) empowers the Commissioner to authorize the collection of personal information otherwise than directly from the individual to whom the information relates. (See the discussion under s.39(1)(c) FIPPA / s.29(1)(c) MFIPPA).

Subsections (d), (e) and (f) respectively permit the Commissioner to engage in research into matters affecting the carrying out of the purposes of the Act, conduct public education programs about the Act and the Commissioner's role and activities and to receive representations from the public concerning the operation of this Act.

Chapter 6: Fees

Table of Contents

- Introduction
 - Types of Costs
 - Taxes
 - Mandatory Application Fee
 - Fees for a Personal Information Request
 - Fees for a General Records Request
 - Costs for Photocopying and Computer Printouts
 - Search Time
 - Record Preparation Charges
 - Computer Costs
 - Costs for Services Outside the Institution
 - Shipping Costs
 - Additional Fees
 - Fee Estimates and Deposits
 - Under \$25.00
 - \$25.00 up to \$100.00
 - \$100.00 or More
 - Other Important Considerations
 - Waiving Fees
 - Appeal Fees
-

Introduction

s.24, 48, 50, 57, 60 FIPPA / s.17, 37, 39, 45, 47 MFIPPA

s.5, 5.2, 5.3, 6, 6.1, 7, 8, 9, O.Reg.460 /s.5, 5.2, 5.3, 6, 6.1, 7, 8, 9, O.Reg.823

The Freedom of Information and Protection of Privacy Act (FIPPA) / Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) adopt a user pay principal.

Under s.57(1) FIPPA / s.45(1) MFIPPA, a person making an access request must pay some of the costs the institution incurs processing the request. The fee schedule is contained in the regulations. Differences in the fees apply depending on whether the request is for general records or the requester's own personal information. The fees must be charged unless they are waived by the institution, or unless a provision is made for charging fees under another statute. The *Municipal Act* does not give local institutions the power to set new fees for records that would

normally be available through MFIPPA. The following are examples where fees can be charged for records that are available to the public without having to make an access request under the FIPPA/MFIPPA.

For example: Under the *Municipal Act*, the council can pass a by-law to set fees for copies of records, books and documents requested from the clerk's office. Those fees would take precedence over the fee provisions in MFIPPA.

Under the *Public Libraries Act* a library board can charge fees for, among other things, services other than for admission, use of library materials and reference and information services.

Under the *Highway Traffic Act*, the Ministry of Transportation sets the fee for driver abstracts.

Types of Costs

Taxes

The Goods and Services Tax and *The Provincial Sales Tax* are not applicable to fees charged under FIPPA/MFIPPA.

Mandatory Application Fee

A \$5.00 mandatory application fee must accompany a request for either personal information or general records under FIPPA/MFIPPA.

Once the application fee is received, s.26 FIPPA / s.19 MFIPPA requires a head to provide a requester with access to records and/or a decision letter within 30 days. This requirement does not apply if the mandatory application fee has not been received by the institution. However, the onus is on the institution to collect this application fee before processing the request if it decides to proceed. Failure to collect the fee application will not prevent the Information and Privacy Commission (IPC) from hearing an appeal about a request that has been completed.

Fees for Personal Information Requests

A request for personal information is a request made by an individual (or another person acting on his/her behalf) for the individual's own information.

For example: If a lawyer has a client's written consent, his/her request for the client's personal information is a personal information request. Likewise, custodial parents' requests for the

personal information of their young children (i.e. children under the age of 16) are personal information requests.

No fees are charged for search or preparation time, but there are fees for photocopying (\$0.20 per page) and computer costs as specified in the regulations.

Fees for General Records Requests

All costs incurred that are specified in the regulations may be charged. These costs which are described below, are calculated from the time a request is received.

Costs for Photocopying, Computer Printouts and Computer Disks

An institution can charge \$0.20 per page for photocopies and computer printouts regardless of whether the request is for personal or general information. This per page charge includes the cost of staff time to feed documents into a photocopy machine. An institution can also charge a fee of \$10.00 for floppy disks.

Search Time

A charge can be made for the amount of time required to search for the records. This includes personnel time involved in searching for the records, examining file indices, file plans or listings of records, either on paper or in a computer.

An institution can charge \$7.50 for each 15 minutes spent by any person in the institution searching for the record. If more than one person is conducting the search, each person's time can be charged.

Search time does not include:

- time spent photocopying the records
- the time it takes an employee to walk from one area in the institution to another to locate responsive records
- the time to drive to an off-site storage to retrieve records (unless costs are invoiced by an outside firm).

Search time includes:

- examining ledger-sized binders of computer sheets to determine whether particular sheets are responsive.

Record Preparation Charges

Personnel time involved in physically preparing the record for disclosure can be charged.

This includes the time involved in severing exempt information prior to disclosure. Severing a record includes physical handling, for instance, putting removable tape over exempt portions of the record before it is photocopied. An institution can charge \$7.50 for each 15 minutes spent by an person for preparing a record for disclosure.

An institution cannot charge personnel time involved in reviewing the records to determine if an exemption applies.

Note: Preparation time does not include the time taken to actually photocopy a record. Twenty cents per page is the maximum amount that may be charged for photocopying and this includes the cost of an individual 'feeding the machine.' In addition, preparation in this section should be read narrowly and it should not include removing staples and paperclips, copying the relevant pages and putting them back to the books where they originated. However, where special preparation is necessary, such as where maps have to be taped together or where records have to be removed from cerlox bound volumes, fees for preparation may be appropriate. (See for example: **Orders #M-301, P-490, P-608, M-360, M-372**)

Computer Costs

An institution can charge \$15.00 for each 15 minutes spent by any person developing a computer program or other method of producing a record from machine readable record.

In some instances producing a record from a machine readable record will require the manipulation of information stored in a computer database. It may be necessary to write a computer program so that the particular information requested can be retrieved.

Costs for Services Outside the Institution

An institution may require outside services to assist in locating, retrieving, processing or copying paper or electronic records.

The costs of these services can be passed on to the requester if two conditions are met:

- the institution receives an invoice for the cost of outside services
- the costs cover services that could not have been provided by the institution's staff.

For example: A request might be for a copy of a record in a format other than a photocopy, computer printout or a computer disc. If an institution does not have the capability to do specialized copies, such as microfilm or fiche, the institution can send the material to outside facilities for copying and invoice the requester.

The costs, even if invoiced, cannot be charged if they would not have been incurred had the request been processed by the institution's staff. (Order #P-1536)

Shipping Costs

Shipping charges incurred by the institution, such as postage or courier costs, can be charged.

Additional Fees

Regulations can be created to allow charging of additional fees.

Fee Estimates and Deposits

See Chapter 3 (Access Procedures) for the procedure for calculating fee estimates.

Under \$25.00

s.57 FIPPA / s.45 MFIPPA

If it costs less than \$25.00 to process a request, it is not necessary to give the requester a fee estimate. Rather, the requester can be informed of the amount to be paid in the decision letter.

\$25.00 up to \$100.00

s.57(3) FIPPA / s.45(3) MFIPPA

The institution shall, before giving access to a record, give the requester a reasonable estimate of any amount that will be required to be paid. If that amount is over \$25.00 and under \$100.00, the institution is not required to collect a 50% deposit.

\$100.00 or more

s.7 O.Reg.460 / s.7 O.Reg.823

A fee estimate must be given if costs will equal \$100.00 or more. An institution may require a deposit of 50% of the estimated fee. Once a fee deposit is requested, an institution is not required to take any further steps to respond to the request until the deposit is paid.

An institution is not required to release records to a requester until the fee has been paid, or the issue of fees has been resolved after an appeal to the IPC.

Other Important Considerations

A fee should be "fair and equitable".

The Commissioner has ruled that in order to determine whether a fee estimate is fair and equitable the following factors are relevant: 1. the manner in which the institution attempted to respond to the appellant's request; 2. whether the institution worked with the appellant to narrow and/or clarify the request; 3. whether the institution provided any documentation to the appellant free of charge; 4. whether the appellant worked constructively with the institution to narrow the scope of the request; 5. whether the request involves a large number of records; 6. whether or not the appellant has advanced a compromise solution which would reduce costs, and 7. whether the waiver of the fee would shift an unreasonable burden of the cost from the appellant to the institution, such that there would be significant interference with the operations of the institution. (See for example: **Orders #P-741, M-408, M-417**)

Where an institution is providing a specific fee for "reproduction, " it must substantiate that fee. If it is for copies, then the institution must indicate the number of estimated pages, or the rate at which the fee is calculated. Sufficient facts and evidence must be provided to enable the requester to review the costs. (See for example: **Orders #M-103, M-163**)

Waiving Fees

It is the requester's responsibility to ask the institution for a fee waiver. However, a request for a waiver need not be explicit, it may be implied. The party seeking a fee waiver also bears the responsibility of establishing his/her case.

For example: If the requester does not supply sufficient information to convince the institution that a fee waiver is justified, the institution is not required to grant the waiver. What an institution considers sufficient information will likely be influenced by the specific facts of the request.

A head shall waive all or part of the fees if in the head's opinion it is fair and equitable to do so after considering:

- the extent to which the actual cost of processing, collecting and copying the record varies from the amount of payment required by the section;
- whether the payment will cause a financial hardship to the person requesting the record;
- whether dissemination of the record will benefit public health or safety;
- whether the person requesting access to the record is given access to it; and
- if the amount of a payment would be \$5.00 or less, whether the amount of the payment is too small to justify requiring payment.

A head's decision not to waive a fee may be appealed to the IPC.

Note: the application fee cannot be waived.

Appeal Fees

There are mandatory fees for a requester appealing decisions to the IPC. A \$10.00 fee applies to personal information request appeals and a \$25.00 fee applies for general records request appeals. No fee is required for a third party to appeal an institution's decision to disclose information.

Chapter 7: Appeals and Compliance

Table of Contents

- Introduction
- The Information and Privacy Commissioner (Commissioner)
 - The Appointment of the Commissioner
 - The Powers of the Commissioner to Hear Appeals
 - The Power of the Commissioner to Review the Exercise of Discretion
- The Appeal Process
 - What Can Be Appealed?
 - Who Can Appeal?
 - Notice of Appeal by a Requester
 - Confirmation of Appeal by the Information and Privacy Commissioner
 - How to Provide Records to the Commissioner During an Appeal
 - The Duty to Provide Records to the Information and Privacy Commission (IPC)
 - Mediation
 - The Inquiry
 - Notice of Inquiry and the Appeals Officer's Report
 - Considering Additional Exemptions and Facts During the Inquiry Process
 - The Burden of Proof
 - Written or Oral Submissions
 - Access to an Institution's or Third Party's Submissions by an Appellant
 - Affidavit Evidence
 - The Effect of a Commissioner's Order
 - Reconsideration of a Commissioner's Orders
- Judicial Review
- Compliance Investigations
 - The Privacy Investigation Process
 - Notice and Request for Information
 - The Investigation
 - Draft Report
 - Final Report
 - Follow Up

Introduction

Ontario's Freedom of Information and Protection of Privacy Act (FIPPA) / Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) establishes a right to appeal decisions

about access to records that are made by institutions covered by the Act. Appeals are filed with the Information and Privacy Commissioner.

This chapter outlines the powers of the Commissioner and the appeal process. Many of the procedures have been developed by the IPC and are subject to change. Where clarification is needed during an appeal, an institution should contact the Appeals Officer assigned to the appeal.

The Information and Privacy Commissioner

The Appointment of the Commissioner

s.4 FIPPA

The Commissioner is appointed by the Lieutenant Governor in Council with the approval of the Legislative Assembly. This means that the Commissioner is an officer of the legislature and is independent of the government of the day.

The Commissioner is appointed for a term of five years and may be reappointed for a further term or terms. The Commissioner is removable at any time for cause by the Lieutenant Governor in Council with the approval of the Legislative Assembly.

The Powers of the Commissioner to Hear Appeals

s.54 FIPPA / s.43 MFIPPA

Decisions institutions make in response to access requests may be appealed to the Commissioner. The Commissioner decides matters under appeal by issuing an order. Subject to the Act, the order may contain any conditions the Commissioner considers appropriate. Commissioner's orders are binding on all parties to the appeal. The Commissioner must notify the appellant, the institution and any person given notice of the appeal as an affected person that an order has been issued; this is done by sending a copy of the order to the parties.

The broad order-making power includes that right to order an institution to search its files in the presence of a Commission staff if the original search is deemed by the Commissioner to be inadequate. However, the Commissioner does not have the power to order an institution to create a record, unless a request is for certain machine readable records.

The Commissioner may also issue an interim decision and may defer a decision until further submissions are provided.

It is an offence to willfully fail to comply with an order of the Commissioner (s.61(1)(f) FIPPA / s.48(1)(f) MFIPPA).

The Power of the Commissioner to Review the Exercise of Discretion

Under FIPPA/MFIPPA most of the exemptions that allow a head of an institution to withhold a record are discretionary, which means that a head can choose whether or not to apply the exemption and withhold the record. While s.54(2) FIPPA / s.43(2) MFIPPA states that the Commissioner cannot substitute his/her discretion for that of a head, the Commissioner may review the way the discretion was exercised, to ensure that it was exercised properly.

The Commissioner may examine the record to determine whether a discretionary exemption in fact applies. In its appeal submissions, the institution will be expected to fully explain its reasons for not disclosing a record. If the rationale for a head's decision is not clear, the Commissioner may order a head to reconsider his/her decision to withhold a record and to supply further written submissions.

The IPC has prepared a list of factors which may assist institutions in exercising their discretion. These factors are not meant to be all-inclusive. They are:

- the general purpose of the Act, which is that institutions should make information available to the public and that individuals should have access to personal information about themselves,
- the actual wording of the discretionary exemption and the interests that the exemption attempts to balance,
- the facts and circumstances of each specific case,
- whether the individual's request could be satisfied by severing the record and by providing the requester with as much information as is reasonably practicable,
- whether the past practice of the institution has been to release similar types of records,
- the nature of the record, its importance to the requester and whether the record is particularly sensitive or significant,
- whether disclosure of the information would increase public confidence in the operations of the institution,
- the age of the record,
- the importance of the record to the requester and whether there is a sympathetic or compelling reason to release the record,
- whether previous orders of the Commissioner have ruled that similar types of records or information should or should not be subject to disclosure,
- when the advice to government exemption is claimed, whether the decision to which advice or recommendations pertains has already been made.

The Appeal Process

What Can Be Appealed?

s.50 FIPPA / s.39 MFIPPA

Generally, any decision that a head makes under the Act may be appealed to the Commissioner, including:

- a decision to extend the time limit for responding to a request,
- refusal to grant access to a record on the ground that the record does not exist,
- refusal to grant access to a record on the ground that the record is excluded from the Act,
- refusal to grant access to a record on the ground that the record is exempt,
- granting access to only part of the record,
- granting a request for access to a record or part that may contain third party commercial information or that contains personal information where the disclosure may be an unjustified invasion of personal privacy,
- refusal to confirm or deny the existence of a record that deals with law enforcement or would, if disclosed, be an unjustified invasion of personal privacy,
- a deemed refusal to grant access to records,
- a refusal to make a correction to personal information requested,
- the amount of a fee charged,
- a refusal to waive a fee charged,
- a refusal to allow a requester to examine the original record.

Who Can Appeal?

s.50 FIPPA / s.39 MFIPPA

The following persons can appeal to the Commissioner:

- a person who has made a request for access to a record under s.24(1) FIPPA / s.17(1) MFIPPA,
- a person who has made a request for access to his/her own personal information under s. 48(1) FIPPA / s.37(1) MFIPPA,
- a person who has requested correction of his/her own personal information under s.47(2) FIPPA / s.36(2) MFIPPA,
- an affected third party who has received a notice under s.28(1) FIPPA / s.21(1) MFIPPA that the head intends to disclose a record that may affect the interests of the third party.

Notice of Appeal by a Requester

s.50(2) FIPPA / s.39(2) MFIPPA

A person who has been notified of a decision by an institution has 30 calendar days to appeal the decision to the Commissioner. The Commissioner may nonetheless hear an appeal that is filed

after the 30-day time limit, unless the institution can show that it would be prejudiced by the delay. For example, prejudice may be established where records that are relevant to the appeal have been destroyed.

The appellant (the person who is appealing) begins an appeal by submitting a request for an appeal (notice of appeal) in writing to the Commissioner. Appellants do not have to use a prescribed form and generally do not understand the appeal process. As a result, appeal requests often do not contain enough information for the Commissioner to understand what is being appealed. Institutions should therefore include a paragraph in their decision letters informing a requester or third party that he/she can appeal the decision to the IPC within 30 days, and that their notice of appeal should be accompanied by:

- the file number assigned to the request by the institution;
- a copy of the decision letter; and
- a copy of the original request for information.

If an appellant is appealing a decision by an institution that the requested records do not exist, the Commissioner may dismiss the appeal if the notice of appeal submitted by the appellant does not present a reasonable basis for concluding that the record ought to exist (s.50(2.1) FIPPA / s.39(2.1) MFIPPA).

Upon receiving a notice of appeal, the Commissioner notifies the institution's Freedom of Information and Privacy Coordinator that an appeal has been filed. The Commissioner must also notify any other person who, in the Commissioner's opinion, is "affected" by the appeal.

If an institution has any information about affected persons who should be notified of an appeal, it should convey this information to the Appeals Officer assigned to the case. Because the Commissioner cannot disclose the contents of the records to an affected party, these individuals should contact the institution's Coordinator if they require further information. The Commissioner does not disclose the identity of the appellant to affected parties if the appellant is an individual.

Confirmation of Appeal by the Information and Privacy Commissioner

The IPC notifies an institution that an appeal has been filed by sending out a "Confirmation of Appeal" letter. It advises the institution of the name of the requester, the IPC's appeal number and the name of the Appeals Officer assigned to the case. It also advises the Coordinator to notify the Appeals Officer if the responsive records are voluminous (500 pages or more and 3 exemptions or more).

The Confirmation of Appeal also asks the institution to provide the following information within 8 working days where applicable:

- a copy of the original request and its file number,

- a copy of the head's decision letter,
- any correspondence related to the request or the decision making process,
- an index of the records under appeal and the exemptions applied to the records (the index may be shared with the appellant so care should be taken that no exempt information appears in the index),
- a severed copy of the records under appeal where severances have been made
- unsevered copy of the records.

The institution is further notified that if it wants to claim any discretionary exemptions additional to those appearing in its decision letter, it must do so within 35 days. Where the appeal relates to either a time extension or the payment of a fee, the request for the last two items on the above list will be omitted. Reasons for launching an appeal are not always provided by an appellant. Institutions may find it helpful to contact the Appeals Officer to see whether grounds for appeal have been identified. The IPC may also be able to provide additional information that will help the institution to deal with the appeal promptly and efficiently.

An institution should provide the IPC with the records relevant to an appeal within 8 days of the date of the confirmation notice. The Commissioner may grant a time extension if an institution can demonstrate that it is not feasible to provide the records within two weeks.

How to Provide Records to the Commissioner During an Appeal

The IPC has issued guidelines on appeal procedures. While subject to change, the office requests institutions to do the following:

1. Upon receipt of the Confirmation of Appeal, the institution should provide the IPC with a copy of the original request, any relevant correspondence with the requester, and the records at issue in the appeal.
2. If the records have been severed, the institution should identify the severances on the record itself either by highlighting the severed portions on a copy of the record, or by providing copies of both the severed and unsevered records to the IPC.
3. Where more than one section of the Act is claimed to justify the severance, or where more than one exemption applies to the record, the institution should:
 - (a) number all documents,
 - (b) number all pages within a document,
 - (c) prepare an index of records containing the following information:

- the document number,
- the page number,
- whether or not an exemption has been claimed,
- the section/subsection of the Act justifying the severance,
- the reason for applying the exemption.

When dealing with more complex requests, compiling an index with the following headings should also be considered:

- document number,
- page number/paragraph,
- severance (yes/no),
- record released (yes/no),
- section of the Act applied,
- reasons for severance.

The Duty to Provide Records to the Information and Privacy Commission

s.52 FIPPA / s.41 MFIPPA

If an institution can demonstrate that it is not feasible to provide the records to the IPC within 8 working days, the Commissioner may grant a time extension.

If an institution fails to provide the records within the required period, the Commissioner may issue an order requiring the records to be produced. Failure to provide the records to the Commissioner may result in a prosecution for willful obstruction of the Commissioner (s.61(1)(d) FIPPA / s.48(1)(d) MFIPPA).

The Commissioner may also require that an institution prepare an affidavit describing the measures taken to search for a record if the institution claims that requested records do not exist.

The Commissioner is entitled to examine any record under appeal even if it is highly sensitive or confidential. The Commissioner's power to require records to be produced may be delegated to an Appeals Officer unless the record is a Cabinet record or a law enforcement record, in which case the delegation may be made only to an Assistant Commissioner. The only exception to this are records which are subject to federal legislation such as the *Young Offenders Act*. No one is liable to prosecution for an offence under any other act because he/she has provided records to the IPC.

When making arrangements for the transfer of sensitive records to the Commission, the head should consider the nature of the record and options for the secure delivery of the records to the IPC. For example, courier companies that have bonded employees and secure transport and storage may be used. Alternatively, an employee of the institution may deliver the records to the Commission.

Records that are kept at IPC premises are subject to significant security requirements. The records cannot be removed from the IPC premises, and must be locked away when not being used. All entry to the premises is controlled by a card access system and visitors are accompanied at all times. The Act prohibits IPC staff from disclosing any information acquired during the performance of their duties. They also cannot be compelled to testify as witnesses in any proceeding with respect to the information.

The IPC does not indefinitely retain records it received during an appeal. Where an appeal is disposed of by order, the records and any copies are either returned to the institution or destroyed one year after the day the order is issued. If an appeal is settled by mediation, the records are retained for nine months. Original records provided to the IPC are returned earlier if they are needed by the institution. Institutions receive notice of these matters from the Commission.

The Commissioner may require records to be produced and may enter and inspect any premises occupied by an institution for the purposes of an investigation. However, a head may require, in exceptional circumstances, that IPC staff examine an original record on site. This power of the head may be invoked, for example, if the record is fragile, unique or there is a large volume of records. Before entering any premises, the Commissioner must first notify the head of the institution. Institutions are discouraged from relying on the provision for on-site examination of records because it would place an undue administrative burden on the Commission.

Mediation

The Commissioner may authorize a mediator (i.e an Appeals Officer) to investigate the circumstances of any appeal and to try to effect a settlement of the matter under appeal (s.51 FIPPA / s.40 MFIPPA). The Appeals Officer will review the relevant records or circumstances under appeal and verify the institution's position. Acting as a go-between, he/she will also try to settle the appeal or simplify the issues, based on discussions with the appellant and the institution. In a mediated settlement all parties reach an agreement about the matter under appeal.

The Commissioner will attempt to settle the issues at appeal before resorting to an order. The general time period allotted for mediation is two months. This time period may be shortened if it is apparent that no agreement can be reached. The appeal will then proceed to an inquiry.

The Inquiry

s.52 FIPPA / s.41 MFIPPA

Notice of Inquiry and the Appeals Officer's Report

Where mediation is unsuccessful, the Commissioner may conduct an inquiry to review the head's decision (s.52(1)(b) FIPPA / s.41(1)(b) MFIPPA). At this stage, the appellant and the institution

receive a "Notice of Inquiry" (NOI) letter from the Commission. The notice informs the parties to an appeal that they are entitled to make representations. The NOI states the facts of the appeal and poses questions to the parties relating to the provisions of FIPPA/MFIPPA that are relevant to the issues under appeal. However, the parties do not have to limit their representations to only those questions raised in the NOI. An institution is expected to respond to the NOI by submitting representations within three weeks of the date of the Notice of Inquiry letter unless an extension is granted.

Considering Additional Exemptions and Facts During the Inquiry Process

The Commissioner may allow an institution to claim additional exemptions or to raise additional reasons for an exemption at the inquiry stage than were claimed originally at the request stage.

An institution may only claim additional **discretionary** exemptions within 35 days after the appeal has been opened. If an institution raises discretionary exemptions after the 35 days, the IPC is not obliged to consider the exemptions, although it may do so in unique circumstances. The institution must send a new decision letter setting out the additional exemption within the 35 day period so that the appellant is given an opportunity to comment on the applicability of the new exemption claim. The initial notice sent out by the Commissioner will specify the deadline for claiming any new discretionary exemptions.

Once an appeal has been filed, it is recommended that the Freedom of Information and Privacy Coordinator meet with the institution's legal advisor to review the exemptions originally claimed to determine whether they should continue to be relied upon.

There may also be occasions where further representations ought to be submitted by the parties. This may occur where the IPC has, in the interim, issued an order relevant to the appeal. In these situations the Appeals Officer may advise the parties that such an order has been issued, and allow for supplementary representations.

The Burden of Proof

s.53 FIPPA / s.42 MFIPPA

The party claiming that a record is exempt from access has the burden of proving that the exemption applies.

For example, if the head denies access to a record or part of a record, he/she must prove on appeal that all or part of a record falls within an exemption under the Act. Or, if a third party who may be affected by the disclosure of a record does not want the record to be released, the third party has to show why the record should not be disclosed.

If an appellant argues that there is a "compelling public interest" in the disclosure of an otherwise exempt record (s.23 FIPPA / s.16 MFIPPA), the burden of proof lies on the appellant. The burden is not absolute, however. Where the appellant is not familiar with the content of the records, the Commissioner will review them to determine whether the provision applies.

Written or Oral Submissions

An inquiry must be conducted in a manner that protects the confidentiality of the records pending the Commissioner's decision. Therefore, the normal rules governing the rights of parties who appear before tribunals do not apply (s.52(2) FIPPA / s.41(2) MFIPPA). These include, for example, the right to a public hearing and the right to cross-examine witnesses.

The Commission's general practice is to conduct inquiries through written submissions. It may require an institution to make certain submissions by affidavit. Any party to the appeal may request an opportunity to make oral submissions, and an oral hearing may be held if the Commissioner believes that it would aid in an exploration of the issues.

If an oral hearing is held, the Commissioner has the power to summon and examine witnesses under oath. Anything said or any document or thing produced during an inquiry, whether oral or written, is privileged to the same extent as it would be before a court. For example, testimony provided during a hearing may not be used in other proceedings, except in cases of a prosecution for perjury.

Access to an Institution's or Third Party's Submissions by an Appellant

The institution, the appellant and any affected party may be represented by counsel or an agent during an inquiry. All of these parties must be given an opportunity to make submissions to the Commissioner, but "no person is entitled to be present during, to have access to or to comment on representations made to the Commissioner by an other person" (s.52(13) FIPPA / s.41(13) MFIPPA).

Except if the appeal concerns a request for correction, the appellant makes his/her submissions without the opportunity to review the records. As a result, the appellant may request access to the institution's or a third party's submissions. The fact that a party is not *entitled* to access an opposite party's submissions does not mean that they are prohibited from seeing them. In restricted circumstances, the Commissioner may permit a party to hear or review the submissions or the other side, if doing so would not reveal the contents of the records in question.

An institution may also rely on s.52(13) FIPPA / s.41(13) MFIPPA to refuse to provide a copy of its submissions to a party who requests them directly from the institution. Other exemptions may also apply to an institution's submissions. If a request under FIPPA/MFIPPA is made for an institution's submissions, it is the Commission's practice to amalgamate any appeals which may

arise from such requests with the substantive appeal to which the request for representations relates.

Affidavit Evidence

On occasion, institutions are asked to provide information to the Commissioner in affidavit form to establish that records do not exist or that an adequate search was undertaken. An affidavit is a witness statement that declares under oath that a certain set of facts are true. The person swearing or affirming the statement reviews and signs it before a Commissioner for Oaths or a lawyer. In appeal inquiries before the IPC, an affidavit is acceptable as evidence in the same way as oral testimony given under oath. It is a criminal offence under the Criminal Code to swear a false affidavit.

The Effect of a Commissioner's Order

After receiving submissions from the interested parties, the Commissioner will issue a binding order that is not subject to appeal. An order may conclude with a statement requiring the institution to disclose the records referred to in the order within 35 days following the date of the order and not earlier than the 30th day following the date of the order. Day one is the first day after the date of the Order. Therefore, if the Order was dated May 1, the counting starts on May 2 and the first release date would be May 31. The institution may release the document on any of the 5 days following May 31st.

Where there are no affected third parties, the Order will usually conclude with a statement requiring the institution to disclose the records within 15 days of the date of the order.

Reconsideration of Commissioner's Orders

There is no express statutory provision in the Act that permits the Commissioner to reconsider an order. A reconsideration of an order is not an appeal of the order on its merits. A decision maker may reconsider a decision in exceptional circumstances where it is established that:

- (a) there is a fundamental defect in the adjudication process;
- (b) there is some other jurisdictional defect in the decision; or
- (c) there is a clerical error, accidental error or omission or other similar error in the decision.

An order will not be reconsidered simply on the basis that new evidence is provided, whether or not that evidence was obtainable at the time of the inquiry.

A request for reconsideration should be made in writing to the original Decision Maker and should include reasons why the application conforms to the criteria for reconsideration described above.

A request for reconsideration does not stay (suspend) the date of compliance for an order. An institution must still comply with the terms of an order unless otherwise directed by the IPC. It is imperative therefore, that a request for reconsideration be filed with the IPC Registrar of Appeals within 21 days of the order date. This will allow the IPC's Decision Maker to be in a position to make a determination on the request prior to the date for compliance of the order.

A request for reconsideration does not preclude a party from seeking other legal remedies that may be available (e.g. see Judicial Review below).

Judicial Review

The Commissioner has the power to issue a binding order that is not subject to an appeal. Appeals are distinct from judicial review proceedings. Judicial review proceedings are governed by the *Judicial Review Procedure Act*. Applications for judicial review may be brought before Divisional Court by a party to an appeal where it is alleged that the Commissioner's decision was patently unreasonable or otherwise outside the Commissioner's jurisdiction.

In the order issued by the Commissioner, the party against whom the order is made is advised of the right to apply for judicial review and is given 30 days to make the application. Where no application for judicial review is made within that period, the party must comply with the order.

Compliance Investigations

FIPPA/MFIPPA recognize that an institution should have basic standards for protecting personal information in its possession. The privacy provisions of the legislation require institutions to use appropriate practices and procedures for collecting, storing, using, disclosing and ultimately disposing of personal information.

Section 59 FIPPA / s.46 MFIPPA gives the Commissions the authority to:

- (a) offer comment on the privacy protection implications of proposed legislative schemes or government programs, and
- (b) after hearing an institution's head, order the institution to:
 - cease a collection of personal information practice, and
 - destroy a collection of personal information that contravene FIPPA/MFIPPA.

Individuals complain to the IPC when they believe that an institution has improperly collected, used, disclosed, retained or disposed of their personal information. The IPC is responsible for reviewing possible breaches of the privacy provisions of the legislation.

Sometimes the complaint is resolved informally through a resolution that is mutually satisfactory to the complainant and the institution. An example of the mediation available at every step of the process may be a simple explanation of the procedure or why the information was used in the way that it was. In these cases, the IPC may confirm the resolution by writing a letter to the institution rather than publishing a formal investigation report. If the complaint is not resolved in this way, a formal investigation proceeds.

The Privacy Investigation Process

There are five steps in the Privacy Investigation Process:

Notice and Request for Information

A letter from the Commission's staff notifies the institution that a complaint has been received and requests information relating to the institution's position on the matter. It also can include specific questions about issues, such as the authority to collect, use or disclose the complainant's personal information.

The Investigation

The institution is informed that every effort will be made to mediate and settle the complaint.

Copies of relevant documents may be required. Sometimes the investigation requires a personal visit to the institution by the investigator and/or meetings with key program staff.

Draft Report

If mediation is unsuccessful and the issues are straightforward or routine, the IPC may conclude the matter with a letter. In other cases the matter will go to a draft and final report.

Where an institution has breached the Act, recommendations to prevent future breaches are included. Both the institution and complainant are asked to comment on errors or omissions in the draft report.

Final Report

The IPC provides the institution and complainant with a final investigation report. Where recommendations have been made, the IPC requests evidence of implementation within six months. Evidence can be in the form of a letter and supporting documentation, such as a copy of a new policy or notice form.

Follow Up

If evidence is not received that the recommendations have been implemented within the six month period, the IPC contacts the institution to find out if they have been implemented, and if not, the reason why.

Chapter 8: Offences and Liability

Table of Contents

- Offences
 - Liability
-

Offences

s.61 FIPPA / s.48 MFIPPA

Certain violations of the Freedom of Information and Protection of Privacy Act (FIPPA) / Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) are considered to be offences. The Act sets out the penalties for these offences and stipulates, when the consent of the Attorney General is required for prosecutions.

It is an offence to intentionally and knowingly disclose personal information in a manner that is not authorized by s.61(1)(a) FIPPA / s.48(1)(a) MFIPPA.

It is also an offence to maintain a secret personal information bank that is not described and made public as required under s.44 FIPPA / s.34 MFIPPA. An employee of an institution who deliberately withholds information about the existence of a personal information bank with the intention that the bank's existence not be published, runs the risk of being prosecuted under s.61(1)(b) FIPPA / s.48(1)(b) MFIPPA.

Making a request for access to or correction of personal information under false pretences is also an offence under s.61(1)(c) FIPPA / s.48(1)(c) MFIPPA.

Other offences relate to obstructing the performance of the Commissioner in his/her duties, or willfully misleading the IPC, or willfully failing to comply with an order of the IPC (s.61(1)(d), (e) and (f) FIPPA / s.48(1)(d), (e) and (f) MFIPPA). A prosecution cannot be started under these subsections without the consent of the Attorney General (s.61(3) FIPPA / s.48(3) MFIPPA).

A person who is found guilty of an offence is liable to a fine not exceeding \$5,000.

Liability

s.62(2), (3) and (4) FIPPA / s.49(2), (3) MFIPPA

Civil actions cannot be brought against an employee of an institution for monetary damages resulting from the disclosure or non-disclosure of a record under the Act, if the action was done in good faith. No civil action can be brought against an employee for failure to give a required notice under the Act if reasonable care was taken to give notice. A record should be kept of the steps taken to provide the notice.

Institutions, as opposed to individual employees, are nonetheless liable to civil proceedings for damages resulting from violations of the freedom of information and privacy legislation (s.62(3), (4) FIPPA / s.49(3) MFIPPA).

Freedom of Information and Privacy Manual

APPENDIX I: SAMPLE BY-LAW

THE CORPORATION OF THE

[insert name]

BY-LAW NO. 98-00

Being a By-law to designate a head of the Municipal Corporation for the purposes of the *Municipal Freedom of Information and Protection of Privacy Act*.

Whereas, under Section 3, subsection 1 of the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c.M.56, the council of a municipal corporation may by by-law designate from among its members an individual or a committee of the council to act as head of the municipal corporation for the purposes of the Act:

And, whereas the council deems it necessary and expedient to designate a head for the purposes of the Act:

NOW THEREFORE THE COUNCIL OF THE CORPORATION OF THE [INSERT NAME] ENACTS AS FOLLOWS:

1. That [name/position of member of council or committee of council] be designated as head for the purposes of the *Municipal Freedom of Information and Protection of Privacy Act*.
2. That this by-law come into force and effect on [insert date here].

Read a first and second time this _____ day of _____, 19____.

[Clerk] [head of Council]

Read a third time and passed this _____ day of _____, 19____.

[Clerk] [head of council]

[seal of the municipal corporation]

Freedom of Information and Privacy Manual

APPENDIX II: SAMPLE RESOLUTION

RESOLUTION

FOR A BOARD, COMMISSION OR OTHER BODY

MOVED BY:

SECONDED BY:

Whereas, under Section 3, subsection (2) of the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990 c.M.56 the members elected or appointed to a board, commission or other body that is an institution under the Act may designate in writing from among its members an individual or committee of the body to act as head of the institution for the purposes of the Act:

And whereas the [**board, commission or other body**] deems it necessary and expedient to designate a head for the purposes of the Act:

Now, therefore, the [**board, commission or other body**] resolves as follows:

1. That the [**board, commission or other body**] hereby designates [**name/position of individual or committee**] as head for the purposes of the *Municipal Freedom of Information and Protection of Privacy Act*.
2. That this resolution come into force and effect on [insert date here].

[SECRETARY] [CHAIRPERSON]

Freedom of Information and Privacy Manual

APPENDIX III: SAMPLE DELEGATIONS OF AUTHORITY

Sample 1

I/we, [head of the institution for the purposes of the Act], delegate the following powers and duties under the [Municipal] Freedom of Information and Protection of Privacy Act to the positions indicated below:

Power or Duty	Officer	A	B	C
Severing records (s.10(2) FIPPA/s.4(2) MFIPPA)		X		
Obligation to disclose (s.11 FIPPA/s.5 MFIPPA)			X	
Deciding if exemptions apply:				
draft by-laws, private bills, closed meetings (s.6 MFIPPA)			X	
advice or recommendations (s.13 FIPPA/s.7 MFIPPA)			X	
law enforcement (s.14 FIPPA/s.8 MFIPPA)			X	
relations with governments (s.15 FIPPA/s.9 MFIPPA)			X	
third party information (s.17 FIPPA/s.10 MFIPPA)			X	
economic and other interests (s.18 FIPPA/s.11 MFIPPA)			X	
solicitor-client privilege (s.19 FIPPA/s.12 MFIPPA)			X	
danger to safety or health (s.20 FIPPA/s.13 MFIPPA)			X	
personal privacy (s.21 FIPPA/s.14 MFIPPA)			X	
information available or soon to be published (s.22 FIPPA/s.15 MFIPPA)			X	
individual's access to own personal information (s.49 FIPPA/s.38 MFIPPA)			X	
Determining compelling public interest (s.23 FIPPA/s.16 MFIPPA)			X	
Assisting requester clarify requests (s.24(2) FIPPA/s.17(2) MFIPPA)			X	
Continuing access requests (s.24 (3), (4) FIPPA)		X		
Forwarding and transferring requests (s.25 FIPPA/s.18 MFIPPA)		X		
Issuing Notices:				
forwarding or transferring requests (s.25(2), (3) FIPPA/s.18(2), (3) MFIPPA)		X		
regarding access to records (s.26, 28, 29 FIPPA/s.19, 21, 22 MFIPPA)		X		
time extensions (s.27 FIPPA/s.20 MFIPPA)		X		
to affected parties (s.28 FIPPA/s.21 MFIPPA)			X	

Decisions <i>re</i> manner of third party representations (s.28(6) FIPPA/s.21(6) MFIPPA)		X		
Granting access to original record (s.30 FIPPA/s.23 MFIPPA)		X		
Making records and records descriptions available (s.32, 33, 45 FIPPA/s.25, 34 MFIPPA)		X		
Preparing annual report (s.34 FIPPA/s.26 MFIPPA)		X		
Notice of collection of personal information (s.39(2) FIPPA/s.29(2) MFIPPA)		X		
Ensuring accuracy of personal information (s.40(2) FIPPA/s.30(2) MFIPPA)		X		
Disposal of personal information (s.40(4) FIPPA/s 30(4) MFIPPA)		X		
Personal information banks (s.46 FIPPA/ s.35 MFIPPA)		X		
Access to personal information (s.48(4) FIPPA/s.37(3) MFIPPA)		X		
Representing institution on appeal (s.52FIPPA/s.41 MFIPPA)				X
Requiring examination of record on site (s.52(6) FIPPA/s.41(6) MFIPPA)		X		
Fees (s.57FIPPA/s.45 MFIPPA)		X		
Providing access - oral requests (s.63FIPPA/s.50 MFIPPA)			X	

Date

Signature(s)

Sample 2

I/we [**head of the institution for the purposes of the Act**], delegate all powers and duties under the [Municipal] Freedom of Information and Protection of Privacy Act to [**position title**].

Date

Signature(s)

Freedom of Information and Privacy Manual

APPENDIX IV: SAMPLE NOTIFICATION LETTERS

#1 Notification to Requester

[Date]Request Number[#]

[Requester's name and address]

Dear _____:

Thank you for your access request which we received on **[insert date]** under the *[Municipal] Freedom of Information and Protection of Privacy Act*. We received your \$5.00 application fee and your request for access to the following:

[insert details of records requested]

Option: Further information/Clarification required

Unfortunately, the request does not provide sufficient detail to identify the record(s). Please supply the following information so that we may begin to process your request:

[insert details of information needed]

We would be happy to answer any questions or assist you in clarifying or reformulating your request.

If we do not hear from you within 30 days of this letter's date, we will close your file.

Option: Transfer/Forward

[Name and address of other institution] has (custody or control of) **OR** (a greater interest in) the records you seek. Under section 25/18 of the Act, we (forwarded) **OR** (transferred) your access request to them [enclose s.25/18]. Since we are not processing your request we are returning your \$5.00 application fee with this letter. Please send a new application fee to the institution listed above.

You may appeal this decision to the Information and Privacy Commissioner. The Commission can be reached at:

See also Additional Information [#11](#)

Please contact [**name, title and phone number of person responsible**] if you have any questions. We would appreciate you using the Request number [#] assigned to your request in any further correspondence.

NOTE: As quickly as possible, the head or delegate should notify the other institution that a request is being forwarded/transferred

Sincerely,

[**signed by head or delegate**]

encl.

Freedom of Information and Privacy Manual

APPENDIX IV: SAMPLE NOTIFICATION LETTERS

#2 Notice to Institution Receiving a Transferred/Forwarded Request

[Date] Request Number[#]

[Name and address of transferee institution]

Dear _____:

The enclosed request for access was received on **[date]**.

This request is [transferred/forwarded] to you under section 25/18 of the [*Municipal Freedom of Information and Protection of Privacy Act*] as we believe your institution has [custody or control of/greater interest in] the record.

We have returned the application fee to the requester and have instructed him/her to send an application fee to you.

Sincerely,

[signed by Freedom of Information and Privacy Coordinator]

Freedom of Information and Privacy Manual

APPENDIX IV: SAMPLE NOTIFICATION LETTERS

#3 Notice of Time Extension

[Date] Request Number[#]

[Requester's name and address]

Dear _____:

Thank you for your access request which we received on **[insert date]** under the *[Municipal] Freedom of Information and Protection of Privacy Act*. We received your \$5.00 application fee and your request for access to the following:

[insert details of records requested]

A request under the Act usually must be answered within 30 calendar days, however section 27/20 (enclosed) allows for time extensions under certain circumstances. The time limit for answering your request has been extended for an additional **[insert number]** days to **[insert date]**.

The reason for the time extension is **[insert reason]**:

You may request that our decision to extend the time limit be reviewed by the Information and Privacy Commissioner. The Commissioner can be reached at:

[insert address]

See also Additional Information [#11](#)

Please contact **[name, title and phone number of person responsible]** if you have any questions. We would appreciate you using the Request number [#] assigned to your request in any further correspondence.

Sincerely,

[signed by head or delegate]

Freedom of Information and Privacy Manual

APPENDIX IV: SAMPLE NOTIFICATION LETTERS

#4 Fee Estimate/Interim Decision Regarding Disclosure

[Date]Request Number[#]

[Requester's name and address]

Dear _____:

Thank you for your request which we received on **[insert date]** under the *[Municipal] Freedom of Information and Protection of Privacy Act* for access to **[describe records requested]**. An initial review of the records indicates that it will cost an estimated **[enter amount]** to process your request. The fee estimate is based on **[explain fee estimate]**.

As we have not yet reviewed the records in detail, no final decision has been made regarding access but the following exemptions will likely apply. **[Generally describe what exemptions might apply to the records]**.

[AND: Where the fee estimate is over \$100.00]

Regulation 460/823 s.7, says that where the fee estimate is over \$100.00, an institution may request a deposit equal to 50% of the estimated fee. We will wait until we receive the amount of **[enter amount]** from you before we resume processing the request.

The Act provides that all or part of the fee can be waived if in our opinion it is fair and equitable to do so, if the fee will cause you financial hardship or if dissemination of the record will benefit public health or safety. You may be required to provide proof to support any waiver claims. Please notify **[insert name, title and phone number]** as soon as possible of your wish to proceed with a request for a fee waiver.

If you disagree with any aspect of the fees, or wish to revise your request, please discuss the matter with us. Afterward, you may request that this fee estimate be reviewed by the Information and Privacy Commissioner. The Commissioner can be reached at:

[insert address]

See also Additional Information [#11](#)

Please note that you have 30 days from the receipt of this letter to request a review from the Commissioner. If we have not heard from you within 30 days we will close your file.

Enclosed is a copy of section 57/45 of the Act and the relevant regulations [**optional**]. Please contact [**name, title and phone number of person responsible**] with any questions. We would appreciate you using the Request number [#] assigned to your request in any further correspondence

Sincerely,

[**signed by head or delegate**]

Freedom of Information and Privacy Manual

APPENDIX IV: SAMPLE NOTIFICATION LETTERS

#5 Notice to Affected Third Party - Section 17/10: Third Party Information

[Date]Request Number[#]

[Affected third party's name and address]

Dear _____:

The **[name of institution]** has received a request for access to records under the *[Municipal] Freedom of Information and Protection of Privacy Act* to disclose **[describe in detail the records as they relate to the s.17/10 affected third party]**.

According to section 28/21 of the Act, a third party whose interests may be affected must be given the opportunity to make representations to the head of an institution concerning disclosure of the records.

To successfully qualify for a third party exemption, *all* of the following three tests must be met:

- the information must fit within one of the specified categories of third party information: trade secret or scientific, technical, commercial, financial or labour relations information;
- the information must have been *supplied* by the third party *in confidence*, implicitly or explicitly; and
- the disclosure of the information could reasonably be expected to cause one of the harms indicated below:
 - prejudice your competitive position or interfere with any contractual rights you possess, or
 - result in you no longer supplying this or similar information to **[name of institution]**, or
 - result in undue loss or gain to any person, business, or organization of which you are aware.

Under section 17/10 of the Act, we must release these records unless the above conditions are met. Please review the attached records.

If you have concerns about the release of the records please contact us, in writing, no later than [insert date] outlining your concerns. In order to support your claims

against the release of the records or portions of the records, you must show how those records meet the third party criteria listed above.

We will notify you in writing by [insert date] about our decision regarding the release of the records.

Enclosed are copies of sections 17/10 and 28/21 of the Act for your convenience and information [optional]. Please contact [name, title and phone number of person responsible] if you have any questions. We would appreciate you using the request number [#] assigned to the request in any correspondence

Sincerely,

[signed by head or delegate]

Freedom of Information and Privacy Manual

APPENDIX IV: SAMPLE NOTIFICATION LETTERS

#6 Notice to Affected Third Party - Section 21 FIPPA/14 MFIPPA: Personal Information

[Date]Request Number[#]

[Affected third party's name and address]

Dear _____:

The **[name of institution]** has received a request under the *[Municipal] Freedom of Information and Protection of Privacy Act* to disclose **[describe in detail the records as they relate to the affected individual]**.

Section 28/ 21 of the Act says individuals have the opportunity to make representations about the release of their personal information to a third party.

Your views regarding disclosure of these records is appreciated. Please indicate in writing whether or not you consider that the disclosure of the enclosed records would be an invasion of your personal privacy. Section 21/14 of the Act outlines circumstances where the disclosure of personal information may be an unjustified invasion of personal privacy.

Your response must be received no later than **[insert date]**. You will be notified in writing by **[insert date]** about our decision regarding the release of the records.

Enclosed are copies of sections 21/14 and 28/21 of the Act for your convenience and information **[optional]**. Please contact **[name, title and phone number of person responsible]** if you have any further questions. We would appreciate you using the Request number [#] assigned to the request in any correspondence.

Sincerely,

[signed by head or delegate]

Freedom of Information and Privacy Manual

APPENDIX IV: SAMPLE NOTIFICATION LETTERS

#7 Notice to Requester Where Third Party is Affected

[Date]Request Number[#]

[Requester's name and address]

Dear _____:

Thank you for your request which we received on **[insert date]** under the *[Municipal] Freedom of Information and Protection of Privacy Act* for access to **[describe records requested]**.

The disclosure of the records may affect the interests of a third party.

The third party whose interests may be affected is being given the opportunity to make representations about the release of the record(s).

A decision on whether or not the record(s) will be disclosed will be made by **[insert date]**, under section 28/21 of the Act.

Enclosed is a copy of section 28/21 of the Act for your convenience and information **[optional]**. Please contact **[name, title and phone number of person responsible]** if you have any further questions. We would appreciate you using the Request number [#] assigned to the request in any correspondence

Sincerely,

[signed by head or delegate]

Freedom of Information and Privacy Manual

APPENDIX IV: SAMPLE NOTIFICATION LETTERS

#8 Notice to Affected Third Party After Representations Where Head Intends to Release the Record(s)

[Date]Request Number[#]

[Affected third party's name and address]

Dear _____:

We have received and considered your representations concerning disclosure of [**details of the record(s)**]. Our decision is to grant access [**or partial access**] to the record(s). [**Give reasons for the decision**].

Under section 28/21 of the [*Municipal*] *Freedom of Information and Protection of Privacy Act*, you may request that this decision be reviewed by the Information and Privacy Commissioner. The Commissioner can be reached at:

[insert address]

See also Additional Information [#11](#)

You have until [**insert date**] to request a review, otherwise the records will be released to the requester.

Please contact [**name, title and phone number of person responsible**] if you have any further questions. We would appreciate you using the Request number [#] assigned to the request in any further correspondence

Sincerely,

[signed by head or delegate]

Freedom of Information and Privacy Manual

APPENDIX IV: SAMPLE NOTIFICATION LETTERS

#9 Notice to Requester Regarding an Access Decision

[Date]Request Number[#]

[Requester's name and address]

Dear _____:

In response to your request under the [*Municipal*] *Freedom of Information and Protection of Privacy Act* for access to [**describe records requested**].

Option: access granted

I am pleased to inform you access is granted to [**insert details**].

Option: subject to copyright

Please note that you are bound by any copyright that applies to the records you receive under this Act.

Option: no records exist

Access cannot be provided to [**insert details of nonexistent records**] as the records do not exist.

Option: denial of access

Access is denied to [**insert details of withheld records**] under section(s) [**insert section numbers**] of the Act. The provisions apply to the record(s) because [**insert reasons**].

Option: refusal to confirm existence

Under section [**12(5)/14(5)**] **OR** [**14(3)/8(3)**], we cannot confirm or deny the existence of the record.

Option: summary of records categories

Due to the complexity of your request, we have summarized the records categories in order to provide you with an overview of the access decision made.

You may request that this decision be reviewed by the Information and Privacy Commissioner. The Commissioner can be reached at:

[insert address]

See also Additional Information [#11](#)

Please note that you have 30 days from the receipt of this letter to request a review.

Enclosed is a copy of section [insert relevant section number] of the Act for your convenience and information [optional]. Please contact [name, title and phone number of person responsible] if you have any questions. We would appreciate you using the Request number [#] assigned to your request in any further correspondence

Sincerely,

[signed by head or designate]

NOTE: In this notice (if partial access is granted), the institution may wish to:

- **indicate the fees for access to the records, if any;**
- **give the requester the option to view the record; or**
- **indicate that identification will be required if access is given to an individual's own personal information**

Freedom of Information and Privacy Manual

APPENDIX IV: SAMPLE NOTIFICATION LETTERS

#10 Notice to Requester - Correction of Personal Information

[Date]Request Number[#]

[Requester's name and address]

Dear _____:

Your request under the *[Municipal] Freedom of Information and Protection of Privacy Act* for a correction of personal information was received on **[insert date]**.

The correction was made and a copy of the corrected record is attached. On request, you are entitled to have the correction sent to those persons to whom the information was disclosed over the past 12 months.

OR

The correction was not made to the personal information. In reaching this decision we considered the following 3 elements: 1) whether the information is personal and private; 2) whether the information is inexact, incomplete or ambiguous and 3) whether the correction would be a substitution of opinion **AND/OR [insert reason why the request was refused][optional]**.

You are entitled to require that a statement of disagreement be attached to the record and that the statement of disagreement be sent to any person to whom the record was disclosed over the past 12 months.

You may appeal this decision to the Information and Privacy Commissioner. The Commissioner can be reached at:

[insert address]

See also Additional Information [#11](#)

Please note that you have 30 days from the receipt of this letter to request a review.

Sincerely,

[signed by head or designate]

NOTE: With this notice, the institution may wish to include a listing of the persons to whom the personal information was disclosed over the past 12 months (this listing will not include those persons listed in the personal information bank index)

Freedom of Information and Privacy Manual

APPENDIX IV: SAMPLE NOTIFICATION LETTERS

#11 Additional Information Where Appeal's are Likely:

If you decide to appeal a decision to the Information and Privacy Commissioner, please provide the Commissioner's office with:

- 1) The request number assigned to the request
- 2) A copy of this decision letter, and
- 3) A copy of the original request you sent to this institution.

Appeals to the Commissioner must also be accompanied by the appropriate fee. Fees vary according to the nature of the request being appealed as follows:

- (a) \$25, if the person appealing has made a request for access to a general record under subsection 24(1) FIPPA / 17(1) MFIPPA;
- (b) \$10, if the person appealing has made a request for access to personal information under subsection 48(1) FIPPA / 37(1) MFIPPA; and
- (c) \$10, if the person appealing has made a request for correction of personal information under subsection 47(2) FIPPA / 36(2) MFIPPA.

No fee is payable for appealing a decision of a head to the Commissioner if the person appealing is a third party given notice of a request under subsection 28(1) FIPPA / 21(1) MFIPPA of the Act.

Freedom of Information and Privacy Manual

APPENDIX IV: SAMPLE NOTIFICATION LETTERS

#12 Internal Memo To Program Area Regarding a FOI Request

MEMORANDUM TO: (Name of Contact and Program Area)

OUR REFERENCE: Request [#]

SUBJECT: Freedom of Information Request

The attached request was made under [*Municipal*] *Freedom of Information and Protection of Privacy Act* and concerns records which we believe to be in the custody of your [area].

Please review the request and conduct a search for the records.

Your response to this request should be forwarded to this office, to be received on or before [date], and should include:

1. copies of the records (if too voluminous to copy, please contact us);
2. an indication of the number of photocopies made in response to this request and a tally of the person-hours spent searching for the record(s); and
3. your written recommendations regarding disclosure.

If the records are not in the custody of your area please provide a "nil" response. It should be noted that "nil" responses may require an affidavit at a later date; therefore, please note the date, time and location of the searches conducted.

Upon receiving your reply, we will review your findings and the requested records and if necessary, consult with our legal counsel before preparing the notification to the requester.

Any decision to apply an exemption will be reviewed with the head before it is sent to the requester.

If you have any questions please call me at [telephone#]

Freedom of Information and Privacy Coordinator

Enclosure

cc. [any appropriate persons]

Freedom of Information and Privacy Manual

APPENDIX V: SAMPLE BIOGRAPHY

JANE CITIZEN

Jane Citizen, of Anyplace, Ont. was recently appointed to the Anyplace Advisory Committee for Parks and Recreation.

Ms. Citizen has lived in Anyplace for the past 10 years. She has considerable volunteer experience in the community, having served as a board member for several local recreational associations, as the president of the Anyplace Tennis Club, and as president of the West Anyplace Neighbourhood Association. She is also a former medal winner for Canada in speed skating at the 1968 Olympics.

Ms. Citizen is President of Jane Citizen Electronics in Anyplace. She has a degree in engineering from the University of Toronto.

Freedom of Information and Privacy Manual

APPENDIX VI: AFFIDAVIT

(General heading)

AFFIDAVIT

OF (*Name*)

I (*full name of deponent*) of the (*City, Town etc.*) of

In the (*County, Regional Municipality, etc.*) of

(*Where the deponent is a part or the solicitor, officer, director, member, employee of a party; set out of deponent's capacity*),

MAKE OATH AND SAY (or AFFIRM):

1. (*Set out the statements of fact in consecutively numbered paragraphs, with each paragraph being confined as far as possible to a particular statement of fact.*)

Sworn (or Affirmed) before me at the (*City, Town etc.*) of

_____, on (date) _____

Commissioner for Taking Affidavits

(or as may be)

(Signature of deponent)

Freedom of Information and Privacy Manual

APPENDIX VIII: RESEARCH AGREEMENT

Freedom of Information and Protection of Privacy Act

This agreement is made between

Name of researcher (referred to hereinafter as the "Researcher") and ----- ---Name of institution (referred to below as the "Institution")
--

The researcher has requested access to the following records containing personal information in the custody or the control of the institution:
--

The researcher understands and promises to abide by the following terms and conditions:

1. The researcher will not use the information in the records for any purpose other than the following research purpose unless the researcher has the institution's written authorization to do so: (Describe the research purpose below).

2. The researcher will give access to personal information in a form in which the individual to whom it relates can be identified only to the following persons: (Name the persons below)

3. Before disclosing personal information to persons mentioned above, the researcher will enter into an agreement with those persons to ensure that they will not disclose it to any other person.

4. The researcher will keep the information in a physically secure location to which access is given only to the researcher and to the persons mentioned above.

5. The researcher will destroy all individual identifiers in the information by _____ . (date)

6. The researcher will not contact any individual to whom personal information relates, directly or indirectly without the prior written authority of the institution.

7. The researcher will ensure that no personal information will be used or disclosed in a

form in which the individual to whom it relates can be identified without the written authority of the institution.

8. The researcher will notify the institution in writing immediately upon becoming aware that any of the conditions set out in this agreement have been breached.

Signed at , this Day of 19

Researcher's Signature	Representative of Institution
Name of Researcher	Name and Position of Representative
Address	Name of Institution
	Address
Tel.no.	Tel.no.

Freedom of Information and Privacy Manual

APPENDIX IX: REQUEST FOR WAIVER OF NOTICE TO INDIVIDUAL OF COLLECTION OF PERSONAL INFORMATION

Freedom of Information and Protection of Privacy Act s.39(2)

Municipal Freedom of Information and Protection of Privacy Act s.29(2)

1. Institution

2. Description of Information to be Collected:

3. Authority for Collection:

4. Manner of Collection:

(i) directly from the individual to whom the information relates.

(ii) indirect collection pursuant to s.39(1) FIPPA/ s.29(1) MFIPPA

5. Anticipated number of individuals in respect of whom Waiver is sought:

6: Use of Personal Information Collected:

(i) Describe Purpose of Collection:

(ii) S.41, 42 FIPPA/s.31, 32 MFIPPA Authorization for Use: (insert section and paragraph number)

(iii) Use listed in Directory

Yes

No (explain)

7. Reason for Waiver:

(i) Reason

Notification Frustrates Purpose of Indirect Collection

Statutory Authority for Indirect Collection

Administrative Burden/Cost of Notification

Authorization of Commissioner

Implied Consent

Collection is from another Institution which has notified Individual

Other (explain)

(ii) Explain why notification cannot be given.

8. Other material attached:

Date:

Head of Institution