Information, Privacy and Archives

Ministry of Government and Consumer Services

# Freedom of Information and Protection of Privacy Manual

Ontario

Information, Privacy and Archives Division
Ministry of Government and Consumer Services

# Acknowledgement

The Information, Privacy and Archives Division wishes to thank all those who provided feedback on draft versions of this manual. In particular, we wish to thank Coordinators and staff at the Ministry of Community and Social Services, Ministry of Economic Development and Growth; Ministry of Government and Consumer Services, Ministry of Municipal Affairs, Ministry of Transportation, Cabinet Office, and Metrolinx.

Table of Contents

**About this Manual** ..... **1**
Purpose ..... 1
Audience ..... 1
Use of the Manual ..... 1
Whom to Contact ..... 2
Related Resources ..... 2
**Glossary** ..... **3**

**Part I: The Legislation, Roles and Responsibilities** ..... **5**
**Chapter 1: The Legislation** ..... **6**
Introduction ..... 6
History ..... 6
Policy Goals ..... 6
Ontario Access and Privacy Laws ..... 7
Purpose of Legislation ..... 8
Access and Privacy Principles ..... 8
Organization of Legislation ..... 9
Interactions with Other Laws ..... 9
Prevailing Legislation ..... 10
Copyright Act ..... 10
Litigation ..... 11
Resources ..... 11
**Chapter 2: Government Roles and Responsibilities** ..... **12**
Introduction ..... 12
Responsible Minister ..... 12
Policy and Legal Support ..... 13
Information and Privacy Commissioner of Ontario ..... 14
Coverage under the Legislation ..... 14
Listing of Institutions and Regulation Updates ..... 16
Exceptions to Coverage ..... 17
Head of an Institution ..... 18
Delegation of Authority ..... 19
Offences and Liability ..... 20
Recordkeeping ..... 21
Resources ..... 21
**Chapter 3: Coordinator Roles and Responsibilities** ..... **22**
Introduction ..... 22
Overview of Roles and Responsibilities ..... 22
Administration ..... 23

Policies and Procedures ..... 23
Processing Requests ..... 23
Case File Management and Reporting ..... 24
Research ..... 24
Mediation and Appeals ..... 25
Issues Management ..... 25
Publications ..... 26
Resources ..... 26
**Part II: Freedom of Information ..... 27**
**Chapter 4: Access Fundamentals ..... 28**
Introduction ..... 28
Applying the Legislation ..... 28
Understanding Records ..... 28
Creating Records ..... 29
Custody or Control ..... 30
Records of Third Parties ..... 31
Notice to Affected Persons ..... 32
Applying Relevant Sections ..... 33
Exclusions ..... 33
Mandatory Exemptions ..... 36
Discretionary Exemptions ..... 36
Exceptions ..... 38
Exercise of Discretion ..... 38
Harms Test ..... 39
Public Interest Override ..... 39
Available for Public Review ..... 40
Institution Records ..... 41
Directory of Institutions ..... 41
Directory of Records ..... 42
Routine Disclosure and Open Government ..... 43
Obligations to Disclose ..... 43
Resources ..... 44
**Chapter 5: Exemptions and Exclusions ..... 45**
Introduction ..... 45
Exemptions ..... 45
Draft By-Laws and Closed Municipal Meetings ..... 46
Cabinet Records ..... 47
Advice to Government/Advice or Recommendations ..... 50
Law Enforcement ..... 52
Civil Remedies Act, 2001 ..... 58

Step 1: Receiving a Request ..... 117
Step 2: Assessing a Request ..... 118
Step 3: Searching and Locating Records ..... 118
Step 4: Reviewing and Analyzing Records ..... 121
Step 5: Finalizing Recommendations and a Decision ..... 123
Step 6: Preparing and Sending Records ..... 124
Step 7: Closing the File ..... 126
Research Agreements ..... 126
Case File and Knowledge Management ..... 128
Statistical Reporting ..... 128
Resources ..... 129

**Part III: Protection of Privacy ..... 131**
**Chapter 7: Privacy Fundamentals ..... 132**
Introduction ..... 132
Understanding Privacy ..... 132
Personal Information ..... 133
Business Identity Information ..... 134
Customer Service Information ..... 134
Common Examples of Personal Information ..... 135
Privacy Rules ..... 135
Authority to Collect ..... 136
Manner of Collection ..... 137
Use and Disclosure of Personal Information ..... 140
Accuracy ..... 144
Retention ..... 144
Security ..... 145
Disposal ..... 145
Public Records of Personal Information ..... 146
Resources ..... 148
**Chapter 8: Personal Information and Correction Requests ..... 149**
Introduction ..... 149
Applying the Legislation for Personal Information Requests ..... 149
Exemptions to the Right of Access to One's Own Personal Information ..... 150
Personal Information of Other Individuals ..... 151
Other Exemptions ..... 151
Correcting One's Own Personal Information ..... 152
Comprehensible Form ..... 152
Resources ..... 153
**Chapter 9: Privacy Management ..... 154**
Introduction ..... 154

Define Roles and Responsibilities ..... 154
Privacy Policy ..... 155
Align Business Practices ..... 155
Monitor and Evaluate Privacy Program ..... 158
Privacy Breaches ..... 159
Privacy Breach Response Plan ..... 160
Resources ..... 163

**Part IV: The Office of the Information and Privacy Commissioner of Ontario ..... 165**
**Chapter 10: Interacting with the IPC ..... 166**
Introduction ..... 166
Guiding Principles ..... 166
Obligations and Best Practices for Staff ..... 167
Seeking Comments or Advice on New Initiatives ..... 167
IPC Initiated Contact with Institutions ..... 168
Resources ..... 168
**Chapter 11: Appeals Process ..... 169**
Introduction ..... 169
Reasons for an Appeal ..... 169
IPC Powers ..... 170
Stages of Appeal ..... 171
Timelines ..... 171
Initiating an Appeal ..... 173
Intake Stage ..... 174
Mediation Stage ..... 175
Adjudication ..... 175
Providing Records to the IPC ..... 177
On Hold and Abandoned Appeals ..... 178
Reconsideration of Orders ..... 178
Constitutional Issues ..... 179
Judicial Review ..... 179
Resources ..... 179
**Chapter 12: Privacy Complaints, Breaches and Investigations ..... 181**
Introduction ..... 181
Privacy Complaints ..... 181
Institution Reported Privacy Breaches ..... 182
Privacy Investigation Process ..... 182
Resources ..... 183

**Part V: Appendices ..... 184**
**Appendix 1: Sample Draft By-Law Designating Head Under MFIPPA ..... 185**

**Appendix 2: Sample Resolution Designating Head Under MFIPPA ..... 186**
**Appendix 3: Sample Delegation of Authority ..... 187**
3.1 – Detailed Delegation of Authority ..... 187
3.2 – Simplified Delegation of Authority for Small Institutions ..... 196
**Appendix 4: Template Letters for Request Processing ..... 197**
4.1 – Letter to Requester Acknowledging Request - Standard ..... 197
4.2 – Letter to Requester Acknowledging Request – Application Fee Missing ..... 198
4.3 – Letter to Requester Acknowledging Request – Clarification Required ..... 199
4.4 – Letter to Requester Acknowledging Request – Proof of Identity Required ..... 200
4.5 – Letter to Requester when Transferring of Forwarding a Request ..... 201
4.6 – Letter to Receiving Institution when Transferring or Forwarding a Request ..... 202
4.7 – Letter to Requester – Notice of Time Extension ..... 203
4.8 – Letter to Requester – Fee Estimate and Interim Decision - $25 to $99 Fee ..... 204
4.9 – Letter to Requester – Fee Estimate and Interim Decision – Over $100 Fee ..... 206
4.10 – Notice to Affected Person for Third Party Information ..... 208
4.11 – Notice to Affected Person for Personal Privacy ..... 210
4.12 – Letter to Requester – Notice of Delay Where a Third Party's Interests are Impacted ..... 211
4.13 – Letter to Affected Person – Notice to Disclose Information ..... 212
4.14 – Letter to Affected Person – Notice to Withhold Information ..... 213
4.15 – Letter to Requester – Decision to Disclose All Records ..... 214
4.16 – Letter to Requester – Decision to Deny Access in Full or in Part ..... 216
4.17 – Letter to Requester – Decision to Refuse to Confirm or Deny Existence of Record 218
4.18 – Letter to Requester – Decision of No Responsive Records Exist ..... 219
4.19 – Letter to Requester – Decision Approving Correction of Personal Information Request ..... 220
4.20 – Letter to Requester – Decision Denying Correction of Personal Information Request ..... 221
4.21 – Letter to Requester Advising Request will be Considered Abandoned ..... 223
**Appendix 5: Sample Record Search Form ..... 224**
**Appendix 6: Sample Fee Estimate Form ..... 226**
**Appendix 7: Sample Index of Records ..... 228**
**Appendix 8: Request for Waiver of Notice to Individual of Collection of Personal Information ..... 229**

# About this Manual

## Purpose

The Freedom of Information and Protection of Privacy Manual is a general guide to the Freedom of Information and Protection of Privacy Act (FIPPA) and the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and administration of these Acts.

The manual combines policy and operational guidance to help Freedom of Information and Privacy Coordinators and their staff:

- Understand the general framework of the legislation;
- Interpret the legislation and regulations;
- Meet administrative and operational requirements; and
- Be aware of best practices for institutions.

The manual also provides information to the general public on how the legislation is administered within institutions.

This manual does not provide guidance on the application of the Personal Health Information Protection Act.

## Audience

The primary audience for the manual is provincial and municipal Freedom of Information and Privacy Coordinators and their staff.

The manual is also intended to be an information resource for the general public.

## Use of the Manual

Coordinators should use the manual with an up-to-date version of the applicable legislation and regulations available through e-laws. There may be sections of the legislation and regulations that are not covered in the manual.

The manual is not meant to provide legal advice. For legal advice, Coordinators should work with Legal Counsel.

## Whom to Contact

Coordinators and the general public may contact staff in the Information, Privacy and Archives Division of the Ministry of Government and Consumer Services (MGCS) about the manual and more information regarding access to information and protection of privacy in Ontario.

Coordinators and the general public may contact the Information, Privacy and Archives Division staff by telephone at 416-327-1600 or 1-800-668-9933 (toll-free in Ontario only). You may also send inquires by email to Web.Foi.MGCS@ontario.ca.

## Related Resources

Related resources from the Office of the Information and Privacy Commissioner of Ontario (IPC) are listed at the end of each chapter.

The appendices to this manual include forms, templates, and letters that may be used and adapted by Coordinators for use in their offices.

The manual includes hyperlinks to the relevant sections of the legislation, IPC documents, other resources, other parts of the manual, and its appendices.

# Glossary

In this manual:

“Case law” means decisions issued by the Courts;

“Coordinator” means any provincial or municipal freedom of information and protection of privacy coordinator or equivalent or that person normally performing the role of the freedom of information and protection of privacy coordinator;

“Exception” means types of records or information that do not qualify for an exclusion or exemption under FIPPA or MFIPPA;

“Exclusion” means a provision under FIPPA or MFIPPA which excludes records or parts of records from the application of the legislation;

“Exemption” means a provision under FIPPA or MFIPPA which exempts records or information from the general right of access;

“Head” means the head of an institution as defined by FIPPA and MFIPPA;

“Institution” means an institution as defined by FIPPA and MFIPPA;

“IPC” means the Office of the Information and Privacy Commissioner of Ontario;

“Legal Counsel” means Legal Counsel assigned to support an institution;

“Legislation” means both FIPPA and MFIPPA and their regulations in instances where the laws are similar; FIPPA and MFIPPA are referred to individually where the laws are different;

“Manual” means the Freedom of Information and Protection of Privacy Manual;

“MGCS staff” means staff in the Enterprise Recordkeeping, Access and Privacy Branch; Information, Privacy and Archives Division of the Ministry of Government and Consumer Services;

“MGCS Legal Counsel” means Legal Counsel in the Access and Privacy Law Group, Ministry of Government and Consumer Services;

“Privacy breach” means an incident where personal information is collected, retained, used, disclosed or disposed of in ways that do not comply with personal information protection requirements in statute and regulation;

“Privacy Impact Assessment” means a process that reviews a new or existing information system or program to determine whether measures are necessary to ensure compliance with personal information protection requirements in statute and regulation and to address the broader privacy implications of the system or program;

“Program area” means related activities or services within an institution for which the institution has authority and responsibility;

“Record” (as defined by FIPPA and MFIPPA) means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise;

“Request” means a Freedom of Information (FOI) access request, including both request for general records and requests for one’s own personal information;

“Responsible Minister” means the Minister of Government and Consumer Services; and

“Senior management” means all levels of managers accountable and responsible for decision-making and approvals.

# Part I: The Legislation, Roles and Responsibilities

# Chapter 1: The Legislation

## Introduction

Access and privacy laws play a central role in government. These laws promote accountability, transparency, public participation and protect the privacy rights of individuals.

This chapter provides broader context and explains how Coordinators should navigate through the legislation. It introduces the history and legal framework of access and privacy laws in Ontario; explains the legislation's purpose and principles; how it is organized; and how it interacts with other laws.

## History

The Ontario Government established the Commission on Freedom of Information and Individual Privacy in 1977 to look at ways to improve public information policies and public sector access and privacy legislation. The Commission was headed by Dr. D. Carlton Williams and is known as the "Williams Commission".

The framework for Ontario's legislation is set out in the Commission's report entitled "Public Government for Private People, The Report of the Commission on Freedom of Information and Individual Privacy" published in 1980.

FIPPA received royal assent in 1987, and came into force on January 1, 1988. The municipal counterpart, MFIPPA, came into force on January 1, 1991.

## Policy Goals

The William's Commission, in making its recommendations, considered policy goals relating to good government such as:

**Transparency:** The public's right to know what government is doing and how decisions have been reached.

**Accountability:** The public's ability to hold elected representatives responsible for how they carry out their roles.

**Public participation:** Citizen involvement in policy development and decision-making.

**Fairness in decision-making:** An individual's ability to present their side of an issue, and their right to access the information on which a decision-maker will act, including the criteria to be applied.

**Personal privacy:** The government's records of personal information and information management practices, and an individual's right to have access to government information concerning them.

**Administrative costs:** The cost-benefit of the resources required to administer the legislation and the benefits to society from a more open government.

## Ontario Access and Privacy Laws

Access and privacy laws are a category of administrative law developed to ensure that:

- The activities of government are authorized; and
- Laws are implemented and administered in a fair and reasonable manner.

In Ontario, there are four main laws that deal with access to information and privacy. Other federal and provincial legislation and municipal by-laws have specific access and privacy provisions that may also apply. The four main laws are listed below:

**Freedom of Information and Protection of Privacy Act (FIPPA)**: Applies to the provincial government of Ontario, universities, colleges, hospitals and designated agencies. FIPPA came into force on January 1, 1988.

**Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)**: Is the local government equivalent of FIPPA and covers municipal institutions such as municipalities, cities, towns, school boards, police services and many other local government entities. MFIPPA came into force on January 1, 1991.

**Personal Health Information Protection Act (PHIPA):** Provides rules specific to personal health information in the custody of health information custodians. Health information custodians include health care practitioners such as hospitals, long-term care facilities, pharmacies and more. PHIPA came into force on November 1, 2004.

**Personal Information Protection and Electronic Documents Act (PIPEDA)**: A federal legislation that governs how private companies and not-for-profit organizations engaging in commercial activities can handle personal information. PIPEDA came into force for federally regulated industries on January 1, 2001 and for all other companies and not-for-profit organizations engaged in commercial activities in Canada on January 1, 2004.

## Purpose of Legislation

FIPPA s.1 / MFIPPA s.1

The legislation begins with stated purposes:

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, and
- 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.

In the context of providing advice or decision-making, Coordinators should consider the purpose of the legislation in their analysis.

## Access and Privacy Principles

The legislation is principle-based. The legislation balances the rights and needs of individuals and institutions by weighing different considerations against each other.

From an access perspective, balance is achieved by providing individuals with the general right to access government records subject to limited and specific exemptions and exclusions.

From a privacy perspective, balance is achieved by protecting personal information in terms of:

- What and how personal information is collected, used, disclosed, and managed by government; and
- Providing access to a requesters own personal information in certain circumstances.

Access and privacy rights are not absolute. The facts of each situation, including the interests of the institution, individuals and the public, determine how the legislation applies and the final outcome of requests.

## Organization of Legislation

FIPPA and MFIPPA are considered substantially similar laws and are organized the same way. The main parts of the legislation and content are summarized below.

**Definitions and Interpretation:** Defines terms for the purpose of interpreting the legislation.

**Administration:** This part appears only in FIPPA, but applies to MFIPPA. This part addresses the designation of the Responsible Minister for the legislation and the establishment of the Office of the Information and Privacy Commissioner.

**Freedom of Information:** Addresses the right of access to records, exemptions, procedures for handling a request, and information to be published.

**Protection of Individual Privacy:** Addresses the collection, use, disclosure and disposal of personal information; and an individual's right to access and correct personal information about them.

**Appeal:** Addresses appeal rights, and procedures for mediation and appeals.

**General:** Addresses other administrative matters including fees, regulations, exclusions, and available information.

**Regulations:** Addresses specifics of the legislation, and rules and procedures that must be implemented. The regulations also list institutions covered by FIPPA and MFIPPA.

## Interactions with Other Laws

The legislation should be read and interpreted together with other applicable laws. Interactions with other laws can be the result of:

- Laws from other jurisdictions, including Federal laws;
- Laws that prevail over FIPPA and MFIPPA; and
- Laws that include confidentiality requirements.

Coordinators should work with Legal Counsel to become familiar with the laws that may govern specific institution or program requirements or general government administrative requirements.

## Prevailing Legislation

FIPPA s. 67 / MFIPPA s. 53

The general rule is that FIPPA or MFIPPA prevail over any other Ontario legislation. However, the legislation lists a number of laws that prevail over FIPPA and MFIPPA.

Other laws must expressly state that it prevails over FIPPA or MFIPPA. If a statute has a confidentiality provision that prevails over FIPPA or MFIPPA, it can prevent an institution from providing access to a record.

Consult the current versions of FIPPA and MFIPPA published on e-laws for a current list of laws that have been identified that prevail over FIPPA and MFIPPA.

## Copyright Act

The Canadian Copyright Act protects creative endeavours by ensuring that the creator has the sole right to authorize their publication, performance, or reproduction. Copyright applies to all original:

- Literary or textual works: books, pamphlets, poems, computer programs;
- Dramatic works; films, videos, plays, screenplays and scripts;
- Musical works: compositions consisting of both words and music, or music only;
- Artistic works: paintings, drawings, maps, photographs, and sculptures; and
- Architectural works.

The Copyright Act authorizes making a copy of a record for the purpose of giving access to a record under FIPPA or MFIPPA. The person who is given access to a record under the legislation is still bound by copyright.

Copyright may apply to records of third parties submitted to an institution or records created by an institution.

Where the Ontario Government creates a record, Crown copyright is indicated by Queen's Printer for Ontario.

## Litigation

FIPPA s. 64 / MFIPPA s. 51

Coordinators may be required to respond to an access request relating to matters in litigation. The legislation cannot be used to withhold information that is required to be produced by law for the purpose of litigation or a matter before an administrative tribunal. Coordinators should work with Legal Counsel to obtain legal advice on this type of request.

## Resources

Freedom of Information and Protection of Privacy Act

FIPPA, R.R.O. 1990, Regulation 459, Disposal of Personal Information

FIPPA, R.R.O. 1990, Regulation 460, General

Municipal Freedom of Information and Protection of Privacy Act

MFIPPA, R.R.O. 1990, Regulation 823, General

MFIPPA, Ontario Regulation 372/91, Institutions

Personal Health Information Protection Act

Personal Information Protection and Electronic Documents Act

Information and Privacy Commissioner of Ontario - Main Page

IPC: Ontario's FIPPA: A Mini Guide

IPC: Ontario's MFIPPA: A Mini Guide

# Chapter 2: Government Roles and Responsibilities

## Introduction

Accountability and oversight is set out in the legislation and makes each institution responsible for complying with the provisions of the legislation and establishes that a Responsible Minister has specified duties. This chapter summarizes the roles and responsibilities of the Responsible Minister, MGCS staff, MGCS Legal Counsel, and the IPC.

The concepts of an institution, a head of an institution, and how responsibilities can be assigned through a formal Delegation of Authority are explained.

Responsibilities of Coordinators and their staff are discussed in Chapter 3: Coordinator Roles and Responsibilities.

## Responsible Minister

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

The MGCS Minister is currently the designated minister of the Crown responsible for both FIPPA and MFIPPA. The Responsible Minister is designated by the Lieutenant Governor in Council. The Responsible Minister's main responsibilities are set out below.

**Internal oversight:** Promote compliance with the legislation and regulations; and address matters of public interest. The Responsible Minister provides advice to Cabinet and institutions and responds to the IPC's annual report.

**Amend and update the legislation and regulations:** Ensure the legislation and regulations are reviewed for effectiveness and accuracy. The Responsible Minister also ensures external and internal stakeholders are consulted as necessary to proposed amendments and updates.

**Provide approvals where required by the legislation:** Ensure that institutions comply with the legislation and regulations in a consistent manner by reviewing and approving requests from institutions on proposed program initiatives.

**Publications:** Ensure that publications required to be made available under the legislation are publicly available. For example, the Responsible Minister is responsible for publishing the Directory of Institutions for all institutions covered by FIPPA and MFIPPA and the Directory of Records for Ontario Public Service ministries.

## Policy and Legal Support

MGCS staff and MGCS Legal Counsel support the Responsible Minister, institutions and Coordinators in carrying out their responsibilities under the legislation. Legal advice can only be provided by Legal Counsel. The primary responsibilities of MGCS staff and MGCS Legal Counsel are listed below:

**Support the Responsible Minister:** Ensure the Responsible Minister meets his or her obligations under the legislation and exercises his or her statutory decision-making responsibilities by preparing briefing notes, speaking notes, correspondence, and media responses.

**Amend and update the legislation and regulations**: Review the effectiveness and accuracy of the legislation and regulations. They provide policy analysis and research, and coordinate and develop materials to support amendments to the legislation and regulations.

**Stakeholder engagement**: Address matters of public interest raised by internal and external stakeholders such as institutions, the IPC, and the public. They undertake consultations as necessary, participate in federal-provincial-territorial access and privacy committees, and lead communities of practice for Coordinators, Legal Counsel, policy, and technology professionals.

**Advice and policy direction:** Support institutions in the administration of the legislation and understanding of relevant policies. They respond to inquiries from institutions and members of the public. They develop policies, guidelines, tools and resources to advance access and privacy.

**Education:** Share information and resources and provide training to institutions about the legislation and administering the legislation.

**Publications:** Ensure the Responsible Minister meets his or her obligations to publish the Directory of Institutions and the Directory or Records. They provide direction to institutions and coordinate publication.

**Annual report:** Review compliance statistics of ministries and undertake special projects to respond to annual report of the IPC.

## Information and Privacy Commissioner of Ontario

FIPPA s. 4, s. 5, s. 6, s. 7, s. 8, s. 9

The Commissioner is an Officer of the Legislature and is independent of the executive branch of government. The Commissioner is appointed by the Lieutenant Governor in Council with the approval of the Legislative Assembly. The Commissioner is appointed for a five-year term and is eligible for reappointment.

The legislation sets out requirements for the IPC's office and staff, but the office establishes its own internal processes and timelines. The IPC's main responsibilities are:

**External oversight:** Ensure that government organizations comply with the legislation. They provide advice and comments on proposed government legislation and policies.

**Education:** Educate the public and institutions about Ontario's access and privacy laws. They publish a variety of resources for the public, organizations and professionals, and conducts research.

**Appeals:** Hear and resolve appeals from refusals to provide access to information, develops appeals processes, and issues orders on the decision of the appeal.

**Privacy investigations**: Investigate privacy complaints made by individuals regarding improper collection, use, or disclosure of their personal information, investigate self-reported privacy breaches, and conduct Commissioner initiated investigations into possible privacy breaches. The IPC can issue public investigation reports with recommendations and can order institutions to destroy personal information that was not collected in accordance with the legislation.

**Annual report:** Table an annual report in the Legislature which includes information about institutions' compliance with FIPPA, MFIPPA and PHIPA and recommendations about the practices of specific institutions and proposed revisions to FIPPA, MFIPPA and PHIPA. The annual report is normally published in the spring of each year.

## Coverage under the Legislation

The legal term for organizations covered by the legislation is "institution". Each institution is a separate entity responsible for administering the legislation.

Provincial and municipal institutions are defined differently. Institutions are either defined in the legislation or listed individually under the regulations.

## Provincial Institutions

FIPPA s. 2, Reg. 460

FIPPA defines institution as:

- The Assembly;
- A ministry of the Government of Ontario;
- A service provider organization within the meaning of section 17.1 of the Ministry of Government Services Act;
- A hospital; and
- Any agency, board, commission, corporation or other body designated as an institution in the regulations.

FIPPA defines educational institutions as:

- A college of applied arts and technology or a university.

Colleges are listed under the regulation as one entry ("Colleges of Applied Arts and Technology"). Universities are listed individually in the regulations.

FIPPA defines hospitals as:

- A public hospital within the meaning of the Public Hospitals Act;
- A community health facility; within meaning of the Oversight of Health Facilities and Devices Act; and
- The University of Ottawa Heart Institute.

## Service Provider Organizations

FIPPA s. 65.1

The Ministry of Government Services Act established entities known as "Service Provider Organizations."

Service provider organizations are not institutions under the legislation; however the legislation establishes rules for how they must operate when providing a service on behalf of the Government or a public body, including how they manage customer service information and personal information.

Examples of service provider organizations and functions are ServiceOntario in the MGCS, and government assistance programs under the Ministry of Revenue Act.

## Municipal Institutions

MFIPPA s. 2, Reg. 372/91

MFIPPA defines an institution as:

- A municipality;
- A school board, municipal service board, city board, transit commission, public library board, board of health, police services board, conservation authority, district social services 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, 2001 or the City of Toronto Act, 2006 or a predecessor of those Acts; and
- Any agency, board, commission, corporation or other body designated as an institution in the regulations.

Other MFIPPA agencies, boards, commissions, corporations or other bodies not listed in the definition may be considered part of a municipality and fall under the authority of the council of the municipality.

The relationships between organizations and whether an organization is an institution or covered under MFIPPA may not be clear. Issues relating to coverage should be discussed with Legal Counsel.

## Listing of Institutions and Regulation Updates

As noted above, institutions are either covered under the legislation by definition or by being listed under regulation. The process for updating the regulations is coordinated by MGCS staff.

MGCS staff coordinate with provincial and municipal institutions to ensure that the listing of institutions is up to date. Amendments to the regulations may include:

- The addition of new institutions;
- The renaming of institutions or heads of institutions; and
- The deletion of institutions.

Coordinators should become familiar with institutions under the regulations that are related to their institution. Coordinators should advise MGCS staff of any changes to the list of institutions.

## Exceptions to Coverage

The legislation does not apply to some public sector organizations. These organizations include:

- Some records of the Legislative Assembly;
- Constituency Offices; and
- Courts.

The sections below will provide more information.

### Legislative Assembly

FIPPA has limited application to the Legislative Assembly and does not apply to Independent Officers of the Legislative Assembly.

The definition of institution includes the Legislative Assembly, but only in respect to records of expense claims of ministers, opposition leaders and their respective staff under the authority of the Politicians' Expense Review Act, and in respect to the personal information contained in these records.

As such, FIPPA does not apply to the following offices:

- Auditor General of Ontario;
- Environmental Commissioner;
- Financial Accountability Officer;
- French Language Services Commissioner;
- Information and Privacy Commissioner of Ontario;
- Integrity Commissioner.
- Ombudsman of Ontario; and
- Provincial Advocate for Children and Youth;

### Member of Provincial Parliament Constituency Offices

The constituency offices of Members of Provincial Parliament (MPP), including ministers, are not covered by FIPPA because they are not part of an institution.

The records of MPPs that relate to ministerial work may be subject to FIPPA.

For example, the policy recommendations related to education reform in the office of the Minister of Education would be subject to FIPPA; however, records related to individual constituents of the same official would not be subject to FIPPA.

### Courts

The courts and the judiciary are not considered part of any ministry and therefore not included in the definition of institution. The role of the judiciary is set apart from government.

### Municipal Councillors' Records

Generally, the legislation does not apply to the records of municipal councillors that relate to their constituents and their private political activities.

However, records of municipal councillors may be subject to the legislation when:

- A councillor is acting as an officer or employee of the municipality, or performs a duty assigned by council, such that they might be considered part of the institution; or
- The records are in the custody or control of the municipality.

Examples of when a municipal councillor may be acting as an officer of the municipality include when a councillor participates on a municipal committee or board or exercises administrative or management functions on behalf of the municipality.

## Head of an Institution

The "head" of an institution is the legal term that refers to the official accountable and responsible for:

- Overseeing the administration of the legislation;
- Ensuring compliance with the legislation and regulations; and
- Making decisions regarding the legislation.

While the legislation refers to responsibilities of the head, responsibilities can be carried out by other positions in an institution through a Delegation of Authority discussed below.

### FIPPA

The head for Ontario ministries is the minister of the Crown who presides over a ministry.

For institutions that are designated under the regulation, the regulation also indicates the officer designated as the head. The minister responsible for an agency is usually the

head. In some cases, a senior executive such as a President or Chair may be designated as the head of an agency, board, or commission.

For public hospitals, the head is defined as the Chair of the Board; and for community health facilities the head is defined as the Superintendent.

For colleges, the head is defined as the Chair of the Board; and for universities, the head is defined as the Executive Head.

### MFIPPA

Under MFIPPA, the head is the council of a municipality or the board of a local board unless they choose to designate as head an individual or sub-group from among themselves. Examples of designations may include the mayor, a warden, a councillor, a special committee or a board member.

The designation must be in writing and in the case of a municipal council; it should be set out in a by-law.

See Appendix 1 for a sample draft by-law designating a head under MFIPPA. See Appendix 2 for a sample resolution designating a head under MFIPPA.

## Delegation of Authority

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

The legislation allows the head of an institution to delegate some or all powers and duties to an officer or officers of an institution or to another institution. This is known as a “Delegation of Authority” (DOA). It is through a DOA that many Coordinator responsibilities are formalized.

A DOA is a legal document and should clearly identify the duties and functions being delegated regarding access and privacy. The responsibility that is usually delegated is decision-making. However, the head of an institution remains accountable for all decisions made and actions taken.

The process for developing a DOA should involve the head of an institution, Legal Counsel, and all delegated decision-makers in order for all parties to fully understand their responsibilities. The DOA should be reviewed regularly and kept up-to-date.

See Appendix 3 for a sample DOA.

## Conflict of Interest

The DOA should include alternate decision-makers where there is a possible conflict of interest. A conflict of interest may be real or can reasonably be assumed. A conflict of interest may exist where:

- A public official knows they have a private interest connected to their public duties, or
- A public official may be perceived to be making decisions based on a personal or private interest rather than the public interest.

# Offences and Liability

FIPPA s. 61, s. 62 / MFIPPA s. 48, s. 49

The legislation includes offences or consequences for intentionally contravening some of its rules.

If an offence is committed, individuals, institutions and employees can be liable for fines up to $5,000.

Offences listed under the legislation include willfully and knowingly:

- Disclosing personal information in a manner that is not authorized;
- Maintaining a secret personal information bank that contravenes the legislation;
- Making a request for access to or correction of personal information under false pretenses;
- Altering, concealing or destroying a record, or the information contained in the record, with the intent to evade access to information requests;
- Causing another individual to alter, conceal or destroy a record, or the information contained in a record, with the intent to evade access to information requests;
- Obstructing the IPC's performance of its duties; and
- Misleading the IPC, or failing to comply with an order of the IPC.

A prosecution for an offence under the legislation must commence within two years of discovery of evidence of the offence. The consent of the Attorney General must be sought before a prosecution can occur.

Employees of an institution are protected against civil actions and liabilities when they are acting in good faith.

## Recordkeeping

FIPPA s. 10.1 / MFIPPA s. 4.2

The legislation requires that reasonable measures are developed, documented and put into place in order to preserve the organization's records in accordance with the recordkeeping rules that apply to the organization. An organization's rules can be established either by policy, by-law or law.

The records of an institution serve as evidence of government activities and transactions. Managed properly, information provides authoritative and trustworthy evidence and provides proof of government decisions and accountability for those decisions.

Good records management also supports compliance with the legislation.

## Resources

Appendix 1 Sample Municipal By-law for Appointing a Head under MFIPPA

Appendix 2: Sample Resolution Appointing a Head under MFIPPA

Appendix 3: Sample Delegation of Authority

MGCS: Recordkeeping Amendments to FIPPA and MFIPPA – Information Sheet

IPC: FIPPA and MFIPPA: Bill 8 – The Recordkeeping Amendments

IPC: MFIPPA and Councillors' Records

IPC: Improving Access and Privacy with Records and Information Management

# Chapter 3: Coordinator Roles and Responsibilities

## Introduction

Coordinators across institutions share common roles and responsibilities. The manual is designed to help Coordinators develop the foundation of knowledge and skills required to administer the legislation.

There are various aspects to the Coordinator's position which may vary depending on institutional factors such as:

- The institution's mandate and size;
- The Delegation of Authority;
- The position of the Freedom of Information and Privacy Office within the institution;
- The number and complexity of access requests;
- The volume and sensitivity of personal information holdings; and
- Stakeholder relations.

Coordinators will need to build and maintain a network of internal and external contacts. For provincial ministries internal stakeholders could include the Minister's Office, Deputy Minister's Office, Legal Counsel, program areas, and communications staff.

For municipalities internal stakeholders could include the City Clerk, municipal councillors, Legal Counsel, program areas, and communications staff.

External stakeholders for all institutions could include individual requesters, the general public, the IPC, other institutions and other governments.

## Overview of Roles and Responsibilities

The Coordinator's responsibilities cover a broad range of access and privacy activities. More details on specific responsibilities and activities are provided throughout this manual.

In most cases, the Coordinator's main roles include:

- Management – administering or supervising the operations of the freedom of information and privacy program.
- Coordination - organizing the various parts of an activity to enable collaboration and efficient communication.

- Advisory - giving information or advice or a recommendation about what should be done.
- Training and awareness – teaching and raising awareness of access and privacy responsibilities.

## Administration

The Coordinator may be responsible for a variety of administrative activities to support the request process and the day-to-day operations of the office. Administrative considerations may include:

- Human resources – hiring and managing staff;
- Office accommodation and record storage – secure space for handling, reviewing and storing records, and dealing with the public;
- Equipment (e.g., phones, computers, fax machine, copier, scanner, projectors);
- Technology (e.g., email, software for severing records, tracking, website);
- Payment processing; and
- Mail and courier services.

## Policies and Procedures

Coordinators develop various policies and procedures to support operational efficiency. Examples of subjects that policies and procedures will need to address include:

- The institution's Delegation of Authority;
- Routine requests;
- Handling sensitive information;
- Publication of records;
- Conducting privacy impact assessments;
- Responding to privacy breaches; and
- Rules for collecting, using and disclosing personal information.

## Processing Requests

Coordinators need to have defined procedures for processing access requests. Procedures should address all aspects of responding to a request including:

- Contacting the office (e.g., phone, mailing address, internet, email);
- Handling inquiries;

- Handling incoming requests and correspondence;
- Processing applications and fees;
- Searching and reviewing records;
- Providing notice to affected parties;
- Conducting research on IPC orders and case law;
- Obtaining legal advice;
- Documenting decisions and recommendations;
- Preparing copies and records for release;
- Reviewing work for accuracy;
- Issues management;
- Obtaining approvals; and
- Packaging and sending records.

More information on processing requests can be found in Chapter 6: Managing the Request Process.

## Case File Management and Reporting

Coordinators must manage request case files and collect data regarding the administration of the legislation. Coordinators may use electronic databases or manual systems to manage and track requests. Effective case file management enables:

- Management of work load and assignments relating to files, appeals, and projects;
- Tracking the status of individual requests and appeal files;
- Information and records management relating to all of the office and request records;
- Tracking the stages and status of responses to privacy breaches and investigations.
- Reporting to senior management; and
- Annual reporting to the IPC.

## Research

Coordinators must conduct research to inform analysis of application of the legislation and to stay current on issues and trends. The following list includes some areas that coordinators may consult as part of the research activity:

- IPC orders and privacy investigation reports, and case law;
- IPC access and privacy resources;

- MGCS access and privacy resources;
- Corporate directives, policies, guidelines and standards in your organization;
- Media reports; and
- Relevant resources and trends in other jurisdictions.

## Mediation and Appeals

Coordinators are involved in some or all parts of the intake, mediation or adjudication stages of the IPC appeal process. This may include the following activities:

- Preparing relevant records for an appeal to the IPC;
- Representing the institution at all stages of the appeal process;
- Conducting in-depth research of IPC orders and case law;
- Obtaining legal advice and legal representation;
- Obtaining affidavits;
- Preparing representations; and
- Presenting the institution's position to the IPC.

More information on IPC appeals can be found in Chapter 11: Appeals Process.

## Issues Management

Coordinators should ensure Senior Management and decision makers are aware of any contentious issues that may arise from received requests or privacy matters. This may include the following activities:

- Providing "heads up" notifications to Senior Management and other offices within the institution involved with communications and issues management when contentious requests are received;
- Providing status updates and briefings to Senior Management as contentious requests are processed; and
- Alerting Senior Management of any contentious issues that may occur in relation to the institution's privacy practices.

For more information on considerations for processing contentious requests, see Chapter 6: Managing the Request Process.

## Publications

Coordinators should ensure that publication requirements under the legislation are met. Publication requirements include:

- Directory of Institutions and Directory of Records; and
- Institution documents available for public review (e.g., public records, manuals, directives).

More information on the Directory of Institutions and the Directory of Records can be found in Chapter 4: Access Fundamentals.

## Resources

IPC: Backgrounder for Senior Managers and Information and Privacy Coordinators, Raising the Profile of Access and Privacy

IPC: Basics for Freedom of Information Coordinators

# Part II: Freedom of Information

# Chapter 4: Access Fundamentals

## Introduction

The legislation provides a general right of access to government information, subject to certain exclusions and exemptions. This chapter introduces the definition of records, how to understand custody and control of records, and third party records. The sections of the legislation that limit and support access to information are explained.

The main topics covered in this chapter include classes of information excluded from the legislation (called “exclusions”), mandatory and discretionary exemptions to the right of access, information available to the public, and disclosure obligations. The exercise of discretion, harms tests, and the public interest override are also covered.

Chapter 5: Exemptions and Exclusions explains how exclusions and exemptions are interpreted and applied to records. More detail on how requests are processed and managed is discussed in Chapters 6: Managing the Request Process.

## Applying the Legislation

In responding to requests made under the legislation, Coordinators take the following basic steps to assess how the legislation applies within the context of each individual access request:

1. Determine if the individual is seeking access to a record.
2. Determine if the records are in the custody or control of the institution.
3. Determine the relevant sections of the legislation that might apply to a record (in whole or in part).
4. Determine if the criteria and tests for each relevant section of the legislation are met.
5. Determine if additional legal tests apply and the criteria are met.

The background and considerations for each step are discussed below.

## Understanding Records

FIPPA s. 2 / MFIPPA s. 2

Individual’s access rights apply to records or parts of records. Record is defined as any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, and includes:

- Books
- Correspondence
- Diagrams
- Documentary material
- Drawings
- Films
- Maps
- Memorandums
- Microfilms
- Plans
- Pictorial and graphic work
- Photographs
- Sound recordings
- Videotapes

The definition is broad and is interpreted to include records that are not completed (e.g., working drafts) and recorded information using current technologies (e.g., voicemail, email). The definition also includes copies and any records that can be produced by computer hardware and software or any other equipment.

In general, the legislation applies to an existing record regardless of whether it was created prior to the legislation taking effect. Hospitals are an exception to this rule because the legislation only applies to records that came into the custody or control of hospitals on or after January 1, 2007.

## Creating Records

Reg. 460 (2) / Reg. 823 (1)

In instances where institutions receive a request for information that may reside in an institution, but not as a record, the Coordinator must determine the feasibility of producing the record. For example, if the information resides in a database.

The legislation does not explicitly require an institution to create a record but there may be situations where it is effective to do so. There is a growing expectation that government use of information technology should facilitate, not limit, public access to information.

Under the regulations a record capable of being produced from machine readable records is not included in the definition of record where the process of producing it would unreasonably interfere with the operations of an institution.

Factors Coordinators should consider when establishing unreasonable interference may include:

- Number of hours required to produce the record;
- Number of staff required to undertake the work and the impact on their regular duties and responsibilities;
- Technical expertise required (e.g., consultant); and
- The impact on the institution's operations and resources (e.g., disruption, delay, hinder effectiveness).

Where the institution is capable of producing a record and the production of the record would not interfere with the operations of the institution then the produced record would qualify as a record under the legislation.

## Custody or Control

The right of access only applies where the records, in whole or in part, fall within the custody or control of an institution.

- Custody means the keeping, care, watch, preservation or security of the record for a legitimate business purpose.
- Control means the power or authority to make a decision about the creation, use, disposal or disclosure of the record.

There are a number of factors that can be considered to determine custody and control.

### Custody

Questions Coordinators' should consider when determining whether the institution has custody of a record include:

- Does the institution have physical 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 purposes of his or her duties as an officer or employee?

These questions are relevant for personal records of an employee that happen to be physically located in the office of an institution. While the record may be physically in the office, if the record does not relate to the employee's duties as an employee they may not be considered in the custody of the institution. For example, generally speaking, an

employee's personal dry cleaning receipt or personal telephone bill would not be considered in the custody of the institution as they do not relate to the employee's duties.

### Control

Questions Coordinators' should consider when determining whether the institution has control of a record include:

- Was the record created by an officer or employee of the institution?
- Does the record relate to the statutory or core business of the institution?
- What use did the creator intend to make of the record?
- Does the institution have a right to possession of the record?
- Does the institution have the authority to regulate use and disposal of the record?
- To what extent has the institution relied upon the record?
- How closely is the record integrated with other records held by the institution?

Coordinators should be familiar with the business and records of the institution, as well as how business is conducted and information is managed.

## Records of Third Parties

Institutions may legitimately obtain or have copies of records of third parties that are within their custody or control. A third party can be any one of the following:

- Person;
- Group;
- Committee;
- Organization;
- Other government; or
- Business.

An employee of an institution is not a third party unless acting in a personal capacity.

Government business and service delivery may result in institutions having custody or control of third party records. Some common examples where government institutions may have custody or control of third party records include:

- Records that have been provided under legislated and regulatory requirements;

- Records including the personal information of individuals applying for benefits or services;
- Records collected as part of a procurement of products or services;
- Records containing expert and legal advice,
- Records gathered during public consultations,
- Records created through federal-provincial-municipal initiatives, and
- Records created through public-private sector partnerships.

Key questions Coordinators may ask to determine whether the institution has custody or control of records of third parties include:

- Who owns the record?
- Who paid for the creation of the record?
- What are the circumstances surrounding the creation, use and retention of the record?
- Is there a contract between the institution and the organization or individual who created the record?
- Was the individual who created the record an agent of the institution for the purposes of the activity in question?
- What is the customary practice of the individual who created the record in relation to possession or control of records of this nature, in similar circumstances?

## Notice to Affected Persons

There are additional requirements for processing requests for access to records that contain information about third parties such as providing notice and obtaining consent where applicable.

Institutions should consider developing a policy or procedure for when third party information is frequently requested.

More information on notice requirements are provided in Chapter 6: Managing the Request Process.

## Applying Relevant Sections

In processing requests, Coordinators must review responsive records to determine if any exclusion or exemption applies to a record, either in whole or in part.

Exclusions and exemptions of the legislation are categorized based on their purpose in regard to limiting or supporting access to records. Each of these categories will be discussed further below.

**Exclusions:** These are provisions which exclude records or parts of records from the application of the legislation.

**Exemptions (general):** These are provisions which exempt records or information from the general right of access. The legislation applies to a record but access can be denied.

> **Mandatory exemption**: If a mandatory exemption applies the head must refuse access to the record unless it has consent to disclose it. In the legislation, mandatory exemptions begin with the words “shall refuse.”
>
> **Discretionary exemption:** An exemption where the head may choose to deny access to a record, but is not required to do so. In the legislation, discretionary exemptions begin with the words “may refuse.”

In order to determine the relevant sections of the legislation that apply to a record, the content and context of a record are important factors. Coordinators may ask the following questions to assess the content and context of the record:

- Who prepared the record?
- What is the purpose of the record?
- Who is the intended audience?
- What is the age of the record?
- What type of information is in the record?
- How sensitive is the information?
- How was the record shared (e.g., internally or publicly)?

## Exclusions

Exclusions mean that the legislation does not apply to certain types or classes of records. Exclusions are intended to be limited in scope. The exclusions do not apply to all institutions equally. Some exclusions are specific to universities, colleges or hospitals.

The legislation does not prevent access to excluded records. If an institution decides to release an excluded record, it can do so “outside” of the legislation. However, this approach means that other rights (e.g., appeal rights) are not available to the requester.

The list below outlines the exclusions and to what institutions they apply:

**Private donations to archives**: Excludes records that have been donated to a public archive by a non-institution such as a private individual, corporation or association. This exclusion applies to the Archives of Ontario and archival repositories in colleges, universities and municipal institutions. FIPPA s. 65 (1) and MFIPPA s. 52 (2).

**Proceedings before a Court:** Excludes records prepared for a person presiding in a proceeding in a court of Ontario such as a judge. This exclusion applies to the Courts. FIPPA s. 65 (3).

**Performance evaluations of judges:** Excludes records and information related a judge’s performance evaluation. This exclusion applies to provincial institutions only. FIPPA s. 65 (4).

**Ontario Judicial Council records:** Excludes records of the Ontario Judicial Council that are deemed confidential, not made available to the public or relate to a proceeding that did not occur in the public. This exclusion applies to provincial institutions only. FIPPA s. 65 (5).

**Case management master investigations:** Excludes records related to investigations into complaints against case management masters under the Courts of Justice Act. This exclusion applies to provincial institutions only. FIPPA s. 65 (5.1)

**Prosecution records:** Excludes records related to prosecutions where all matters related to the prosecution have not been completed. This exclusion applies to all provincial and municipal institutions. FIPPA s. 65 (5.2) and MFIPPA s. 52 (2.1).

**Ecclesiastical records:** Excludes the records of church or religious organizations affiliated with an education institution or hospital. The exclusion applies only to hospitals, universities and colleges. FIPPA s. 65 (5.3).

**Hospital foundations:** Excludes records of hospital foundations, even when in the custody of hospitals. This exclusion applies only to hospitals. FIPPA s. 65 (5.4).

**Administrative records of health professionals:** Excludes records of health professionals using hospital offices for personal practice. This exclusion applies only to hospitals. FIPPA s. 65 (5.5).

**Charitable donations:** Excludes records related to charitable donations to hospitals. This exclusion applies only to hospitals. FIPPA s. 65 (5.6).

**Labour relations and employment-related:** Excludes the majority of records related to labour relations and employment. This exclusion applies to all provincial and municipal institutions. FIPPA s. 65 (6) and MFIPPA s. 52 (3).

**Church or religious appointments of individuals:** Extends the employment records exclusion to religious appointees in institutions. The exclusion only applies to all provincial institutions. FIPPA s. 65 (6) 4.

**Hospital appointments of persons with privileges:** Extends the employment records exclusion to doctors who have privileges at a hospital. This exclusion applies to hospitals only. FIPPA s. 65 (6) 5.

**Adoptions related:** Excludes certain records related to adoptions. This exclusion applies to all provincial institutions. FIPPA s. 65 (8).

**Research and teaching materials:** Excludes records related to research and teaching materials for individuals employed or associated with a college, university or hospital. The exclusion applies only to colleges, universities and hospitals. FIPPA s. 65 (8.1).

**Peer evaluations of research and teaching materials:** Excludes records related to peer evaluation of research and teaching materials of individuals employed or associated with a college, university or hospital. The exclusion applies only to colleges, universities and hospitals. FIPPA s. 65 (10) s. 49 (c.1).

**Medical assistance in dying:** Excludes identifying information of individuals and facilities associated with services related to medically assistance in dying. FIPPA s. 65 (11).

**Abortion related services:** Excludes identifying information of individuals and facilities associated with services related to abortion services. It applies to all provincial institutions. FIPPA s. 65 (13) (14) and (15).

## Mandatory Exemptions

In general, a record that falls under a mandatory exemption cannot be disclosed unless the institution obtains the consent of the affected party. In the legislation, mandatory exemptions start with “shall refuse”.

A notable difference between the municipal and provincial legislation is that MFIPPA has a mandatory exemption for relations with other governments and FIPPA has a discretionary exemption for relations with other governments.

The four mandatory exemptions are listed below.

**Cabinet records:** Protects the substance of deliberations of Executive Council or its committees. FIPPA s. 12.

**Personal privacy:** Protects against an unjustified invasion of privacy of an individual other than the requester. FIPPA s. 21, MIFPPA s. 14.

**Relations with other governments:** Protects confidential information received from other Canadian and foreign governments. MFIPPA s.9. Note: a similar exemption is discretionary under FIPPA.

**Third party information:** Protects third parties from financial or other harms. FIPPA s. 17, MFIPPA s. 10.

## Discretionary Exemptions

A discretionary exemption means that refusing access to a record is permitted, but not required. In the legislation, discretionary exemptions begin with the words “may refuse”. In general, a decision to refuse access to a record requires further analysis known as an exercise of discretion discussed below. It involves weighing the pros and cons of providing access to a record or not.

Most of the discretionary exemptions are common to both FIPPA and MFIPPA. However, the discretionary exemptions specific to FIPPA are:

- Defence;
- Government relations; and
- Species at risk.

The discretionary exemption specific to MFIPPA is draft by-laws and records of closed meetings.

The discretionary exemptions and their main purpose are listed below.

**Draft by-laws and records of closed municipal meetings:** Protects deliberations in closed meetings or draft by-law. MFIPPA s.6.

**Advice to government/Advice or recommendations:** Protects records or parts of records containing advice or recommendations used in government decision-making. FIPPA s. 13, MFIPPA s. 7.

**Law enforcement:** Protects various types of records and activities relating to law enforcement and security. FIPPA s. 14, MFIPPA s.8.

**Civil Remedies Act, 2001:** Protects records that if released could interfere with the Attorney General's ability to conduct a proceeding under the Civil Remedies Act. FIPPA s. 14.1, MFIPPA s. 8.1.

**Prohibiting Profiting from Recounting Crimes Act, 2002:** Protects records that if released could interfere with the Attorney General's ability to conduct a proceeding under the Prohibiting Profiting from Recounting Crimes Act, 2002. FIPPA s. 14.2, MFIPPA s. 8.2.

**Relations with other governments:** Protects confidential information received from other Canadian and foreign governments. FIPPA s.15. Note: a similar exemption is mandatory under MFIPPA.

**Relations with Aboriginal communities:** Protects confidential information received from Aboriginal communities. FIPPA s. 15.1, MFIPPA s. 9.1.

**Defence:** Protects records related to the national defence of Canada or a foreign state. FIPPA s.16.

**Economic and other interests of Ontario:** Protects records where disclosure could damage an institution's economic or other interests. FIPPA s.18, MFIPPA s.11.

**Closed meetings:** Provides universities and hospitals with similar confidentiality provisions in the deliberative processes of their respective governing bodies. FIPPA s. 18.1.

**Solicitor-client privilege:** Protects records subject to common-law solicitor-client privilege and litigation privilege. FIPPA s.19, MFIPPA s.12.

**Danger to safety or health:** Protects records that if released could cause serious threats to safety or the health. FIPPA s. 20, MFIPPA s. 13.

**Species at risk:** Protects information that if released could endanger species at risk or their habitat. FIPPA s.21.1.

**Information soon to be published:** Protects records that are published, currently available to the public, or will be published. FIPPA s.22, MFIPPA s.15.

## Exceptions

Some exclusions and exemptions include exceptions. Where the exception applies, the exclusion or exemption would not be applicable to the record.

Some exceptions relate to factual information that may be of interest or use to the public and specific types of records or reports produced in the course of government work. For example, in the advice to government/advice or recommendations exemption, subsection 2 lists a number of classes of records that the section does not apply to including: factual material, a statistical survey, a report by a valuator, and an environmental impact statement.

Other exceptions set time limits for when exemptions can be used. For example, in the Cabinet records exemption, subsection 2 (a) states that the exemption cannot be claimed on records more than 20 years old.

## Exercise of Discretion

When deciding not to disclose a record the factors and reasons for the exercise of discretion should be well documented to support the decision, in the event of an appeal.

The IPC has developed a list of considerations for a proper exercise of discretion. The factors include:

- The purpose of the legislation; including the principles that:
    - Information should be available to the public
    - Individuals should have a right of access to their own personal information
    - Exemptions from the right of access should be limited and specific
    - The privacy of individuals should be protected;
- The wording of the exemption and the interests it seeks to protect;
- Whether the requester is seeking his or her own personal information;
- Whether the requester is an individual or an organization;
- The relationship between the requester and any affected persons;

- Whether disclosure will increase public confidence in the operation of the institution;
- The nature of the information and the extent to which it is significant and/or sensitive to the institution, the requester, and any affected person;
- The age of the information; and
- The historic practice of the institution with respect to similar information.

In contrast, an improper exercise of discretion occurs when:

- It is done in bad faith or for an improper purpose;
- It takes into account irrelevant considerations; or
- It fails to take into account relevant considerations.

Where an institution makes an error in the exercise of discretion, the IPC may send the matter back to the institution to re-exercise discretion.

## Harms Test

Some exemptions in the legislation are harms-based. In order to apply these exemptions under the legislation, institutions or third parties may have to demonstrate the harms that could result in the disclosure of information.

In general, meeting the criteria of a harms test requires:

- Detailed and convincing evidence; and
- A strong connection between the harm and disclosure of the record.

More information on how harms tests are considered within the context of specific exemptions is discussed in detail in Chapter 5: Exemptions and Exclusions.

## Public Interest Override

FIPPA s. 23 / MFIPPA s. 16

The public interest override provision provides another opportunity to consider whether a record should be disclosed for some exempted records.

A two-part test determines whether public interest override applies to a record:

- There must be a compelling public interest; and
- The compelling public interest must clearly outweigh the purpose of the exemption.

This section of the legislation states that certain exemptions do not apply when a compelling public interest in the disclosure of a record clearly outweighs the purpose of the exemption.

This section is commonly referred to as public interest override. It cannot be applied to information withheld under the following exemptions:

- Cabinet records (FIPPA s. 12);
- Defence (FIPPA s.16);
- Draft by-laws, etc. (MFIPPA s. 6);
- Law enforcement (FIPPA s. 14, MFIPPA s. 8);
- Solicitor-client privilege (FIPPA s. 19, MFIPPA s. 12);
- Information soon to be published (FIPPA s. 22, MFIPPA s. 15).

Factors that Coordinators should consider when determining whether the public interest override applies include:

- Where there is a relationship between the record and the legislation's central purpose of shedding light on the operations of government?
- Where the record serves the purpose of informing the public to make political choices and express public opinion? or
- Whether the interest in the record is public or private.

Generally, a public interest does not exist where the requester's interests in a record are essentially private in nature.

## Available for Public Review

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

The legislation requires that the Responsible Minister and institutions make certain information available to the public for review to support:

- Public awareness of government information holdings;
- Public access to information outside of the formal information request process, and
- An individual's ability to contact institutions and request information.

## Institution Records

FIPPA s. 33

The legislation requires that certain records of institutions be available to the public for review. The requirement applies where records about the interpretation of laws and programs of the institution are necessary for the purpose of:

- Determining applications by individuals for rights, privileges or benefits;
- Changes to the provision or the new conditions of rights, privileges, or benefits already granted; and
- General administration or enforcement.

Other such records of institutions include manuals, directives, guidelines, instructions, procedures, objectives prepared for the officers of an institution. The publishing requirement does not apply to internal operations and administration of the institution (e.g., equipment manual).

The documents required for publishing are subject to the same exemptions under the legislation. Portions can be severed if they are exempt from disclosure under the legislation. Any severing or deletion must include a statement that a deletion has been made, the nature of the information deleted and the exemption applied.

These documents must be available for inspection and copying by the public, in these locations:

- On the Internet; or
- In a reading room, library, or designated office.

Available for public review does not imply the record is provided to the public at no cost. Fees may be associated with accessing certain institutional records.

## Directory of Institutions

FIPPA s. 31, s. 35, s. 36 / MFIPPA s. 24

The Directory of Institutions (DOI) is a compilation of all institutions covered by the legislation. The DOI sets out where a request for information should be made by providing the title, address and other contact information for the individual responsible for administering the legislation in the institution.

Publication of the DOI is a responsibility of the Minister and is coordinated by MGCS staff. The DOI is published every three years.

## Directory of Records

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

The Directory of Records (DOR) is a publication that provides:

- A description of the programs, functions or responsibilities of offices within an institution;
- Information on the general classes or types of records of each institution; and
- An index of the personal information banks maintained by each institution.

Publication of the DOR for Ontario Public Service ministries is a responsibility of the Minister and is coordinated by MGCS staff. The head of each provincial institution is responsible for providing this information to the Minister for publication.

Hospitals, universities, some provincial agencies and MFIPPA institutions are also required to make similar information available about their institution but do so independently.

### Personal Information Banks

FIPPA s. 44, s. 45 / MFIPPA s. 34

The index of Personal Information Banks (PIB) forms part of the DOR. A PIB is any collection or set of personal information where personal information is organized by:

- The individual's name;
- An identifying number or symbol; or
- Other particular identifier assigned to the individual.

A PIB could be an electronic database or a paper filing system.

The PIB index sets out the following for each PIB:

- Its name and location;
- Legal authority for its establishment;
- Types of personal information maintained in it;
- How the personal information is used on a regular basis;
- To whom the personal information is disclosed on a regular basis;
- Categories of individuals about whom personal information is maintained; and

- Policies and practices applicable to the retention and disposal of the personal information; and
- Exceptions to the uses and disclosures noted above.

## Routine Disclosure and Open Government

FIPPA s. 63 / MFIPPA s. 50

The legislation does not prevent institutions from providing information to the public through alternative means outside of the formal request process. Institutions may proactively make records available through routine disclosure or other initiatives.

"Open Government" refers to government programs aimed at improving public access to government information and data; and increased public participation in policy development and dialogue between individuals and the government.

The IPC is a strong supporter of Open Government as it enhances transparency of government actions and decisions, improves accessibility of government services and information, and promotes public participation.

Coordinators and Legal Counsel should participate in routine disclosure or Open Government initiatives to ensure that the information and raw data being published does not reveal personal information of identifiable individuals or other sensitive information.

## Obligations to Disclose

FIPPA s. 11 / MFIPPA s. 5

The legislation requires disclosure of a record that reveals a grave environmental, health or safety hazard to affected persons or the public, and where it is in the public interest.

This section overrides all other provisions of the legislation. There is no requirement that a request must be made before action is taken. While this section includes a notice provision to any person to whom the information relates, it must be practicable to do so. The record must be disclosed as soon as possible. Disclosure is to be made by announcement to the public generally or to those individuals that are particularly affected by the information in the record.

The following conditions must be met:

- The information must be in record form; and

- The situation must be grave meaning serious and likely to produce great harm or danger.

## Resources

MGCS: Directory of Institutions

IPC: Accessing Information

IPC: Open Government

# Chapter 5: Exemptions and Exclusions

## Introduction

As discussed in Chapter 4: Access Fundamentals, the legislation provides a general right of access to records in the custody or control of institutions, subject to limited and specific exemptions.

This chapter will review the exemptions to the right of access. Some exemptions exist only in FIPPA or MFIPPA. This guide will indicate the applicable legislation for each exemption.

The legislation also outlines a number of classes of records that are excluded from the legislation in their entirety. This chapter will review in detail these exclusions and indicate the applicable legislation for each exclusion.

This chapter does not identify all the interpretations or issues related to these exemptions and exclusions that have been considered by the IPC and the Courts. As such, this chapter is not meant to be exhaustive, but only to summarize how the exemptions and exclusions generally operate.

The law relating to the interpretation of these exemptions and exclusions is constantly evolving and it is up to individual reader to ensure that their understanding of a provision is up to date. Coordinators should always refer to the legislation for the exact language of a provision they are considering and not rely solely on the paraphrasing or descriptions of the provisions contained in this chapter.

## Exemptions

Exemptions to the general right of access are either mandatory or discretionary. The sections below will review each exemption and outline:

- The nature of the exemption;
- Any legal tests that may apply;
- Factors to consider in determining whether the exemption applies to a record;
- Any exceptions to the exemption that exist;
- Whether the public interest override applies to the exemption.

Note that a record may contain information subject to more than one exemption.

## Draft By-Laws and Closed Municipal Meetings

MFIPPA s. 6

### Draft By-Laws

The discretionary exemption protects draft by-laws or draft private bills that have not 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 cannot be applied to prevent their release.

### Closed Meetings

This discretionary exemption also protects from disclosure the deliberations at meetings of a council, board, commission, or other body, or a committee of any of those bodies made in camera (meaning in private or in absence of the public). For this exemption to apply, the in camera nature of the meeting must be authorized by a statute.

This exemption also permits the institution 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 that:

- A meeting was held in the absence of the public;
- A statute authorizes the holding of the meeting in the absence of the public; and
- Disclosing the record would reveal the actual substance of deliberations of the meeting.

The term "substance of deliberations" has been interpreted to mean more than the subject of the deliberations but instead the actual substance of the deliberations. The exemption has been found to not protect records that merely refer to matters discussed at the in camera meeting. For example, the exemption would not apply to names of attendees or dates, times, and locations of meetings.

A distinction, however, must 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, municipal councillors deliberated on the line items of a budget during an in camera meeting and later the consolidated budget was formally adopted at a public meeting. The consolidated budget was found by the IPC to be only the product of the subject matter of the deliberations in camera (regarding the line items), rather that the subject matter of the deliberations itself. Therefore, the deliberations about the line items in the budget were not found to have been "considered" at the public meeting, and were still subject to this exemption.

### Exceptions

For draft by-laws and private bills, this exemption does not apply where the draft has been later considered in open meetings.

With respect to in camera deliberations, if the subject matter of the deliberations is later considered in an open meeting, this exemption no longer applies to the record.

For both the draft by-law and the closed meetings, the exemption does not apply to records more than 20 years old.

### Public Interest Override

The public interest override does not apply to this exemption.

## Cabinet Records

FIPPA s. 12

This mandatory exemption protects deliberations of the Executive Council and its committees from disclosure. Deliberations have been interpreted as discussions conducted with a view towards making a decision.

The FIPPA exemption for Cabinet records applies to the Executive Council (Cabinet) or its committees including:

- Treasury Board/Management Board of Cabinet,
- Legislation and Regulations Committee, and
- Cabinet policy committees.

A current list of Cabinet policy committees can be found on the Ontario government's website.

Evidence that a record was either sent to Cabinet or its committees for its deliberation or was prepared with the specific intention of presenting it to Cabinet or its committees, is critical in determining if this exemption applies to a record.

In rare cases, records do not have to be directly sent to Cabinet or its committees to be exempt. Where the disclosure of records would permit a reader to draw an accurate inference concerning the substance of deliberations, the exemption would likely apply.

An institution has the right to claim the exemption even if the record was disclosed without the knowledge of the institution. However, where an issue or matter never gets to Cabinet or its committees and where there is no prospect that it ever will, the exemption cannot be claimed.

This exemption is broadly defined. Any record that would reveal the substance of deliberations at Cabinet or its committees is subject to the exemption. This section also provides a non-exhaustive list of types of records that are included in this exemption:

- An agenda, minute or other record of deliberations or decisions;
- Policy options or recommendations submitted or prepared for submission;
- Background explanations or analyses of problems submitted or prepared for submission for consideration before decisions are made and implemented;
- The subject of consultations among ministers on matters relating to government decision-making or the formulation of policy;
- Briefing materials for a minister in relation to matters before or proposed; or are the subject of consultations among ministers relating to government decision-making or the formulation of policy; and
- Draft legislation or regulations.

A discussion of policy options and recommendations (e.g., Cabinet submission) that is exempt under this section will continue to be exempt from disclosure even after the related decisions is made. Records about the implementation of a policy or recommendation that was previously approved may still include policies or recommendations and therefore may still be exempt.

Background explanations and analyses (e.g., briefing notes) must be submitted or prepared for submission to Cabinet in order to be exempt under this section. This type of background information is time limited and is only exempt until steps are taken to give effect to a decision.

Consultations among ministers may involve records such as memoranda to and from ministers, and minutes of meetings. Consultations among deputy ministers and public

servants are not exempt unless those consultations would reveal the substance of deliberation of Cabinet or its committees.

Briefing a Minister usually involves records prepared by an institution's staff or a minister's political staff. The reason why the record was prepared should be clear, and linked to matters currently before or proposed to be brought before Cabinet in order to claim the exemption.

Draft legislation and regulations are exempt from disclosure until the draft has been considered by Cabinet and Cabinet has consented to the public distribution of the draft for comment. A Minister can approve sharing draft statute and regulations with interested parties in the development process of the legislation.

## Exceptions

An institution must, on request, disclose a Cabinet record that is more than 20 years old.

Records that are 20 years old or less can be disclosed where the Cabinet for which the record was prepared gives consent. One Cabinet cannot consent to the release of another's records. A Cabinet is considered to have changed where there has been an election or a change of government. Consent of a previous government cannot be practically sought.

While an institution is not required to seek consent of a current Cabinet, it should consider the merits of seeking Cabinet consent in every case because it can be an issue raised on appeal. Whether to seek consent should take into consideration:

- The subject matter;
- If the government policy has been announced or implemented;
- If disclosure would reveal the nature of Cabinet discussion; and
- If the record has, in fact been considered by Cabinet.

## Public Interest Override

The public interest override does not apply to this exemption.

## Advice to Government/Advice or Recommendations

FIPPA s. 13 / MFIPPA s. 7

This discretionary exemption is called Advice to Government under FIPPA and Advice or Recommendations under MFIPPA. There are minor differences in wording between the two legislations.

Under FIPPA, the advice and recommendations must be given by a public servant, any person employed in the service of the institution, or a consultant retained by the institution. A consultant provides professional services under a formal agreement.

Under MFIPPA, the advice and recommendations must be given by an officer or employee of an institution, or a consultant retained by an institution. An officer is considered a high ranking individual in municipal government who has management and administrative functions. Municipal or city councillors are not officers.

A record continues to be exempt under this exemption, even if the institution has completed its decision-making, or acted on the recommendation at issue.

“Advice” and “recommendations” have two distinct meanings.

Recommendations refer to a suggested course of action that will ultimately be accepted or rejected by the person being advised. Recommendations can be expressed or inferred.

Advice has a broader meaning and can include “policy options.” This can include:

- Lists of alternative courses of action to be accepted or rejected in relation to a decision that is to be made;
- An employee’s identification and consideration of alternative decisions that could be made; and
- Views and opinions of an employee as to the range of policy options to be considered by a decision-maker, even if they do not include a recommendation.

If an accurate inference concerning advice and recommendations may be drawn from a record it would be exempt. The exemption applies to both draft documents that have not yet been given to decision-makers as well as finalized documents that have been delivered to decision-makers for consideration.

## Exceptions

This exemption sets out a number of exceptions that are not considered advice or recommendations. These exceptions ensure that factual information often found in reports is available to the public, if other exemptions do not apply to the records.

A report has been interpreted as a formal statement or account of the results of the collation and consideration of information. A report is not just observations or recordings of fact.

The following lists the types of information and reports that are exceptions to the exemption and may be disclosed (provided that they are not subject to other exemptions):

- Factual material;
- A statistical survey;
- A report by a valuator;
- An environmental impact statement or similar record;
- A report of a test carried out on a product for the purpose of government equipment testing or a consumer test report (FIPPA only);
- A report or study on the performance or efficiency of an institution;
- A feasibility study or other technical study;
- A report containing the results of field research;
- A final plan or proposal to change a program of an institution, or for the establishment of a new program;
- A report of an interdepartmental committee task force or similar body, or of a committee or task force within an institution, which has been established for the purpose of preparing a report on a particular topic;
- A report of a committee, council or other body which is attached to an institution and which has been established for the purpose of undertaking inquiries and making reports or recommendations to the institution;
- 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 discretionary power conferred by or under an enactment or scheme administered by the institution.

Under both FIPPA and MFIPPA, the exemption does not apply to records that are more than twenty years old.

Further, under FIPPA only, this exemption does not apply to a record that has been publicly cited by the head of an institution as a basis for making a decision or formulating policy.

### Public Interest Override

The public interest override applies to this exemption.

## Law Enforcement

FIPPA s. 14 / MFIPPA s. 8

The discretionary exemption for law enforcement protects various types of records and activities relating to justice issues such as:

- Policing;
- Investigations;
- Prosecutions;
- Court proceedings;
- Intelligence information;
- Crime prevention;
- Corrections; and
- Safety and security.

The legislation defines law enforcement as:

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, or
c) The conduct of proceedings referred to in (b).

The context for law enforcement records has been found to be broader than criminal law and policing. The exemption applies to all federal and provincial laws and municipal by-laws that provide authority for law enforcement.

Some institutions also have broad regulatory and law enforcement powers established by a statute. Examples include the Ministry of Labour's ability to investigate under the Occupational Health and Safety Act and the Office of the Fire Marshal under the Fire Prevention and Protection Act.

An institution's records may fall under the law enforcement exemption because the institution:

- Has law enforcement responsibilities for other organizations; or
- Is the subject of an investigation.

An institution is not required to carry out law enforcement activities for the exemption to apply to a record under its custody or control.

The exemption allows an institution to refuse to confirm or deny the existence of a record under this exemption where:

- The record, if it exists, would quality for exemption under this section; and
- Disclosure of whether the record does or does not exist would, in and of itself, disclose enough information that could reasonably be expected to harm an interest protected by the exemption.

A harms test applies to where the phrase "could reasonably be expected to" is used. Detailed and convincing evidence has been found to be necessary is order to show that the risk of harm is well beyond the merely possible or speculative although it need not prove that that disclosure will in fact result in such harm.

The law enforcement exemption has several subsections that address a range of scenarios.

Each of the scenarios listed in the subsections of the exemption will be discussed below. A head may refuse to disclose a record where the disclosure could reasonably be expected to:

**Interfered with a Law Enforcement Matter**

This exemption applies if disclosure could reasonably be expected to interfere with a law enforcement matter.

"Interfere" has been interpreted to mean that the disclosure would have the effect of hindering or impeding the carrying out of a law enforcement activity. Interfere 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.

A "matter" may go beyond a specific investigation, such as a firearm registry database created and used by the police or a prosecution before a court.

For this exemption to apply, the law enforcement matter must be ongoing.

### Interfere with a Law Enforcement Investigation

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.

An “internal or employment-related investigation” may also be a “law enforcement investigation” if it:

- Involves the police, or result in subsequent police investigation; or
- Leads to a proceeding that could result in internal discipline, termination of an employee or other actions.

### Reveal Investigative Techniques

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. Institutions should be able 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 to the public, reliance on this exemption would not be successful.

### Reveal a Confidential Source

An institution may refuse disclosure 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.

A “confidential source of information” must have a reasonable expectation that the information provided would be kept confidential, based on the sensitivity of the matter and seriousness of consequences.

### Endanger the Safety of a Law Enforcement Officer or Any Other Person

An institution may refuse disclosure of a record where it would endanger the safety of a law enforcement officer or any other person. This provision is similar to the danger to safety and health exemption in the legislation.

### Compromise a Fair Trial or Impartial Adjudication

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 or impartial adjudication.

This subsection does not contain a reference to law enforcement and, accordingly, the exemption could apply to proceedings that do not fall within the definition of law enforcement such as tribunals established by law to adjudicate individual or collective rights. There must be evidence that the disclosure of the records would result in unfairness.

The term “person” is not limited to a specific person and may include some unknown person or persons in the future.

### Reveal Intelligence Information

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 defined as information gathered by a law enforcement agency in a covert manner with respect to ongoing efforts devoted to the detection and prosecution of crime or the prevention of possible violation of law.

### Reveal Confiscated Records

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

### Endanger the Security of Property

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.

### Facilitate Escape

Records are exempt where the disclosure could reasonably be expected to facilitate the 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 has been found to apply, for example, 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. There must still be a determination of whether the current plans under the current circumstances would reasonably be expected to facilitate an escape.

### Jeopardize the Security of a Centre for Lawful Detention

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.

### Facilitate an Unlawful Act

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 conduct” means a violation of a statute or regulation or of a municipal by-law.

The exemption also lists a number of records that may be exempted based on their type or nature. For these records, the institution does not need to prove that the disclosure of the record would result in a specific harm unless the wording of the subsection indicates that requirement. A head may refuse a record that is:

### A Law Enforcement Report

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.

### Protected by an Act of Parliament

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

For example, the Youth Criminal Justice Act makes it an offence to knowingly disclose certain court, police and government records relating to young offenders, except as authorized by that Act.

### Could Expose Someone to Civil Liability

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.

Civil liability could include lawsuits against law enforcement officials, witnesses or informants for defamation.

### Related to a Person Under the Control or Supervision of a Correctional Authority

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.

### Exceptions

There are two categories of exceptions to the exemption:

- Routine inspection reports; and
- Law enforcement program success (e.g., statistical analysis).

As discussed above, reports prepared in the course of law enforcement, inspections or investigations are a type of report which is exempt from disclosure, but routine inspection reports are not included in this exemption. *"*Routine inspections*"* are inspections that are carried out by an agency with statutory authority to enforce and regulate compliance with standards (e.g. the enforcement or compliance branch of an institution); and where there are no specific allegations that standards have been breached. However, other exemptions, such as personal privacy, may apply to portions of these records.

The exception for law enforcement program success means the exemption cannot be applied to statistical analyses of law enforcement programs unless the disclosure of such a record may prejudice, interfere with or adversely affect any of the matters referred to in those sections.

### Public Interest Override

The public interest override does not apply to this exemption.

## Civil Remedies Act, 2001

FIPPA s. 14.1 / MFIPPA s. 8.1

This discretionary exemption allows institutions to withhold information that could reasonably be expected to interfere with the ability of the Attorney General to determine whether a proceeding should be commenced under the Civil Remedies Act, 2001, conduct a proceeding under that Act, or enforce an order under that Act.

Institutions may also refuse to confirm or deny the existence of a record if it would likewise impact the ability of the Attorney General to undertake the same processes related to the Civil Remedies Act, 2001.

### Public Interest Override

The public interest override does not apply to this exemption.

## Prohibiting Profiting from Recounting Crimes Act, 2002

FIPPA s. 14.2 / MFIPPA s. 8.2

This discretionary exemption allows institutions to withhold information that could reasonably be expected to interfere with the ability of the Attorney General to determine whether a proceeding should be commenced under the Prohibiting Profiting from Recounting Crimes Act, 2002, conduct a proceeding under that Act or enforce an order under that Act.

Institutions may also refuse to confirm or deny the existence of a record if it would likewise impact the ability of the Attorney General to undertake the same processes related to the Prohibiting Profiting from Recounting Crimes Act, 2002.

### Public Interest Override

The public interest override does not apply to this exemption.

## Relations with Other Governments

FIPPA s. 15 / MFIPPA s. 9

The FIPPA exemption for relations with other governments is discretionary; however, it is a mandatory exemption under MFIPPA. While this exemption is discretionary under FIPPA, if an institution wishes to disclose records for which the head has reason to believe this exemption applies, the head must obtain prior approval from the Executive Council.

Under both statutes, this exemption protects records which could reasonably be expected to reveal information received in confidence by an institution from another government or its agencies, or an international organization of states or its bodies.

Under FIPPA, this exemption also applies where the disclosure of the record could reasonably be expected to prejudice the conduct of intergovernmental relations.

"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;
- An agency of government referred to above; or
- An international organization of states (e.g. United Nations).

Ontario municipalities are not considered “other governments” under either legislation.

There are further differences in the wording of this exemption between FIPPA and MFIPPA. For example, within MFIPPA, the exemption explicitly states that 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 FIPPA.

The types of records that may come under this exemption include letters, meeting notes or minutes, transcripts of confidential meetings, draft agreements, briefing materials, presentations, and reports.

An institution must provide evidence that the record was received implicitly in confidence. For example, a record may be clearly marked “in confidence” or the parties may have an agreement that supports confidentiality.

### Public Interest Override

The public interest override applies to this exemption.

## Relations with Aboriginal Communities

FIPPA s. 15.1 / MFIPPA s. 9.1

This discretionary exemption would allow institutions to withhold records where disclosure could reasonably be expected to prejudice the conduct of relations between an Aboriginal community and the institution; or reveal information received in confidence from an Aboriginal community by an institution.

The exemption is similar to the exemptions for relations with other governments.

In the legislation, an “Aboriginal community” means:

a) A band within the meaning of the Indian Act (Canada),
b) An Aboriginal organization or community that is negotiating or has negotiated with the Government of Canada or the Government of Ontario on matters relating to,
    i. Aboriginal or treaty rights under section 35 of the Constitution Act, 1982, or
    ii. A treaty, land claim or self-government agreement, and
c) Any other Aboriginal organization or community prescribed by the regulations.

The regulations under FIPPA and MFIPPA do not, at this time, identify any other "Aboriginal organizations."

In Ontario, Aboriginal people belong to a rich and diverse range of communities, cultures, membership and affiliations. Section 35 of the Constitution Act, 1982 uses the term "aboriginal peoples of Canada" to include the "Indian, Inuit and Métis peoples of Canada".

If it is unclear if a specific community or organization is captured in the definition, Coordinators may wish to seek advice from Legal Counsel.

### Public Interest Override

The public interest override applies to this exemption.

## Defence

FIPPA s. 16

This discretionary exemption protects the national defence of Canada and international relations. Defence includes the prevention of attacks or other acts of aggression. The exemption also addresses espionage, sabotage and terrorism. The focus is on prejudice and injury that may result from disclosure.

The exemption extends to protect foreign states allied or associated with Canada from prejudice or injury resulting from disclosure of a record. 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.

Defence is primarily a federal concern. However, the Ontario government may have records that relate to national defence as a result of working in areas of broader international concern or negotiations such as:

- The environment;
- Energy;
- Emergency planning;
- Immigration;
- Economic development,
- Trade;
- Education; and
- Cultural and social matters.

The Ontario government is consulted by the federal government and may act on its own in contacting representatives of other governments. As such, there is a range of provincial diplomatic activity which generates records relating to international relations.

Factual information relating to defence or international relations can be sensitive and require protection from disclosure. Factual information may include technical and non-technical information.

It is difficult to predict future events and what information may be of interest to a foreign government or a hostile party. Whether portions or types of information are available from other public sources has been found to be not, on its own, a determinative factor. The inclusion of factual or other information in a record exempt under defence may result in all of the information in the record being exempt.

An institution must seek Cabinet consent to disclose a record under the defence exemption.

### Public Interest Override

The public interest override does not apply to this exemption.

## Third Party Information

FIPPA s. 17 / MFIPPA s. 10

This mandatory exemption protects confidential information supplied to institutions by a third party. A third party can be any supplier of information to an institution that meets the section requirements including a:

- Person;
- Group;
- Committee;
- Organization,
- Institution; or
- Business, including contracted vendors.

Generally, an employee of an institution and other institutions under the legislation are not considered a third party.

The exemption does not protect all third party information but informational assets that have “value” such as:

- Trade secrets;
- Scientific information;
- Technical information;
- Commercial information;
- Financial information; and
- Labour relations information.

Institutions typically have third party information because of:

- Legal or regulatory requirements such as assessments or reporting; and
- For the purchase of goods and services including information received in a competitive bidding process.

The exemption is intended to protect the position and interests of a third party rather than the institution. The areas of possible harm are:

- Significant prejudice to a competitive position or significant interference with contractual or other negotiations;
- Similar information no longer being supplied to an institution where it is in the public interest that similar information continue to be so supplied;
- Undue loss or gain;
- Revealing information relating to a labour relations dispute; and
- Revealing tax information relating to tax liabilities and collection (FIPPA only).

There must be a reasonable expectation of harm to the third party not merely speculation of harm.

A three-part test must be met for the exemption to apply. Each part must apply in order for the exemption to apply. If information fails one part of the three-part test, further analysis would not be required and the exemption could not be claimed. The three-part test requires that:

1. The records must include information that is a trade secret, or scientific, technical, commercial, financial or labour relations information.
2. a) The information must be supplied by the third party to the institution.

   b) The information must be supplied in confidence, implicitly or explicitly.
3. The disclosure of the information could reasonably be expected to cause one or more of the specified harms above.

An institution may disclose records if the third party or third parties to whom the information relates consent to the disclosure.

**Part 1: Type of Information**

The legislation identifies six types of information eligible for the exemption. The list below provides a definition and examples of each. The terms have specific meanings and are distinct from each other.

**Trade secret:** 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. Examples include software or hardware system, a vaccine formula, and an algorithm.

**Scientific:** An organized field of knowledge in either the natural, biological or social sciences or mathematics that must also relate to observing and testing specific hypotheses or conclusions and be undertaken by an expert in the field. Examples include research, results of raw data analysis, and chemical substance testing.

**Technical:** An organized field of knowledge that would fall under the general categories of applied sciences or mechanical arts, and will usually involve information prepared by a professional in the field. Examples include records relating to architecture, engineering, electronics, or construction including drawings, site plans and specifications for building.

**Commercial**: The buying, selling or exchange of products or services, and can apply to both profit-making and non-profit organizations. Examples include product information, tenders, marketing strategies, cost quotations, price, supplier, and customer lists, client information, and business proposals.

**Financial:** Specific data and information that relates to finance or money matters, including the use and distribution of money. Examples include accounting methods, financial statements, pricing practices, bid information, property tax information, sales revenues, and employment costs.

**Labour relations:** The collective bargaining relationship between an employer and its employees. Examples include records relating to the impact of human resources policies, labour dispute plans and pay equity plans.

**Part 2a: Supplied by a Third Party**

Information is supplied when a third party gives or submits it to an institution and the information is not subject to change. The manner in which information is supplied is not relevant.

If a record includes information that may reveal or enable an inference to be made about information supplied by a third party, it may still qualify as being supplied.

Below is a list of examples where information could be considered to be supplied by a third party:

- The third party is required by statute to supply the information;
- The third party supplied the information in response to a request for proposal (RFP);
- The third party supplies specific product or technical details as a schedule to an agreement or contract with an institution; and
- The third party submits test results.

Information is not considered supplied when:

- The institution produces or calculates the information independently;
- The information is generated together by a third party and an institution;
- The information is a product of negotiations; and
- The information is merely about a third party.

Below is a list of examples where information would not be considered to be supplied by a third party:

- An employee of an institution performs an inspection of a third party;
- A project status report;
- A negotiated agreement between an institution and a third party; and
- Procurement evaluation information (that does not include informational assets taken directly from a RFP, methodology, and results.

A negotiated agreement between an institution and a third party normally does not qualify as having been supplied because terms of contracts are generally mutually generated by both the institution and the third party, rather than “supplied” by the third party. This applies even when the contract is preceded by little or no negotiation or where the final agreement reflects information that originated form a single party.

There are two exceptions to this general rule which are described as the “inferred disclosure” and “immutability” exceptions. The “inferred disclosure” exception applies where disclosure of the information in a contract would permit accurate inferences to be made with respect to underlying non-negotiated confidential information supplied by the third party to the institution. The immutability exception arises where the contract contains information supplied by the third party, but the information is not susceptible to negotiation. An example would be schedules to a contract that include detailed price lists for services or products supplied by the vendor.

**Part 2b: Supplied in Confidence**

A third party must have an expectation of confidentiality at the time the information was supplied. The expectation can be:

- Implicit – meaning it is understood without being stated directly; or
- Explicit – meaning stated directly or explained so that you cannot doubt what is meant.

The main factors that have been used to determine reasonableness are set out below.

- If the document marked as “Confidential”;
- If the third party communicated to the institution that the record is confidential and is to be kept confidential; or
- If a confidentiality clause in a contract.

Factors to consider when determining if the information was protected as confidential include:

- Was access to the record or information limited, such as being available on a “need to know” basis?
- Was a policy for security or recordkeeping followed?
- Hs the record been consistently treated as confidential by the third party through demonstrated concern for its protection from disclosure prior to disclosure to the institution?
- Was the information available to the public through other sources?
- Did the institution or third party publicly disclose the information?
- Was the information guarded from competitors?
- Was the information prepared for a purpose that would not include disclosure?
- Does the record reveal the substance negotiations?

**Part 3: Expectation of Harm**

The discussion of harm is concerned with the third party whose information may be disclosed, not the institution. In some cases a harm may also occur to another person, group, or to an organization, other than the third party.

Both an institution and the third party should provide representations about harms. More than one of the harms can apply to the information but at least one must apply.

The third party is in the best position to make a strong and informed argument regarding the likelihood of harms. The particular facts of each case must be evaluated. The evidence must be detailed and convincing.

The Courts and the IPC have confirmed that the "could reasonably be expected" threshold does not require proof that harm is probable or that on a balance of probabilities the harm will occur. There must, however, be a reasonable basis to support the identified risk. The party relying on the exemption must show that the risk of harm is well beyond the merely possible or speculative using detailed and convincing evidence.

Below is a discussion of some types of harms and circumstances where these harms could be found to "reasonably be expected to" result after the disclosure of the third party information.

**Competitive position:** For this harm to meet the test, the impact must be significant. The factors that have been found to be relevant include:

- A competitive industry;
- A critical success factor to a business;
- Time and expense invested in development;
- Usefulness to a competitor;
- Detailed pricing or breakdown of pricing; and
- A measureable harm or injury.

**Interference with contractual obligations or negotiations:** For this harm to meet the test, the impact must be significant. This section is often applied in the context of commercial or union negotiations that have not been finalized.

**Similar information no longer supplied:** For this harm to meet the test, the supply of information must be voluntary and there must be a public interest in the continued supply of the information. This harm is concerned with situations where a third party, faced with the prospect that their information will be disclosed under the legislation, may no longer voluntarily supply similar information in the future to the institution.

**Undue loss or gain**: For this harm to meet the test, the loss or gain must be undue which means:

- Excessive,
- Disproportionate,
- Not suitable, and
- Not owed.

Losses and gains are generally argued together because a loss to one party usually means a gain to another party. Losses or gains are generally related to investments of money, time, and effort; and impact revenues. The possibility of a law suit is not sufficient grounds for the exemption to apply

The loss or gain can be to any person, group, committee, financial institution or agency, and not necessarily to the third party submitting the information.

**Labour relations disputes**: For this harm to meet the test, individuals or third parties must be appointed under law to resolve a labour relations dispute. Examples include mediators, conciliation, review, and labour relations officers. Harm would be found to result if disclosure of the record could be reasonably expected to reveal the information produced for or prepared by these third parties.

### Tax Information

Under FIPPA only, there is an additional exemption for tax information. Disclosure must reveal information obtained on a tax return, or information gathered to collect or determine a tax liability of a specific taxpayer.

The tax information section only applies to FIPPA and the harms test of “could be reasonably expected to” does not apply.

### Public Interest Override

The public interest override applies to this exemption.

## Economic and Other Interests

FIPPA s. 18 / MFIPPA s. 11

This discretionary exemption allows institutions to protect certain proprietary information and prevent the premature disclosure of certain plans or negotiating strategies. This gives the Ontario government and institutions similar protection to that given to third parties under the third party information exemption.

The protections are focused on issues such as:

- Generating revenue,
- Competitive position,
- Monetary gain or loss, and
- Strategic positioning.

The exemption covers various business roles and activities of the Ontario government and institutions such as:

- Engaging in commercial activities;
- Conducting research;
- Managing finances and the economy;
- Carrying out negotiations;
- Managing the administration of institutions and personnel;
- Proposing plans, policies, and projects;
- Conducting examinations and testing; and
- Deciding on municipal boundary submissions.

The exemption protects the parties involved from gaining any advantages or disadvantages from the disclosure of information. The exemption takes into account the impact of premature disclosure of information in activities that are current or not yet completed.

The protections are against prejudice or injury. A harms test applies to some but not all of the subsections.

The exemption has nine subsections. Some of these refer to the Government of Ontario broadly, some refer to an institution, and some refer to both.

In some subsections “information” is referenced generally and in others specific types of information or records are identified and the definitions of these terms must be applied in the analysis.

**Commercial Information**

This exemption is commonly referred to as commercial information. The definitions are the same as the third party information exemption, with the exception of labour relations which is omitted. It has a three part test.

The institution must establish that the information contained in the record:

1) Is a trade secret, or financial, commercial, scientific or technical information; and
2) Belongs to the Government of Ontario or an institution; and
3) Has monetary value or potential monetary value.

**Part 1: Type of information**

This exemption identifies five types of information:

- Trade secret;
- Scientific information;
- Technical information;
- Commercial information; and
- Financial information.

Definitions based on interpretations of these types of information can be found in the above section on the third party exemption.

**Part 2: Belongs to an institution**

The information must belong to the Government of Ontario or an institution.

“Belongs to” refers to more than just bare or simple ownership or possession. There must also be some proprietary interest. A proprietary interest can be an intellectual property interest. Examples include copyright or trademark.

A proprietary interest can also exist where the law would recognize a substantial interest in protecting the information from misappropriation by another party. Examples include trade secrets, customer or supplier lists, or price lists.

The information may belong to the institution with custody of the record or another institution. If the information is in the public domain, the exemption may not apply.

**Part 3: Monetary value**

The information must have monetary value or potential monetary value which means that the information can yield a price in the market or is potentially marketable.

Monetary value can be established by demonstrating:

- A market or demand for information;
- Similar records are available for a fee (more than just an administrative fee);

- Willing buyers and sellers for the information; and
- An intention to provide the information for monetary gain.

**Employee Research**

This exemption protects information obtained through employee research where disclosure could reasonably be expected to deprive the employee's priority of publication.

The definition of research is the same as in other sections. Research has been defined by the IPC as "a systematic investigation designed to develop or establish principles, facts or generalizable knowledge, or any combination of them, and includes the development, testing and evaluation of research."

The research must be linked to a specific researcher. There must be strong evidence of an intention to publish such as:

- A sworn affidavit;
- A document prepared for internal peer review;
- An announcement at a conference; or
- Having data already available for publication.

The exemption does not apply to raw data.

**Economic and Competitive Interests of an Institution**

This exemption protects an institution's economic interests and competitive position against prejudice. This has been interpreted to not require that the information belong to the institution that is claiming the exemption. To claim this exemption, the institution must provide detailed and convincing evidence that 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, related costs and prices.

Competitive position applies where institutions are engaged in the supply of goods and services for profit and compete for business on a competitive basis.

The exemption does not apply where an institution has a monopoly or there are no competitors. Also, certain information may lose value as it gets dated.

Questions to consider in determining if this exemption applies include: Could the institution pay a higher price for goods and services if the information is disclosed? Could the institution lose revenue if the information is disclosed?

An institution should have the ability to negotiate the best possible deal regardless of the type of contract. Contractual negotiations are implicit in some of the examples above but the exemption may also apply to financial settlements.

Relevant factors relevant in assessing whether records relating to contractual negotiations are exempt could include:

- Are the negotiations current?
- Will disclosure affect the willingness of parties to negotiate in the future?
- Will disclosure affect the institution's ability maximize profits?
- Will there be a chilling effect on future business ventures?
- Will disclosure affect Ontario's ability to prepare and submit competitive bids for industry (compared to other provinces)? or
- Is a significant donation involved?

The exemption is found not to apply to contract information that may help a competitor in other ways such as responsibility for delays, non-performance, revenue sharing, term of the agreement, or termination provisions.

The exemption does not apply to disclosure of a final agreement unless it can be established that other parties may use past information or reveal information about the institution's position, such as whether the institution is willing to absorb costs. Also, a confidentiality clause in settlement agreements may not be enough for the exemption to apply.

**Government's Financial Interests and Managing the Economy**

This exemption protects the broader economic interests of Ontario against injury. Where economic interests are negatively affected, financial interests are usually also affected. To claim this exemption the institution must provide detailed and convincing evidence that disclosure could reasonably be expected to be injurious to the financial interests of the government or to manage the economy of Ontario.

Examples of how financial interests of the Government of Ontario may be affected include:

- Where the government is the sole shareholder;
- Where the government faces serious threats to economic security;
- Where the government faces security threats to infrastructure or buildings;
- Where the government may be required to make a significant financial payment as a remedy;
- Where the integrity of a government system could be jeopardized.

There must be a link between disclosure of a record and the injury. The exemption does not apply to an injury that may result from the government's own conduct or practices.

**Proposed Plans or Criteria for Negotiations**

This exemption protects the ability of the Government of Ontario or an institution to negotiate effectively with third parties.

A negotiation means discussions and communications where the government or an institution and a third party are seeking to arrive at a legally binding agreement, settlement or contract.

Negotiations must be in the context of financial, commercial, labour, international or similar situations such as:

- Aboriginal land claims;
- Commercial fishing agreements;
- Allocation of forest resources; and
- Settlement of litigation.

This exemption does not apply where the government is consulting stakeholders with a view to developing policy or legislation, or regarding possible litigation.

The exemption applies to positions, plans, procedures, criteria, or instructions to be applied to any negotiations.

A plan is defined as a formulated and detailed method by which a thing is to be done, or a design or scheme.

Positions, procedures, criteria, instructions are pre-determined courses of action or ways of proceeding, and includes comments on the strength of positions, bottom line or fall-back positions, options, or tactics developed as part of the negotiation process.

The exemption has a four-part test:

Part 1: The records must contain positions, plans, procedures, criteria or instructions.

Part 2: The records must be applied to or intended to be applied to the negotiations.

Part 3: The negotiations must be current and ongoing which means carried on or to be carried on.

Part4: The negotiations must be conducted by or on behalf of an institution or the Government of Ontario.

The exemption does not apply to:

- Factual information used to develop positions, plans etc.;
- Information that could apply to future negotiations not yet contemplated, planned or started; or
- Minutes of settlement, release, and resignation with an employee.

**Plans for Management of Personnel or Administration**

This exemption protects plans relating to managing personnel or the administration of an institution that are not yet in operation or public. The purpose is to protect an institution's internal management plans such as a reorganization, relocation, or creation of an agency prior to implementation.

The timing and the nature of the plan are important factors. A plan must have sufficient detail to qualify such as methods, schemes or designs, recommendations, and plans for action. A plan that has been put into effect or been announced does not qualify.

The exemption has a three part test:

Part 1: A record must contain a plan or plans.

Part 2: The plan or plans must relate to the management or personnel of the administration of the institution.

Part 3: The plan or plans have not yet been put into operation or made public.

**Proposed Plans, Policies and Projects**

The exemption protects proposed plans, policies or projects that may result in:

- Premature disclosure of a pending policy decision; or
- Undue financial benefit or loss to a person.

A harms test must be met, meaning that the institution must be able to demonstrate a harm would likely result from the disclosure of these records. The exemption only applies when one of the two specified results can reasonably be expected to occur due to the disclosure. Records must be prescriptive rather than descriptive.

The term proposed means a planned undertaking that has not already been completed. There must be a decision which the institution has already made.

A pending policy decision refers to a situation where a decision has been reached but not yet implemented. The exemption may apply to operational decisions depending on the circumstances of each case.

Undue means excessive, disproportionate, not suitable, and not owed, similar to how it has been interpreted in other sections.

The exemption does not refer to a situation where a policy paper or consultations undertaken for a policy review, or a policy decision is before an institution for consideration or deliberation.

The undue financial benefit or loss must be to the third party and not the institution.

**Examinations and Testing**

This exemption protects questions used in examinations and tests by institutions with an educational purpose which is generally informed by the mandate of the organization, such as schools, colleges, universities.

The exemption covers questions that:

- Are to be used; or
- Have been used that can lead to an accurate inference of future questions.

Relevant factors include:

- The difficulty of generating new questions;
- If a re-use protocol is in place; and
- If feedback is given without returning tests.

The fact that an institution may choose to re-use the same questions is not sufficient to satisfy the requirement. Other factors must exist for the exemption to apply to reused questions.

The wording of the exemption is different under FIPPA and MFIPPA. The FIPPA exemption broadens the wording to include testing procedures and techniques.

Another difference is that FIPPA includes a harms test while MFIPPA does not. FIPPA requires that the disclosure could reasonably be expected to prejudice the use or results of the tests or testing procedures and techniques.

**Municipal Boundary Submissions**

This exemption protects submissions made by a municipality or other body in respect of a matter under the Municipal Boundary Negotiations Act before this statute was repealed by the Municipal Act, 2001. The matter must have been commenced before the repeal and it must not be resolved yet.

**Quality of Care Information**

This exemption protects information provided in confidence to a hospital, or records prepared with the expectation of confidentiality by a hospital committee, to assess or evaluate the quality of health care and directly related programs and services provided by a hospital, if the assessment or evaluation is for the purpose of improving that care and the programs and services.

### Exceptions

Only FIPPA provides for exceptions to the economic and other interests exemption. The exemption does not apply to a record that contains the results of product or environmental testing carried out by or for an institution, unless:

- Testing is done as a service for a fee to a person, group of persons or an organization other than an institution; or
- Testing was conducted as preliminary or experimental tests for the purpose of developing methods of testing.

### Public Interest Override

The public interest override provision applies to this exemption.

## Universities, Colleges and Hospitals Closed Meetings

FIPPA s. 18.1

The discretionary exemption for closed meetings applies to universities, colleges and hospitals. It is similar to the draft by-laws and closed meetings exemption under MFIPPA and provides universities, colleges and hospitals with similar confidentiality provisions in the deliberative processes of their respective governing bodies.

The exemption is intended to be limited and specific and to protect deliberations where the substance of those deliberations deals with the:

- A draft of a by-law, resolution, or legislation; and

- Litigation or possible litigation.

The exemption requires that a meeting and deliberations take place. A meeting is not any gathering. A meeting occurs where attendees come together for the purpose of exercising their power or authority or in preparation of doing so. Deliberations refer to discussions conducted with a view towards making a decision.

The exemption requires that meetings be held in the absence of the public which are generally known as in camera meetings. The requirements for an in camera meeting include:

- Legal authority under a statute to hold a closed meeting;
- That the body holding the closed meeting has proper legal authority;
- That the closed meeting was properly convened in the absence of the public; and
- That meeting records are kept confidential.

### Exceptions

The exemption does not apply when the information is not held confidentially or the subject matter of the deliberations was considered in a meeting open to the public.

The exemption does not apply to records that are more than twenty years old.

### Public Interest Override

The public interest override applies to this exemption.

## Solicitor-Client Privilege

FIPPA s. 19 / MFIPPA s. 12

The discretionary exemption of solicitor-client privilege covers records subject to the common law solicitor-client privilege (referred to as “Branch 1”). The exemption also covers 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 litigation or for use in litigation (referred to as “Branch 2”).

"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 legal opinions are not released to another party as the solicitor-client privilege might be jeopardized.

**Branch 1 –**The common law privilege applies to:

- All communications, verbal or written, of a confidential character, between a client, or their agent, and Legal Counsel employed by the institution, directly related to seeking, formulating or giving of legal advice or legal assistance (including the Legal Counsel's working papers directly related thereto); and
- Papers and materials created or obtained especially for a Legal Counsel'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 Counsel; and
- The communication must be directly related to seeking, formulating or giving legal advice.

Solicitor-client privilege protects the confidentiality of communications between Legal Counsel and a client to ensure full, free and frank communications. This privilege is permanent, subject to waiver. A confidential relationship is essential condition of the effective administration of justice.

**Branch 2 – Records Prepared by or for an Institution's Legal Counsel for Use in Giving Advice or Contemplation of Litigation:** This branch of the exemption applies to all materials prepared for use in actual or contemplated litigation. The records do not have to contain confidential communications between the institution and counsel or be communications at all.

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

- Contemplated litigation must be the dominant purpose for preparing the record, and

- 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.

Litigation privilege applies to settlement and mediation records that are considered confidential communications between parties trying to settle a dispute, including oral and written communications made with a view to reconciliation and settlement.

Litigation privilege has been found to extend to alternate dispute resolution records.

Common law litigation privilege applies only until the end of the litigation; however, the statutory litigation privilege has been found to be permanent.

This is similar to the common-law privilege but specifically identifies the lawyer as being Crown counsel or counsel employed or retained by an educational institution or hospital. The privilege applies to both advice given and records made in contemplation of for use in litigation.

Counsel employed by the Ontario government, including outside counsel retained by the Ontario government are “Crown” counsel.

In government, the solicitor-client relationship is typically between the institution’s counsel and the institution. When Legal Counsel advises on non-legal issues, it is not considered legal advice. The exemption does not apply just because Legal Counsel reviews a document. Advice must be related to legal issues.

## Waiver of Solicitor-Client Privilege

Solicitor-client privilege is a client’s privilege, and a client may decide to disclose privileged information obtained from their Legal Counsel and in this way “waive” the privilege.

Waiver does not occur where the disclosure of information is required by law. It is also not considered to be waived if privileged information is shared with other employees within an institution or department.

Waiver is established where the client as the holder of the privilege:

- Knows of the existence of the privilege;
- Voluntarily demonstrates an intention to waive the privilege;
- The record was disclosed to an outside party; or
- The communication was made in open court.

Disclosure of privileged information to outsiders generally constitutes waiver. For example, waiver would be applied to a letter sent between opposing counsel.

Solicitor-client privilege is not considered to be waived when records are provided to the IPC for the purposes of an appeal.

A waiver does not necessarily occur when a small amount of information from the conclusion of a legal opinion or a summary statement of a legal opinion is disclosed. The substance of the whole legal opinion may remain privileged.

A waiver does not occur when solicitor-client privileged information is shared among parties who are found to have a common interest. Examples of where common interest may exist include:

- The sender and receiver anticipate litigation against a common adversary;
- A legal opinion was distributed to a group of entities in connection with shared advice; and
- Multiple parties shared a legal opinion in confidence in an effort to put them on equal footing in negotiations.

This exemption is considered to be class-based and therefore records subject to this exemption cannot be severed, but rather are withheld in full.

### Public Interest Override

This exemption is not subject to the public interest override.

## Danger to Safety or Health

FIPPA s. 20 / MFIPPA s. 13

This discretionary exemption is focused on serious threats to the safety or the health of an individual if a record is disclosed. The term individual is meant to include any individual, regardless of whether the individual is acting in a personal or professional capacity.

Generally an individual is identifiable or named but it is not necessary for the exemption to apply.

The exemption may also apply in situations where an individual is:

- Acting on behalf of a group;
- A member of a group at risk; or

- Employed to do dangerous or controversial work.

This exemption is related to the law enforcement exemption which protects against danger to the life or physical safety, but not the health, of law enforcement officers and any other person.

A harms test has been developed for this exemption. The harms test does not require the institution to prove that harm resulting from the disclosure is probable, but that there is a reasonable basis for believing that disclosure could "seriously threaten the safety or health of an individual."

The reasonable expectation of harm must be objective rather than subjective. There must be clear and direct evidence of a connection between the disclosure of the contents of the record and the expectation of harm.

An individual's fear alone may not be enough to satisfy the requirement. Factors to consider when determining if the harms test is met include:

- An actual threat;
- Persistent and harassing behaviour;
- Pattern of abusive and intimidating correspondence;
- Past violent behaviour;
- Likelihood of retaliation;
- History of frivolous or vexatious complaints;
- Time between alleged behaviour and request.

The exemption may be found to apply where a record reveals a physical location that may be linked to an individual.

The exemption does not apply to general or statistical information, for example in a case concerning suicide statistics. The statistics did not reveal the locations or methods of the suicides and the institution was found not to have provided enough evidence of a reasonable expectation of harm resulting from the disclosure of the statistics.

## Public Interest Override

The public interest override applies to this exemption.

## Personal Privacy

FIPPA s. 21 / MFIPPA s. 14

This mandatory exemption protects the personal information of individuals other than the requester, except in the circumstances specified in this section. See Chapter 7: Privacy Fundamentals, for a detailed definition of personal information.

This section is one of the keystone provisions in the legislation. It balances the public's right of access to records and the individual's right of privacy respecting personal information.

This exemption requires institutions to refuse disclosure of personal information to individuals other than to which the information relates except in the circumstances specified in the legislation.

The exemption also allows institutions to disclose personal information in certain circumstances, as set out below.

**Written consent:** When an individual provides written consent to the disclosure of their personal information to another person.

**Health and safety of an individual:** When compelling circumstances affecting the health or safety of an individual require disclosure. Institutions must provide notification of the disclosure to the affected individual at the individual's the last known address.

**Public record:** When the personal information was collected and is maintained specifically for the purpose of creating a record available to the general public. For more information on personal information maintained for the purposes of creating a public record, see Chapter 7: Privacy Fundamentals.

**Authorized by statute:** When an Act of Ontario or Canada expressly authorizes the disclosure of personal information.

**Research agreement:** Personal information can be disclosed for research purposes if certain conditions are met. For more information on research agreements, see Chapter 6: Managing the Request Process.

**No unjustified invasion of privacy:** Disclosure of personal information is also permitted if the disclosure would not constitute an unjustified invasion of privacy.

The exemption sets out a non-exhaustive list of criteria for determining whether the disclosure of personal information would constitute an unjustified invasion of privacy.

Some of the criteria favour disclosure, while others favour non-disclosure of personal information. Criteria that favour disclosure include:

- Is the disclosure is desirable for the purpose of subjecting the activities of the Government of Ontario and its agencies to public scrutiny?
- May access to the personal information promote public health and safety?
- Would access to the personal information promote informed choice in the purchase of goods and services? and
- Is the personal information relevant to a fair determination of rights affecting the person who made the request?

Criteria that favour non-disclosure include:

- Would the individual to whom the information relates be exposed unfairly to pecuniary or other harm?
- Is the personal information highly sensitive?
- Is the personal information unlikely to be accurate or reliable?
- Was the personal information supplied by the individual to whom the information relates in confidence? and
- Would the disclosure unfairly damage the reputation of any person referred to in the record?

The exemption also sets out the types of personal information that, if released, are presumed to result in an unjustified invasion of personal privacy. The list includes personal information that:

- Relates to medical, psychiatric or psychological history, diagnosis, condition, treatment or evaluation;
- Was compiled and is identifiable as part of an investigation into a possible violation of law, except to the extent that disclosure is necessary to prosecute the violation or to continue the investigation;
- Relates to eligibility for social service or welfare benefits or to the determination of benefit levels;
- Relates to employment or educational history;
- Was obtained on a tax return or gathered for the purpose of collecting a tax;
- Describes an individual's finances, income, assets, liabilities, net worth, bank balances, financial history or activities, or creditworthiness;
- Consists of personal recommendation or evaluations, character references or personnel evaluations; and
- Indicates the individual's racial or ethnic origin, sexual orientation or religious or political beliefs or associations.

The exemption further sets out instances where the disclosure of personal information would not constitute an unjustified invasion of personal privacy. These instances include:

**Certain employee information:** The classification, salary range and benefits, or employment responsibilities of an individual who is or was an officer or employee of an institution or a member of the staff of a minister. Disclosure of exact salary information and other details related to employees of an institution, in some cases, may constitute an unjustified invasion of personal privacy.

**Details of contracts for personal services:** Financial or other details of a contract for personal services between an individual and an institution.

**Discretionary financial benefits:** In FIPPA only, details of a licence or permit or a similar discretionary financial benefit conferred on an individual by an institution or a head under circumstances where the individual represents one per cent or more of all persons and organizations in Ontario receiving a similar benefit, and the value of the benefit to the individual represents one per cent or more of the total value of similar benefits provided to other persons and organizations in Ontario.

**Personal information about a deceased individual:** Personal information about a deceased individual may be disclosed to the spouse or a close relative of the deceased individual, if the head is satisfied that, in the circumstances, the disclosure is desirable for compassionate reasons.

The legislation defines “close relative” a parent, child, grandparent, grandchild, brother, sister, uncle, aunt, nephew or niece, including by adoption.

Compassionate circumstances are not defined in the legislation; however, the IPC has found that compassionate circumstances includes when providing the information will allow close family members to have more information about the circumstances surrounding the death of a loved one, or to help provide closure.

The legislation allows an institution to not confirm or deny the existence of a record if disclosure of the existence of a record would constitute an unjustified invasion of privacy. If the decision to not confirm or deny the existence of a record is appealed to the IPC, an institution must provide detailed and convincing evidence that:

- The disclosure of the mere existence of the requested records would convey information to the requester, and
- This nature of this information alone would constitute an unjustified invasion of privacy.

For example, an institution may refuse to confirm or deny the existence of a record where acknowledging the existence of a record would confirm that an individual was the subject of a law enforcement investigation.

Though not expressed in the legislation, the IPC has considered the absurd result principle in adjudicating appeals related to this exemption. The absurd result principle states that to prevent disclosure of information which the requester had provided to a government body would be a manifestly absurd result, and the exemptions related to privacy protection would not apply in these circumstances. The absurd principle applies where the requester originally supplied the personal information of others or the requester is otherwise aware of it. For example, when the requester is seeking access to his or her own witness statement given to the police.

### Public Interest Override

The public interest override applies to this exemption.

## Species at Risk

FIPPA s. 21.1

This discretionary exemption under FIPPA has no MFIPPA equivalent. It makes reference to the provisions in the Endangered Species Act, 2007.

This exemption permits an institution to withhold information that could reasonably be expected to lead to the killing, harming, harassing, capturing or taking a living member of a species that is at risk of extermination.

Further, information that could reasonably be expected to lead to the possessing, transporting, collecting, buying or selling of a living or dead member of a species would also be exempt from disclosure.

Finally, information that if released could reasonably be expected to lead to the damaging or destroying of the habitat of a species at risk would also be exempt.

For the list of species at risk, see Ontario Regulation 230/08.

### Public Interest Override

The public interest override applies to this exemption.

## Information Soon to be Published

FIPPA s. 22 / MFIPPA s. 15

This discretionary exemption provides institutions with the ability to exempt information that is already publicly available or published or will be published within 90 days of receipt of the request, or within such time as is necessary for printing or translating material.

This exemption also allows institutions to refer requesters to existing publications and information that is, or soon will be, publicly available.

According to decisions of the IPC, in order for the institution to claim this exemption, the requested record must be either published or publicly available through a regularized system of access. Examples of a regularized system of access include a public library or a government publication centre.

Where there is a fee to obtain the information, the information may still be considered publicly available as long as the fee is applied to anyone who wishes to obtain the information and the fee is not prohibitively expensive. The pricing structure of the supplier does not have to align with the fees set out in the legislation.

### Public Interest Override

The public interest override does not apply to this exemption.

## Exclusions

In addition to the exemptions that are listed above, the legislation also establishes classes of information that are excluded from coverage of the legislation.

Unlike exemptions, exclusions are classes of information where the public has no general right of access to the information. Though information may be excluded from the legislation, institutions may still choose to provide public access to the information. However, such access would be at the sole discretion of the institution based on the institutions own policies.

The sections below describe each exclusion and identify any exceptions to the exclusions. Where an exclusion only applies to a specific institution or type of institution (such as hospital or educational institution) this will be noted.

## Private Donations to Archives

FIPPA s. 65 (1) / MFIPPA s. 52 (2)

The legislation does not apply to records placed in the Archives of Ontario, the archives of a college or university, or the archives of a municipal institution when the donor of the records is not an institution under the either FIPPA or MFIPPA, or a health information custodian as defined in Personal Health Information Protection Act.

As such, records donated to archives by outside individuals, families, corporations, associations or groups do not become subject to the legislation when donated.

This exclusion does not apply to records deposited in the above mentioned archives by institutions. Government records that were previously subject to the legislation remain subject to the legislation after transfer to an archive.

## Proceedings Before a Court

FIPPA s. 65 (3)

FIPPA does not apply to notes prepared by or for a person presiding in a proceeding in a court of Ontario if those notes are prepared for that person's personal use in connection with the proceeding. A person presiding in a court of Ontario could be a judge or other judicial official.

The exclusion has not been found to extend to the notes of board members of tribunals. The IPC looks at whether a tribunal, as an institution, has custody or control over the notes of members in making its determination.

## Performance Evaluations of Judges

FIPPA s. 65 (4)

FIPPA does not apply to "anything" contained in a judge's performance evaluation or to "any information" collected in connection with a judge's performance evaluation under the Courts of Justice Act.

To qualify for the exclusion the information only requires “some connection” to the prosecution. The exclusion is not limited to just a Crown prosecutor’s brief.

Once the prosecution is over, the exclusion does not apply. The request for records must then be processed under the legislation, including consideration of any applicable exemptions.

## Ecclesiastical Records

s. 65 (5.3)

FIPPA does not apply to the ecclesiastical records of a church or religious organization that is affiliated with a college, university or hospital.

“Ecclesiastical records” are defined in FIPPA as the operational, administrative and theological records, including records relating to the practice of faith, of a church or other religious organization.

## Hospital Foundation

s. 65 (5.4)

FIPPA does not apply to records regarding the operations of a hospital foundation. It would seem likely that records of hospital foundations in the custody of hospitals remain excluded under the legislation.

## Administrative Records of Health Professionals

s. 65 (5.5)

FIPPA does not apply to the administrative records of health professionals that relate to the health professional’s personal practice.

## Charitable Donations

s. 65 (5.6)

FIPPA does not apply to records of charitable donations made to a hospital.

## Labour Relations and Employment-Related

s. 65 (6), 65 (7) / s. 52 (3), 52 (4)

The legislation does not apply "to records collected, prepared, maintained or used by or on behalf of an institution in relation to any of the following":

- 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;
- 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; and
- Meetings, consultations, discussions or communications about labour relations or employment-related matters in which the institution has an interest.

The exclusion has been interpreted broadly and most records that relate to employee management or labour relations are generally considered excluded. The exclusion is not time sensitive and once records are excluded, they remain excluded.

Labour relations generally refer to the relationship between a union and an employer in a unionized workplace.

Employment generally refers to the relationship between an employer and an employee

This exclusion would apply to records such as those regarding internal complaints against employees, investigations of employee misconduct, grievances under a collective agreement or arbitration proceedings. The exclusion also applies to records regarding former employees and individuals considered for employment through a hiring or recruitment process.

The exclusion would also apply to records regarding the planning of labour relations or employee related issues including legal opinion.

### Exceptions

There are exceptions to this exclusion. The following types of records are considered to be subject to the legislation:

- An agreement between an institution and a trade union;

- 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;
- 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; and
- 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 or her employment.

The records listed above are subject to the legislation and therefore may be disclosed under a request, subject to a review for the application of any other exemptions that may apply to the records.

## Church or Religious Appointments of Individuals

s. 65 (6), s. 65 (7)

Hospitals engage church and religious individuals in various positions but these individuals may not be found to be “employees”. This exclusion provides similar protection to the employment records exclusion.

FIPPA does not apply to the appointment or placement of individuals by a church or religious organization within an institution, or within the church or religious organization. The exclusion applies to meetings, consultations, discussions or communications in the appointment process.

## Hospital Appointments of Persons with Privileges

s. 65 (6), s. 65 (7)

Many doctors and other professionals are granted privileges in hospitals but may be found to not be "employees". This exclusion provides similar protection to the employment records exclusion.

FIPPA does not apply to hospital appointments, the appointments or privileges of persons who have hospital privileges, or anything that forms part of their personnel file.

## Adoptions Related

s. 65 (8)

This exclusion applies to all FIPPA institutions and applies to the following information:

- Notices registered under section 48.3 of the Vital Statistics Act and notices and information registered under section 48.4 of that Act;
- Notices, certified copies of orders and other information given to the Registrar General under section 48.5-48.10 of that Act
- Disclosure vetoes registered under section 48.5 of the Vital Statistics Act; and
- Information and records in files that are unsealed under section 48.6 of the Vital Statistics Act.

## Research and Teaching Material

s. 65 (8.1), s. 65 (9)

FIPPA does not apply to the research and teaching work of employees or persons associated with an educational institution or hospital. This allows the exclusion to apply to students and other research partners who are not formally employed by the institution.

FIPPA does not apply to:

- Records respecting or associated with conducted or proposed research; and
- Records of teaching materials collected, prepared, or maintained for the institution.

The only difference between educational institutions and hospitals is that clinical trials are also excluded for hospitals.

The IPC has interpreted what is research and what is considered a research project through adjudicative decisions.

Research has been found to refer to “a systematic investigation designed to develop or establish principles, facts or generalizable knowledge, or any combination of them, and includes the development, testing and evaluation of research.”

Research must refer to a specific, identifiable project that has been conceived by a specific faculty member, employee or associate of an educational institution or hospital that can include a non-employee at an off-site location.

The phrase “conducted and proposed” requires consideration of the facts and context to determine what stage research is in.

### Exceptions

An educational institution or hospital must disclose the subject matter and amount of funding being received for research projects undertaken by the institution or a person associated with the institution.

## Peer Evaluations of Research and Teaching Materials

FIPPA s. 65 (8.1), s. 65 (10)

The term “peer evaluations” is not used in the wording of this exclusion. The legislation refers to evaluative or opinion material compiled in respect of teaching materials or research. This information is normally excluded from FIPPA.

### Exception

Despite the exclusion, evaluative and opinion material compiled in respect of teaching materials or research is subject to FIPPA only in the context of an individual’s request for their own personal information. In the context of a personal information request, individuals maintain a right of access to this material, subject to limited and defined exemptions.

See Chapter 8: Personal Information and Correction Requests for more information on exemptions to the right of access to one’s own personal information.

## Medical Assistance in Dying

s. 65 (11), s. 65 (12)

FIPPA does not apply to “identifying information” in a record relating to medical assistance in dying.

In this section, “identifying information” means information that:

- Relates to medical assistance in dying, and

- Identifies an individual or facility, or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual or facility.

"Medical assistance in dying" means medical assistance in dying within the meaning of section 241.1 of the Criminal Code of Canada.

## Services Relating to Abortion

s. 65 (13), s. 65 (14), s.65 (15)

FIPPA does not apply to information relating to the provision of abortion services if:

- The information identifies an individual or facility, or it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual or facility; or
- Disclosure of the information could reasonably be expected to threaten the health or safety of an individual, or the security of a facility or other building.

In this subsection a "facility" includes reference to a pharmacy, hospital pharmacy or institutional pharmacy, as those terms are defined in subsection 1 (1) of the Drug and Pharmacies Regulation Act.

The legislation specifies that FIPPA applies to statistical or other information relating to the provision of abortion services that does not identify individuals or facilities or could not reasonably be expected to threaten the health or safety of an individual or security of a facility.

# Chapter 6: Managing the Request Process

## Introduction

The legislation establishes administrative procedures for responding to requests for information received under the legislation.

This chapter focuses on how institutions manage the request process. This includes information about requesters, types of requests, timelines for response, and step by step guidance on processing requests.

Within the step by step instruction is information related to various requirements under the legislation including calculation of fees, providing notice to affected parties and more.

## Providing Assistance to Requesters

In addition to striving to achieve legal compliance with the legislation, institutions should provide quality customer service. Coordinators should assist requesters by:

- Providing information about the request process;
- Communicating in a professional and timely manner; and
- Accommodating special needs of the requester.

Coordinators also assist requesters by providing guidance on reformulating unclear requests through clarification. Clarifying requests is discussed later in this chapter.

All written communications with a requester and third parties should:

- Use plain language;
- Be responsive to all issues in the request;
- Explain decisions and reasons fully; and
- Specify timelines for response and relevant dates.

Template letters are available Appendix 4. These templates include details that are required under the legislation to include within certain communications and can be modified by the institution based on the context of the request. Consult the table of contents for a list of the available template letters.

## Requesters

The legislation allows any person to make a request for access to records. A requester is not required to identify or justify the purpose for making a request. The right of access is not limited by citizenship or place of residence.

A person making a request can be an individual or organization. There may be situations where one person represents another individual or an organization.

The legislation allows an individual's rights or powers to be exercised by:

- A person with the written consent of the individual that has been verified (e.g., agent, lawyer).
- A person having lawful custody of a child under the age of sixteen. A person with lawful custody of a child does not have absolute access rights. The exercise of any rights should be in the best interests of child and not for the personal objectives of the custodian.
- A guardian for an individual appointed by a court, or the individual's attorney under power of attorney, or the Public Guardian and Trustee; under the Mental Health Act or Substitute Decisions Act.
- A personal representative of a deceased individual (e.g., executor named in a will, administrator or trustee appointed by a court) only if the exercise of the power relates to the administration of the individual's estate.

In instances where individuals or agents request information on behalf of another individual, institutions will require official documentation to prove an individual or agent has the authority to act on behalf of another individual or organization. Examples of official documentation an institution could accept include:

- Signed consent form accompanied with a photocopy of government issued photo identification;
- A notarized will identifying the name of the executor to an estate;
- A signed affidavit or court order identifying an individual as the guardian to an individual under the age of 16; or
- A notarized Power of Attorney.

## Maintaining Confidentiality of a Requester

When responding to a request for general records, Coordinators should safeguard all information about a requester's identity and the request should remain confidential.

When an individual makes a personal information request, the Coordinator may identify the requester on a need to know basis to other employees in order to locate the records or make decisions on access.

Anyone should be entitled to make a request without being unnecessarily identified and without fear of negative repercussions.

A disclosure of the identity of a requester could be an invasion of an individual's privacy. These confidentiality requirements also apply to privacy complaints and investigations.

## Request Requirements

FIPPA s. 24, s. 48, s. 63 / MFIPPA s. 17, s. 37, s. 50

A request can be made in two ways: formally under the legislation and informally. A request can be made for a general record or for a personal information record.

To be considered a complete request, a formal request for a general or a personal information record must be:

- In writing;
- Include sufficient detail for an experienced employee to identify the record;
- Indicate the request is being made under the legislation; and
- Include a $5.00 application fee.

An individual requesting their personal information must also provide valid identification to the institution prior to receipt of a record. Valid identification may include government issued photo identification such as drivers licence or passport. In instances where no official identification is available, the institution should work with the requester to verify their identity. The application fee cannot be waived.

### Informal Requests

The legislation does not prevent giving access to information in the absence of a formal request. This is referred to as an informal request. Informal requests are not processed under the legislation and allow an institution to handle a request verbally.

To handle a request informally, the individual and institution must be in agreement to do so because the individual loses the opportunity to appeal an institution's decision on access. Any agreement to manage the request informally should be confirmed in writing with the requester.

## Types of Requests

The legislation distinguishes between two primary types of requests:

- General record requests where the requester is asking for general information or information that includes personal information about someone else; and
- Personal information requests where the requester, or authorized representative, is asking for information about himself or herself.

This chapter will primarily address general record requests. Many of the provisions outlined in this chapter apply to both general record requests and personal information requests. For example, time limits for response, clarifying requests, and fee estimates. Where differences exist, such as allowable fees, it will be noted. For additional information and considerations for requests for personal information, see Chapter 8: Personal Information and Correction Requests.

Formal requests can vary in size, scope and complexity. The sections below will examine:

- Routine requests;
- Contentious requests;
- Voluminous requests;
- Continuing access requests; and
- Frivolous and Vexatious requests.

These request types are not specified within the legislation; however, categorizing requests in this manner may be helpful to institutions depending on the volume and complexity of requests received by an institution.

### Routine

A routine request is straightforward in terms of search, content, disclosure, and decision-making. Routine request are requests where responsive records are:

- On a related topic; and
- Frequently requested.

## Contentious

A contentious request is a request where the records contain sensitive information that is likely to be widely disseminated.

There are two criteria that define contentious requests:

- The request is submitted by an individual or organization that may disseminate requested information publicly.
- The records contain sensitive information. In this case, the source of the request is not a determining factor.

The IPC does not oppose the institutions establishing a contentious issues management process as long as the process:

- Does not impact decision making on access;
- Does not lengthen timelines on response; and
- Does not reveal the identity of the requester.

For more information on issues management activities, see Chapter 3: Coordinator Roles and Responsibilities.

## Voluminous

A voluminous request generally involves one or more of the following:

- A search through a large number of records;
- The review of a large number of responsive records;
- The coordination of searches through multiple program areas in the institution;
- Potential interference with the institution's operations; or
- The requirement of additional staff or resources to complete the request.

A time extension may be required when responding to a voluminous request if the request cannot be responded to within the 30 day limit.

Some strategies for working with the requester and managing resources may include:

- Contacting the requester and discussing options to narrow the scope of the request to reduce the time required to respond and fees potentially;
- Working with the requester to agree on a compromise such as offering the requester an opportunity to review the original records and only select those they wish to have copies of;

- Establishing an agreement to a staged release of records based on the requester's priorities; or
- Allocating additional staff resources to work on the request on an ad-hoc or emergency basis.

## Requests for Continued Access

s. 24 / s. 17

A requester can make a request and seek continuing access to the records for a period of up to two years. This is called continued access and applies to general records only (i.e., not personal information). The record must exist at the time of the request.

Continuing access is not intended for records that are only produced once; but rather is intended for records that are produced on an ongoing basis. Continued access is not appropriate where:

- Access is denied in full to the initial request; and
- There is no possibility that future records will come into existence during the two-year continuing access period.

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.

An institution provides the requester with a proposed schedule of dates for disclosure based on a reasonableness test. For example, if a requested record is produced on a quarterly basis, it would be reasonable to establish a quarterly schedule. The institution should provide the requester with a rationale for the schedule. The proposed schedule can be appealed to the IPC.

In practical terms, the original request is brought forward on each of the dates listed in the schedule and processed as if it were made on that day. The $5.00 application fee is required for each of the schedule dates. For convenience, it is advisable for institutions to request payment for application fees in a lump sum. For example, the institution may request $25.00 for five requests. Requesters may also pay individual $5.00 application fees according to the schedule if that is their preferred option.

Each time the request is scheduled to begin, the request needs to be reviewed and an access decision needs to be made. An institution cannot rely on its first decision for subsequent requests in the schedule. As a result, different requests under a single continuing access request may have different decisions on access, depending on the

responsive records in each request and what exemptions or exclusions may apply to the records.

## Frivolous and Vexatious

FIPPA s. 10 (1) (b), s. 24 (1.1), s. 27.1, Reg. 460 (5.1) / MFIPPA s. 4 (1) (b), s. 17 (1.1), s. 20.1, Reg. 823 (5.1)

An institution may issue a decision letter to a requester indicating that no records will be provided if the institution views the request as frivolous or vexatious. 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;
- The requester is acting in bad faith or for a purpose other than access; or
- Responding to the request would interfere with the operations of the institution.

According to the IPC, examples of abuse of process include using the request process to:

- Make repeated requests for the same or similar information;
- Make an excessive number of requests;
- Resubmit a request previously abandoned;
- Make requests that are excessively broad in scope or unusually detailed;
- Coincide with the timing of other events (e.g., court proceedings); or
- Accomplish an objective unrelated to the process (e.g., harass, cause a nuisance, break or burden the system).

A requester's pattern of conduct could unreasonably interfere with the operations of an institution which means that responding to the requests would obstruct or hinder the effectiveness of the institution's activities. The concept of interference is relative to the circumstances and size of the institution.

A request is also frivolous and vexatious when it is made in bad faith. This implies the conscious doing of wrong for a dishonest purpose (e.g., creating a nuisance). It also suggests a state of mind which views the request process with contempt. Bad faith is not simply bad judgment or negligence.

According to the IPC, factors to consider in establishing bad faith include:

- Nature and quality of interaction between the requester and the institution's staff; and
- There is an escalation of a requester's uncooperative and harassing behaviour.

The institution is required to inform the requester why the request is denied and the reasons it is considered frivolous and vexatious.

The requester may appeal a determination that the request is frivolous or vexatious. In the case of such an appeal the institution is required to present evidence that the request is frivolous or vexatious and the IPC will determine if the institution's decision is reasonable.

## Time Limits

FIPPA s. 25 (1) (2), s. 26, s. 27, s. 28 / MFIPPA s. 18 (2) (3), s. 19, s. 20, s. 21

In the context of processing a request, there are time frames for responding to requesters. This is commonly referred to as the "clock."

In general, access requests must be completed within 30 calendar day (i.e., counting Monday to Sunday). The 30 day time limit starts the day the institution receives a complete request and finishes the day the final decision letter is sent.

If the time limit expires on a Saturday, Sunday or statutory holiday, the timeframe for responding to the requester is extended to the next business day of the institution.

The day the request is received is considered "day zero." When calculating the due date for a request, Coordinators should count 30 days starting from the next calendar day from when a request was received.

If a request is received after business hours, the request is generally considered to have been received the next business day. For example, if a request is submitted at 9:00 pm to an office that closes at 5:00 pm, the request will be considered received by the institution the following day.

If an institution fails to issue a decision letter to a requester within the 30 day time limit (if no time extension or notice to affected person is issued), it may be considered a deemed refusal. A requester can appeal a deemed refusal to the IPC.

The table below gives more information on how the 30 day clock is impacted by different administrative actions:

| Issue | Clock Status | Time Limit to Issue Decision | Considerations |
|---|---|---|---|
| Forwarding a request | Clock does not stop. | 30 days | Must be done within 15 days. It is advisable to transfer a request as soon as possible.<br>Clock does not stop while the request is in transit. |
| Transferring a request | Clock does not stop. | 30 days | Must be done within 15 days of receipt. It is advisable to transfer a request as soon as possible.<br>Clock does not stop while the request is in transit. |
| Clarifying a request | Clock does not start until request is clarified with requester. | 30 days from date of clarification | Request must be considered complete in order for the clock to begin.<br>If clarification is required, this indicates the requester has not provided enough information for an experienced employee to locate a record. |
| Fee Estimate /Interim Decision – Fee Estimate Under $100 | Clock does not stop. | 30 days in total unless a time extension is applied | Requesters are not required to pay a deposit on requests where fees are estimated to be below $100. |
| Fee Estimate /Interim Decision – Fee Estimate Over $100 | Clock stops on the date the fee estimate is issued.<br>Clock starts again on the date the fee deposit is received. The institution has | 30 days in total unless a time extension is taken | Requesters are required to pay a 50% deposit when fees for processing the request are over $100.<br>When deposit is paid, the clock starts again. For example, if the institution issues a letter on day 10, the institution has 20 days left to issue a final |

| Issue | Clock Status | Time Limit to Issue Decision | Considerations |
|---|---|---|---|
| | the remaining days to complete. | | decision after receiving the deposit. |
| Notice to Affected Person /Third Party Notice | Clock continues, but request due date changes to be 30 days after the notice is issued. | 30 days from issuing the notice to affected parties decision must be issued to requester.<br><br>Within these 30 days, the affected parties have 20 days to respond to the institution. The institution then has 10 days to issue a decision. | The institution must issue the notice to affected person within 30 days of receipt of the request or within extended time limits. |
| Time Extensions | Clock continues. | The timeline for the extension is not defined in the legislation but is based on a reasonable assessment of time required. | Only one time extension allowed and must be taken within 30 days of receipt of the request.<br><br>Time extensions can only be granted for volume of search or responsive records; or where consultation with an outside individual is required to complete the request.<br><br>If a Notice to Affected Person is issued during a time extension, this may further extend the timelines for response. |

## Administrative Actions to Support Processing Requests

In order to process requests under the legislation, there are various administrative tasks and processes that may need to be completed depending on the circumstances.

The legislation provides rules around these administrative actions. Many of these processes involve communicating with the requester who has the right to appeal to the IPC on the validity of applying some of these provisions.

The sub-sections below provide details on when these actions are required or allowed and what information institutions must communicate to the requester.

### Clarifying Requests

FIPPA 24 (2) / MFIPPA 17 (2)

When a request is not clear and experienced employees of an institution do not have sufficient information to begin a search for responsive records, Coordinators are obligated to clarify the request. The legislation requires requesters to provide sufficient detail to enable an experienced employee to identify the requested records.

It is necessary to clarify a request when:

- The request is open-ended, vague or unclear;
- The record is not described sufficiently to allow an experienced employee to undertake a search; or
- The request comes in the form of a question where no record exists to satisfy the answer.

Clarifying a request can be done by phone or in writing. The institution and requester can work together to reformulate the request. See Appendix 4.3 for a template letter acknowledging a request that requires clarification.

Coordinators can also help the requester better understand what types of records may be responsive to a request and what is, and is not, available in response to the request. In addition, it may be helpful for Coordinators to explain processing fees and provide an estimate of costs, if possible. Potential fees are often an important consideration for a requester. With this knowledge, the requester can then decide how to proceed.

After a request has been clarified it should be clear to both the institution and the requester what records are being requested. For an institution this means that an experienced employee will be able to identify the requested records. This agreement should be confirmed in writing and essentially makes the request complete.

## Narrowing a Request

Sometimes a request will capture a significant number of records, because of the way it has been worded (e.g., “access to any and all records”) or due to an extensive timeframe for the record search. A broad request can still provide sufficient detail to identify records. Narrowing a request refers to reducing the scope of the request (e.g., reducing a request for three years of records to one year of records).

Narrowing the scope of a broad request is not considered to be a clarification if the original request provided the institution with sufficient detail about the requested record, and narrowing simply reduces the scope.

Coordinators should work collaboratively with requesters to narrow the scope of a request. Alternatively, the Coordinator can choose to interpret the request literally, which may involve an institution-wide search for records and potential time extensions.

## Forwarding a Request

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

Sometimes a requester may send a request to the wrong institution. When a request is received and the institution does not have custody or control of the records, the legislation requires that:

- Inquiries be made to determine if another institution has responsive records; and
- The first institution should forward the request to the institution, as required.

Requests can only be forwarded between any provincial or municipal institutions.

Coordinators should take action to forward the request within 15 days or as soon as possible, because the clock will continue to run while the request is being forwarded.

Coordinators should take the following steps:

- Make reasonable inquiries to determine if another institution has the record if unknown;
- Notify or telephone the Coordinator at the correct institution;
- Forward the request and determine whether to:
    - Return the application fee payment (e.g.: cheque or money order) to the requester and advise them to submit a new payment to the correct payee;

- Forward the application fee to the new institution (if the institutions are the same payee); or
- Deposit the application fee on behalf of the receiving institution (if the institutions are the same payee); and

- Notify the requester about the new contact in writing.

See Appendix 4.5 for a sample template letter to use when notifying a requester a request has been forwarded or transferred to another institution. See Appendix 4.6 for a sample template letter to use notifying another institution when a request has been transferred or forwarded.

## Transferring a Request

FIPPA s. 25 (2) (3) / MFIPPA s. 18 (2) (4)

An institution may receive a request that applies to records that another institution may have a greater interest in, and it would be more appropriate that the other institution make a decision on access. Often this occurs when institutions share records for the purpose of seeking advice or when partnering or collaborating on a project.

The legislation allows a request and a record to be transferred to any provincial or municipal institution. The purpose of transferring a request is to ensure the institution best positioned to make an access decision may do so.

Transferring a request and record is discretionary which means an institution is not obligated to do so. Institutions may also transfer a request in part, where each institution issues decision letters on the records that the institutions have a greater interest in disclosure.

An institution has a greater interest in a record than another institution if:

- The record was originally produced in or for that institution; or
- The other institution was the first institution to receive the record or a copy of it.

Coordinators should take action to transfer the request within 15 days or as soon as possible, because the clock continues to run while the request is being transferred.

Coordinators should take the following steps:

- Make reasonable inquiries to determine if another institution has a greater interest in the record if unknown;
- Notify or telephone the Coordinator at the institution;

- Transfer the request and determine whether to:
    - Return the application fee payment (e.g.: cheque or money order) to the requester and advise them to submit a new payment to the correct payee;
    - Transfer the application fee to the new institution (if the institutions are the same payee); or
    - Deposit the application fee on behalf of the receiving institution (if the institutions are the same payee); and
- Notify the requester about the new contact in writing.

See Appendix 4.5 for a sample template letter to use when notifying a requester a request has been forwarded or transferred to another institution. See Appendix 4.6 for a sample template letter to use notifying another institution when a request has been transferred or forwarded.

## Records of Other Governments

Institutions can only forward or transfer requests to provincial or municipal institutions. Therefore institutions cannot forward or transfer a request to the federal government, another provincial government, a municipality outside of Ontario or the government of another country.

When a requester sends a request to the wrong government, Coordinators should return the request and application fee to the requester and advise them to re-submit the request to the appropriate government.

## Time Extensions

FIPPA s. 27/ MFIPPA s. 20

The legislation allows a time extension where it is unreasonable to complete the request within the 30 day time limit. The legislation is not explicit about the amount of allowable time so any time extension must be reasonable and justifiable.

A Coordinator should consider all of the potential factors that may contribute to the need for a specific length of a time extension. A decision to extend the time limit must be made within the 30 day limit and the requester must be given notice. Only one time extension can be taken for each request. It is generally best practice to inform the requester of the time extension concurrently with informing the requester of estimated fees (if any). More information on fee estimates is provided later in this chapter.

Time extensions are permitted for two reasons:

- When requests that have a high volume of records to search or review and the extensive search and review would unreasonably interfere with operations; and
- When requests require consultations with a person or organization outside the institution in order to complete the request.

The IPC encourages institutions to work with requesters to find practical solutions when several requests are submitted at one time. Time extensions for a request are determined on a case by case basis.

Factors generally found to support a time extension include:

- A large number of records requiring careful review; and
- A substantial amount of time required to prepare records at a critical operational time requiring staff to attend to their duties.

Factors generally found not to support a time extension include:

- The number of requests being processed at any given time;
- Staff vacation;
- The expense of producing a record where the expense is caused by the size, number or physical location of records.

Written notice must be provided to the requester when a time extension is being applied. The institution must communicate to the requester:

- The reason for the time extension;
- The length of the time extension and the new due date for the request; and
- That the requester has the right to request the IPC review the decision by the institution to apply the time extension.

See Appendix 4.7 for a template letter notifying a requester of a time extension.

## Consultations

FIPPA s. 27/ MFIPPA s. 20

The purpose of consultations is generally to obtain information or advice that can inform decision-making. Consultations are different from providing notices to affected persons as discussed below.

Consultations may be required with a person (e.g., past employee) or organization (e.g., other governments) outside the institution who may have knowledge of the records at

issue. For example, a consultation may be required when responsive records to a request include records prepared by another government body and subject matter expertise is required in order to make a decision on access.

The legislation allows a time extension for consultations that is reasonable in the circumstances.

## Notice to Affected Person (Third Party Notice)

FIPPA s. 28 / MFIPPA s. 21

Some records responsive to a request may contain information concerning an affected party such as a person other than the requester. In these instances, institutions are required to provide notice to the affected persons. Further, the institution must provide a notice of delay to the requester regarding the notice process.

A notice to an affected party must be given if the institution has reason to believe that the records might contain third party information or contain personal information of an identifiable individual, and the institution is contemplating disclosing the records.

The notice process gives the affected party an opportunity to make representations about the proposed disclosure of records that affect them. The threshold for determining if the third party information exemption applies to a record is very low. This means that institutions should carry out the notice to affected persons process whenever the responsive records “might” be subject to this exemption. Observing a low threshold ensures procedural fairness and reduces the risk that exempted information is disclosed in error.

A notice to the affected person must include the following information:

- A statement that the institution intends to release a record or part of a record that may affect the interests of the person or organization;
- The contents of the record or the part that relates to the affected person;
- That the affected person must make representations in writing as to why the record in whole or in part should not be released; and
- That the affected person has 20 days after the notice is given to reply.

There is discretion to hear representations verbally if necessary.

Affected persons may not be familiar with the legislation. It is advisable that Coordinator’s contact affected to explain the notice process and answer any questions they may have. It is also helpful to provide:

- Copies of the relevant sections of the legislation; and
- An actual copy of the record where practical.

After the 20 day time limit for response from the affected party has elapsed, institutions have 10 days to issue a decision on access to the requester.

Institution's may agree or disagree with the response from an affected person. The affected person has a right to appeal the institution's decision on the access request regardless of whether the institution agrees or disagrees with their response. As a result, the institution must hold the records until the appeal period of 30 days has past. Once the appeal period has passed, the Coordinator should confirm with the IPC that no appeal has been received before releasing the records to the requester (subject to payment of fees).

If records capture information that is not subject to notice, institutions should disclose the records which are not subject to the notice at the time the decision letter is issued (subject to the application of other exemptions and exclusions and payment of fees).

The timelines stated above may be extended if the 20 day response time presents a "barrier" as defined by the Accessibility for Ontarians with Disabilities Act. Under that legislation, a barrier means "anything that prevents a person with a disability from fully participating in all aspects of society because of his or her disability, including a physical barrier, an architectural barrier, an information or communications barrier, an attitudinal barrier, a technological barrier, a policy or a practice."

When timelines are extended for the notice to affected due to accessibility reasons, the requester should be informed of the new expected due date for response.

See Appendix 4.10 for a template letter providing notice to affected person for third party information. See Appendix 4.11 for a template letter providing notice to affected person for personal privacy. Finally, see Appendix 4.12 for a template letter to provide notice to requester of delay where a third party's interests are impacted.

## Fees

FIPPA s. 57, Reg. 460 (5.2), (6), (6.1) / MFIPPA s. 45, Reg. 823 (5.2), (6), (6.1)

The legislation adopts a user pay principle. This means an individual making a request must pay some of the costs the institution incurs to process the request.

For this reason, a requester must have sufficient information to review the costs and decide how to proceed.

Fees must be calculated for every request starting from the time a request is received. The fees apply to time, materials and services. The fees are set out in the regulations.

Fees must be charged unless they are waived by the institution, or unless another statute has an overriding provision for charging fees.

Fees and fee estimates can be appealed to the IPC. Fees and fee estimates should be detailed and reasonable. The IPC can order institutions to lessen or change fees if they find the institution has erred in their calculation of fees.

## Types of Fees

Reg. 460 (5.2), (6), (6.1) / Reg. 823 (5.2), (6), (6.1)

The fees that are chargeable under the legislation are described below. Note that not all fees can be charged for personal information requests.

Federal and provincial sales tax is not chargeable for application and processing fees.

**Application fee:** A $5.00 application fee is required for all requests. Failure to collect the application fee may not prevent the IPC from hearing an appeal about a request that has been completed.

**Search time:** Institutions may charge $7.50 per 15 minutes for each staff member's time to manually search for responsive records. Searching includes examining file plans, listings of records and paper or electronic searches.

Search time cannot be applied to other administrative tasks such as photocopying and travel to offices.

Search time can only be charged for general record requests and not personal information requests.

**Preparation time:** Institutions may charge $7.50 per 15 minutes for each staff member's time to prepare records for disclosure. Preparation includes severing a record, activities required to generate computer reports and running computer reports, and scanning records into digital format.

Preparation time cannot be applied to other tasks such as reviewing records for relevant exemptions and exclusions, photocopying records, preparing an index of records, preparing records for third party notice, or transporting records.

Preparation time can only be charged for general record requests and not personal information requests.

**Computer time:** $15.00 per 15 minutes for any person developing a computer program or other method of producing a record from a machine readable record.

Computer time cannot be applied to existing search functions to generate reports, SQL queries or data manipulation.

**Photocopies and computer printouts:** Institutions may charge $.20 per page to photocopy or print material for disclosure. Double-sided copies count for 2 copies.

**Compact Disks:** Institutions may charge $10.00 per disk for disclosing records in electronic format.

**External Services:** Institutions may charge for work that is required to be completed that cannot be done by internal staff due to the specialization required. An example would be reformatting or copying rare media types. In order to charge this fee, institutions must receive an invoice for the cost of the outside service.

This fee cannot be applied to work that could be completed by an institution's staff, even if an invoice exists.

**Shipping:** Institutions may charge for postage and courier delivery for disclosed records.

See Appendix 6 for a Sample Fee Estimate Form program areas can use to calculate and document fee estimates.

## Estimating Fees and Interim Decisions

FIIPPA s. 57 (3), Reg. 460 (7) / MFIPPA s. 45 (3), Reg. 823 (7)

Institutions have different notice requirements depending on the estimated amount of fees required for processing the request.

Three thresholds for fees and steps Coordinators should follow are outlined below.

**Fees less than $25:** The institution is not required to send a fee estimate to the requester for fees less than $25.00. The institution completes all necessary work and notifies the requester of the fee amount to be paid in the final decision letter. Fee payment is required before records are released.

**Fees between $25 and $100**: The institution must notify the requester of the approximate fee. No deposit is required for fees in this range and the institution completes all necessary work and issues a final decision letter. Fee payment is required before records are released.

**Fees in excess of $100:** Institutions must prepare a detailed fee estimate with an interim decision letter. The institution may require a 50% deposit before taking further action on processing the request. This means the "clock" is stopped and the request is on hold until the institution receives the deposit. Upon receipt of the deposit payment, the institution completes all necessary work and issues a final decision letter with the final fee calculation. Fee payment of the remaining balance is required before records are released.

An interim decision is not final or binding and cannot be appealed. An interim decision also lets the requester know what exclusions and exemptions may apply to the records and that a fee waiver can be claimed by the requester.

While the initial determination that some exemptions are likely to apply cannot be appealed, requesters may appeal fee estimates to the IPC.

When a search is required through a large number of records or where a large number of records are responsive to a request, a fee estimate for searching records can be calculated using a representative sample. A representative sample should be complete and include:

- A search of all types of records (e.g., paper, electronic, special media);
- A reasonable sample size of a computer file folder, drawer, storage box; and
- A useful measurement is a paper stack where one-inch of paper holds about 150-200 single-sided pages.

The estimated total search time can be calculated using:

- Number of hours to search the sample;
- Number of responsive pages in the sample;
- Number of pages requiring severances;
- Number of severances per page; and
- Any additional work estimated to complete the request.

It is best practice to inform the requester of any time extension when providing a fee estimate and interim letter as this information will impact the requester's decision to pay a fee deposit.

See Appendix 4.8 for a sample template letter to use for fee estimates and interim decisions where the fee estimate is between $25.00 and $99.00. See Appendix 4.9 for a sample template letter to use for fee estimates and interim decisions where the fee estimate is $100 or more.

## Payment of Fees

Institutions generally receive payment for application and other fees by cheque, though other forms of payment are acceptable (e.g., electronic, money order, cash). Institutions cannot stipulate how payment is made. Also, institutions are not required to accept methods of payment they are not set up to do so (e.g., credit card, electronic transfer).

For provincial ministries and some agencies, boards and commissions cheques are made payable to the "Minister of Finance". For other provincial and municipal institutions, cheques are payable directly to the institution.

## Waiving Fees

FIPPA s. 57 (4), Reg. 460 (8) / MFIPPA s. 45 (3), Reg. 823 (8)

Processing fees are mandatory under the legislation; however, a requester may seek a fee waiver. Institutions must notify requesters of their right to request a fee waiver when issuing fees or fee estimates. A requester is responsible for submitting a request for a fee waiver and providing a rationale as to why granting a fee waiver would be fair and equitable.

The legislation and regulations lists factors for institutions to take into account when determining whether granting a fee estimate would be fair and equitable. These factors include:

- The extent to which the actual cost of processing, collecting and copying the record varies from the amount of payment required;
- Whether the payment will cause a financial hardship to the requester;
- Whether the access to the record will benefit public health or safety;
- Whether the requester gets access to the record; and
- Whether the amount of the payment is too small to justify requiring payment (e.g., $5.00 or less).

While the institution must consider these factors, these factors do not necessarily need to be present in order for the institution to grant a full or partial fee waiver.

Other relevant factors should also be considered when deciding whether or not a fee waiver is fair and equitable. These include:

- The manner in which the institution attempted to respond to the appellant's request;
- Whether the institution worked with the appellant to narrow and/or clarify the request;
- Whether the institution provided any documentation to the appellant free of charge;
- Whether the appellant worked constructively with the institution to narrow the scope of the request;
- Whether the request involves a large number of records;
- Whether or not the appellant has advanced a compromise solution which would reduce costs; and
- Whether a fee waiver would shift an unreasonable burden of the cost from the appellant to the institution, and cause significant interference with the operations of the institution.

If a requester seeks a fee waiver, they must submit the request for the waiver in writing. Institutions are required to review and decide whether or not to grant a full or partial fee waiver. The institution's decisions to grant or not grant fee waivers may be appealed by the requester to the IPC.

## Abandoned or Withdrawn Requests

When a requester communicates to an institution that they are no longer seeking access to the requested information, the request can be considered "withdrawn." Coordinators should retain documentation, such as email correspondence with the requester that shows the requester's intent to withdraw the request. When a requester withdraws a request verbally, it is best practice to confirm this intention in writing.

When a Coordinator has attempted to contact a requester in order to proceed with processing the request and has not had a response from the requester, the request can be considered "abandoned." The IPC advises institutions to allow 30 days to pass before marking a request as abandoned for general record requests. For personal information requests, the IPC advises allowing one year for response before closing the request.

Requesters should be notified in writing that their request may be abandoned. The letter should state the exact date at which the institution will close the file if no response is received. Institutions may choose to include this in a fee estimate letter or clarification letter; or write a separate abandonment letter.

See Appendix 4.20 for a sample template letter to use to advice requesters their request will be considered abandoned if no response is received by the institution.

## Request Processing Step by Step

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

Responding to requests is a collaborative process that includes a number of steps. The sections below outline these steps at a high level. Not all steps may be required for processing all requests depending on the institution and the context of the request.

## Step 1: Receiving a Request

The legislation requires that requests be received by the institution in writing and accompanied with a $5.00 application fee. For practical reasons, most institutions can only receive requests by mail or in-person delivery. Some institutions may have the ability to receive requests online or via fax.

Once a request is received, Coordinators and their staff should:

- Review the request to ensure the request is complete, which means the request is in writing, includes the $5.00 application fee, and provides sufficient detail.
- Open a file, assign a file number, and calculate the 30 day time limit for a response. Note that if the due date falls on a Saturday, Sunday or holiday, the due date is moved to the next business day.
- If the institution is using an electronic case file management system, update the system.
- Make copies of the original request to work with.
- Make copies of any administrative forms to put in the file.
- Notify the program area or a program contact if known, of a request.

Coordinators should communicate to the office or offices that are likely to have responsive records (program area) and provide them with the following information:

- Wording of the request;
- Instructions for conducting the search and recording actions and time taken;
- Timelines for completing the record search; and
- Instructions on how to deliver copies of responsive records to the FOI office.

Coordinators should contact requesters immediately if the request is missing the application fee or requires clarification in order to proceed. See Appendix 4.2 for a template letter acknowledging receipt of a request that requires a $5.00 application fee and Appendix 4.3 for a template letter acknowledging receipt of a request that requires clarification.

## Step 2: Assessing a Request

For routine requests, Coordinators can proceed directly to searching for records or finalizing recommendations and a decision. However, for many requests, additional steps may be required to assess how to proceed with processing a request.

In all instances, it is best practice for the institution to send an acknowledgement letter to the requester confirming the receipt of the request. This acknowledgment letter should include the request number assigned to the request, indicate the date of receipt of the request and provide contact information of the staff member responsible for processing the request. See Appendix 4.1 for a template letter for a standard acknowledgement letter.

Coordinators or their staff should discuss the request with the program area that is likely to have responsive records in order to understand their business, any concerns, possible impact of the search on operations, and alternate ways to respond.

If the request has been sent to your institution in error, or if another institution has a greater interest in the disclosure of the record, Coordinators should take reasonable steps to determine which institution should receive the request and forward or transfer the request.

Coordinators should determine if the request provides sufficient detail for an experienced employee to locate responsive records. If the request does not have sufficient detail, Coordinators should clarify the request with the requester.

If it is determined that a request is considered contentious, Coordinators should notify their issues management team of the request and timelines for response.

## Step 3: Searching and Locating Records

The legislation requires that institutions complete a “reasonable search” for responsive records to a request. A search is considered reasonable when an experienced employee expending reasonable effort conducts a search to identify any records that are reasonably related to the request in locations where records in question might

reasonably be located. An institution does not have to prove absolutely that no records exist but, only that it conducted a reasonable search.

IPC appeals respecting the adequacy or reasonableness of a search often require an institution to demonstrate that steps were taken to work cooperatively with a requester in scoping their request.

The following are the essential steps that should be taken into consideration in order to conduct a reasonable search.

**Clearly understand the search parameters:** Requests must be reviewed in detail by the Coordinator and affected program areas responding to ensure there is a clear understanding of what is being requested. Clarification is an important first step and should be undertaken as soon as possible after receipt of the request where a request is unclear or ambiguous. Refer to the section on clarification for more information.

**Initiate the record search and ensure all relevant documents are retained:** The Coordinator should immediately notify all program areas that may have responsive records to alert them about the request and to ensure that potentially responsive records are secured.

**Identify staff to conduct searches:** Experienced staff with knowledge of the subject matter of the request and the records management system should oversee and/or conduct searches for responsive records.

Institutions should also assign program area contacts to be responsible for overseeing search efforts in their program. These individuals should work in consultation with the Coordinator to ensure they are familiar with the requirements to fulfil a reasonable search.

**Provide clear search instructions:** Ensure all employees participating in the search are provided with clear written instructions about what to search for and how to conduct the search. Consider including a step-by-step guide instructing staff how to conduct email, electronic and paper record searches. Coordinators should work with program areas to develop step-by-step guides relevant to the records management practices in those offices.

Specify a date to complete the search, keeping in mind the legislated timeline for response and all of the tasks associated with completing the file. Time extensions may be required in appropriate circumstances and should be discussed with the Coordinator as soon as possible.

**Identify all databanks and places to be searched and develop a search plan:** Experienced staff with knowledge of the subject matter of the request and/or with special knowledge of the institution's record holdings should be the ones to identify the databanks and places to be searched.

Searches must include all record repositories that may reasonably be expected to contain responsive records including: on-site file storage and off-site storage facilities. In this regard, records retention schedules and file plans for each office should be consulted.

In general, a search of electronic records should be undertaken where such records may reasonably exist in the electronic recordkeeping environment established by an institution, including email accounts, shared drives, electronic archives, and other electronic storage systems.

Exceptionally and in extraordinary circumstances, a search of a system maintained for disaster recovery purposes (e.g. back-up tapes) may be considered, for example, where evidence exists that responsive records may have been deleted or lost out of the normal recordkeeping environment and the lost records are likely to be located on the back-up tapes. In these cases, consultations should be undertaken with the institution's Coordinator, records management leads, Legal Counsel and information technology staff prior to commencing a search.

**Document search steps:** All staff who participated in the search for responsive records should document their search steps including their name, the date they conducted a search, the databanks, the types of files, and other record holdings searched, and finally their search results (even when a search does not locate records).

In case of an appeal, an institution should be prepared to verify in an affidavit:

- Staff who conducted the search;
- Staff qualifications, position, and responsibilities;
- The dates staff conducted the search;
- Information about the type of files searched;
- The nature and location of the search; and
- Any further steps undertaken.

The affidavit should be signed by the person who conducted the search or was responsible for overseeing it.

See Appendix 5 for a sample template form program areas can use to document search activities. Also see Appendix 6 for a sample template fee estimate form program areas can use for extensive searches that may require a fee deposit before work is completed.

## Step 4: Reviewing and Analyzing Records

When the search has been completed and all responsive records have been identified, the next step is for Coordinators or their staff to review and analyze the records.

The program area that conducted the search may conduct a preliminary review of the records and identify any concerns regarding access. As the program area is the custodian of the record, they are often in a better position to understand the context of the records. For example, the program area would know whether records received by a third party were supplied in confidence.

A review of records requires careful examination of the content of records, in consideration of how the legislation applies to make an access decision. The process of reviewing records is iterative and may take place numerous times until a final decision is made.

Reviews and consultation may be necessary with program areas, Legal Counsel and decision-makers. In the review process, it may become evident that the following additional steps may be required:

- Issuing a time extension for volume of records or consultations;
- Notifying an affected person; and/or
- Issuing a fee estimate and interim decision.

Institutions should include the responses from affected parties in their analysis when determining whether an exemption applies to a record.

If the request is for access to personal information for research purposes, Coordinators should consider whether a research agreement would be appropriate. More details on research agreements are provide later in this chapter.

Coordinators and their staff should research IPC orders and judicial review case law for interpretation of the relevant sections of the legislation. Guidance documents and internal policies and procedures may also be helpful in determining whether exemptions or exclusions apply to a record.

Coordinators should review previous decisions they have made regarding access to similar records for consistency. However, Coordinators should not rely on past

decisions alone as the legislation may have been amended, or new case law may exist that has changed interpretations of the legislation.

The legislation requires that institutions only sever the information that is subject to exemptions or exclusion. Institutions should take steps to sever only exempted information and disclose as much of the records as can be reasonably disclosed without revealing the information that falls under one of the exemptions or exclusions.

A requester must be notified of the section or sections that apply to the severed information. This should be noted on the record beside the severed information. In some instances where few exemptions are cited, this information can be summarized in the decision letter to the requester.

Severing should not be applied where the legislation exempts an entire class of records or where severing would leave only disconnected pieces of information within a record. For example, an entire Cabinet agenda would be exempt under the Cabinet records exemption. In this case, the record should be withheld in full. Institutions should inform the requester of the number of pages of records that have been withheld in full and the exemption or exclusion that applies.

Coordinators may consider creating an index of records to help organize information to respond to the request. The index of records typically includes sufficient detail to support decision-making. In the event of an appeal, the IPC will require the institution to create an index of records for any records that have been severed or withheld in full.

An index of records should include:

- The assigned document number to each record;
- Date of the record;
- Page number/paragraph;
- A general description of each record;
- The exemption or exclusion claimed (if any); and
- Indicate whether access has been granted or refused for all or part of the record.

The index of records should not include personal information or other information that would reveal the substance of an exemption. For instance, the index of records should not reveal the substance of a Cabinet meeting or the subject of solicitor-client privilege communication.

See Appendix 7 for a sample template index of records.

## Step 5: Finalizing Recommendations and a Decision

Finalizing recommendations and a decision on disclosure involves preparing records and a draft final decision letter to the requester, as well as getting approvals and sign-off from decision-makers. Approvals processes will vary depending on the request and an institution's delegation of authority.

It is best practice to document the recommended decision in writing by preparing a briefing note. The requirements for recommendations on access will vary amongst institutions. Briefings may not be required for all requests. Routine requests may be processed without detailed documentation.

A briefing note can form the basis for future appeal submissions to the IPC, if access decisions are appealed. A briefing note is especially useful in an institution where decision-making has been delegated to senior officials who need relevant and concise information to make an informed decision.

A briefing note will typically contain six sections:

**Background:** This section of the note should describe the request either as it was received, or in its clarified form. Other relevant matters that may help put records in context should also be described, for example, the current status of a program or initiative that records relate to. It may be important for a decision-maker to know whether a program is in the planning, pre-implementation or operational stage of development, as there are different considerations regarding the release of records, depending on the maturity of the project.

Additional information, such as the outcome of any past requests for the same or similar information, should also be described in this section.

**Description of records:** This section should describe the different types of responsive records. Listing the broad categories of documents is sufficient along with the general content of the records. This description should identify which program areas conducted the search for responsive records.

When a request is voluminous, an index of records may be prepared for the decision-maker to review.

**Analysis:** This section of the note provides decision-makers with an understanding of how any recommended exemption or exclusion applies to the requested records, and, more importantly, why there is a need under the circumstances that exist at the time of the request to withhold information.

Highlighting relevant case law and/or describing similar decisions previously made by the institution will help assure the decision-maker there is a sound legal basis for the decision. Where there are complex legal points, it may be sufficient to provide an overview and confirm that the Coordinator and Legal Counsel were consulted and have endorsed a particular recommendation.

**Exercise of discretion:** This section should list the relevant factors considered by the Coordinator in conducting an exercise of discretion. This will ensure that the decision-maker has undertaken the required exercise of discretion, and will serve as evidence of that fact if the institution's decision is appealed to the IPC.

**Fees:** This section should provide the decision-maker with background information on how fees were calculated, especially for requests where a large fee estimate was issued and/or there is a possibility that fees may become an issue on appeal.

A decision-maker may be required to decide whether or not to waive fees associated with processing a request. Where a request for a fee waiver has been requested this can be noted in this section along with the reason for the fee waiver request.

**Recommendation:** This section provides a clear statement of the recommended access decision. Access recommendation statements can include:

- Access is provided to the records in full;
- Access is provided to the records in part, noting the exemptions or exclusions that are claimed,
- Access is withheld in full, noting the exemptions or exclusions that are claimed; or
- Access cannot be provided as no responsive records exist.

Other possible decisions, such as the application of fees or the granting of a fee waiver, should also be stated.

Reasonable steps should be taken to ensure approvals are finalized within legislated timelines.

## Step 6: Preparing and Sending Records

Upon approval of the access recommendation, Coordinators and their staff should take steps to issue the final decision letter to the requester and prepare records for disclosure.

A decision letter outlines to the requester the final decision on granting or denying access to a record. The legislation outlines requirements for decision letters. The list below includes legislated requirements and best practices based on the circumstances of the request:

- The volume of responsive records located;
- What records are being released in full;
- The exemptions and exclusions applied (if any);
- The number of pages severed or withheld for each exemption or exclusion;
- Copies of the relevant sections of the legislation;
- If any fees apply, the final calculation of fees and required payment;
- If any fees apply, information on requests for fee waivers;
- The name and position of the decision-maker for the request;
- For high volume requests, consider including a copy of the index of records;
- Notice that the requester can appeal the decision to the IPC within 30 days and appeal requirements; and
- Contact information for an individual who can answer questions regarding the processing of the request.

Disclosure of responsive records may be dependent upon receipt of final fee payment and/or allowing 30 days for affected parties to appeal decisions on access.

The legislation allows a requester the option to:

- Receive a copy of all or part of a record;
- Examine an original record; and
- Request a copy of all or part of a record after examining a record.

The legislation qualifies the above by using the term where it is reasonably practicable to do so. The particular facts of each case must be considered before making a decision.

A requester may seek records in a preferred format when it is reasonably practical for the institution to do so. An example is providing electronic copies of records that only exist in paper form.

A requester must be given a copy of what has been requested unless there is good reason not to provide copies. Copies of records must be clean and legible when possible. A copy of a record should be clearly marked where copyright protection applies.

It may not be reasonably practicable to examine original records because of:

- Age and condition of records;
- Physical location of records;
- Size or volume of records;
- Cost of transporting records to a convenient site;
- Security of the records cannot be ensured and original records could be damaged, altered, or stolen;
- Undue inconvenience or disruption of operations of the institution; and
- Legal requirements for maintaining records on site.

It is recommended to have staff present when a requester is viewing original records especially if some of the responsive information is being withheld under an exclusion or exemption.

See Appendix 4 for template decision letters.

## Step 7: Closing the File

Upon issuing the final decision letter, the request case file should be closed and information related to the request should be recorded for statistical compliance purposes.

If an institution is using a case file management system, staff should update the system to indicate the date the final decision was communicated to the requester, the outcome of the request including whether or not any exemptions or exclusions were applied to the records.

The request case file should be kept in an accessible location for the 30 day appeal period and in accordance with records retention schedules or policies.

## Research Agreements

FIPPA s. 21 (1) (e), Reg. 460 (10) / MFIPPA s. 14 (1) (e), Reg. 823 (10)

In the context of a request, personal information may be disclosed for research purposes under a research agreement when certain conditions are met. "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 the legislation. "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.

The conditions that need to be met in order to provide access to personal information for research purposes include:

- The disclosure is consistent with the conditions or reasonable expectations of disclosure under which the personal information was provided, collected or obtained;
- The research purpose for which the disclosure is to be made cannot be reasonably accomplished unless the information is provided in individually identifiable form; and
- The person who is to receive the record has agreed to comply with the conditions relating to security and confidentiality prescribed by the regulations.

A research agreement that the institution and researcher enter into governs the conditions listed above. The regulations under the legislation reference the standard agreement available on the Central Forms Repository of the Government of Ontario. The following links direct users to downloadable versions of these template agreements for FIPPA and MFIPPA.

The following considerations should be included in a research agreement:

- The researcher must agree to use the information only for a research purpose set out in the agreement or for which the person has written authorization from the institution;
- The agreement must name any other persons who will be given access to personal information in a form in which the individual to whom it relates can be identified;
- The researcher must keep the information in a physically secure location to which access is given only to the person and to the persons authorized;
- The researcher must destroy all individual identifiers in the information by the date specified in the agreement;
- The researcher must not contact any individual to whom personal information relates, directly or indirectly, without the prior written authority of the institution; and

- The researcher must notify the institution in writing immediately if the person becomes aware that any of the conditions set out in this section have been breached.

## Case File and Knowledge Management

In order to manage the request process, institutions must implement a case file management system, whereby information associated with requests is easily accessible.

Case file information may be managed either with an electronic case file management system, a manual register such as excel spreadsheets, or in paper format.

In addition to case file management Coordinators should maintain documentation to support decision-making. To ensure effective knowledge management, resources that should be maintained include:

- Guidance and resources from MGCS and the IPC;
- Case law established by IPC orders and court decisions;
- An institution's corporate policies, guidelines and standards; and
- Relevant resources and trends in other jurisdictions as required.

Coordinators should routinely review active request files to ensure the request is on track to completion within the legislated timelines. Part of this review should include ensuring proper documentation exists for administrative actions taken on the request.

Coordinators should contact their institution's records management office for more information on their institution's records retention policies and procedures.

## Statistical Reporting

FIPPA 34 / MFIPPA 26

All institutions need to meet the reporting requirements of the IPC for annual reporting. The IPC publishes guidelines and procedures to be followed on their internet site.

The following information should be tracked for statistical reporting purposes:

- Number of requests received and completed within reporting year;
- Type of record requested (e.g., general or personal information);
- Number of requests for correction received and completed within a reporting year;

- Request source (e.g., individual, agent, business, media, academic, association, government);
- Number of requests transferred to or from another institution
- Number of requests responded to within 30 days, 31-60 days, 61-90 days and more than 90 days;
- Number of requests where timelines were extended under allowable time extension;
- Number of requests where notices to affected parties were issued;
- Number of requests completed within legislated timelines, including extended timelines;
- Disposition of request:
    - All information disclosed
    - Partial information disclosed
    - No information disclosed
    - Request withdrawn or abandoned
    - No records exist
- Frequency of application of exemptions or exclusions to a request; and
- Fees collected and fees waived

Institutions may find it useful to track other information that may help plan, assign resources or improve performance.

## Resources

Appendix 4: Template Letters Request Processing

Appendix 5: Sample Records Search Form

Appendix 6: Sample Fee Estimate Form

Appendix 7: Sample Index of Records

IPC: Fact Sheet – Frivolous and Vexatious Requests

IPC: Fact Sheet – Reasonable Search

IPC: Fees, Fee Estimates and Fee Waivers

IPC: Practice 15 – Clarifying Requests

IPC: The Year-End Statistical Report for the IPC - Workbook and Completion Guide, FIPPA

IPC: The Year-End Statistical Report for the IPC: Workbook and Completion Guide, MFIPPA

Ontario Central Forms Repository: Access or Corrections Request Form

Ontario Central Forms Repository: Security and Confidentiality Agreement of Personal Information for Research Purposes - FIPPA

Ontario Central Forms Repository: Security and Confidentiality Agreement of Personal Information for Research Purposes - MFIPPA

# Part III: Protection of Privacy

# Chapter 7: Privacy Fundamentals

## Introduction

One of the primary purposes of the legislation is to protect the privacy of individuals with respect to their personal information in the custody or control of institutions. This chapter introduces the concepts of privacy protection and personal information.

The legislation protects privacy by providing rules for institutions to follow for the collection, use, disclosure, accurate maintenance, retention, security and disposal of personal information. This chapter reviews these privacy rules in detail and outlines how institutions can be compliant with the legislation.

Chapter 8: Personal Information and Correction Requests explains special considerations for requests for an individual's own personal information and requests to correct personal information in the custody or control of an institution. Chapter 9: Privacy Management provides best practices for how institutions can create a privacy management program to ensure compliance with the legislation.

Some institutions may also be subject to the Personal Health Information Protection Act. These institutions will have additional considerations for rules regarding the collection, use and disclosure of personal health information within their custody. This chapter does not provide guidance on this topic, and institutions should refer to the IPC for more information.

## Understanding Privacy

The legislation does not define privacy explicitly. The legislation defines personal information and sets out privacy rules regarding the collection, use, disclosure, retention, security, disposal and destruction of personal information that institutions must follow.

The legislation protects privacy by:

- Providing rules as to what and how personal information can be collected by institutions;
- Providing rules on how institutions handle, manage, and share personal information between institutions and other government organizations; and
- Establishing procedures for individuals to access their own personal information, subject to some necessary and defined exemptions.

## Personal Information

FIPPA s. 2 / MFIPPA s. 2

The legislation defines personal information as recorded information about an identifiable individual. Personal information does not include information about an individual that has been deceased for more than 30 years.

Information will likely qualify as personal information if an individual can reasonably be identified from either the information alone, or from the information in combination with other information.

An important exception to the definition of a “record” is that personal information may also include information that is not recorded (e.g., a verbal disclosure).

Personal information includes, but is not limited to:

- Name
- Personal address
- Personal email address
- Personal telephone number
- Race
- National origin
- Ethnic origin
- Skin colour
- Religion
- Age
- Date of birth
- Sex
- Sexual orientation
- Marital status
- Family status
- Education
- Medical history
- Employment history
- Financial transactions involving the individual
- Identifying number
- Identifying symbol
- Photograph of the individual
- Other identifying particular
- Finger prints

- Blood type
- Correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, or replies to the correspondence that would reveal the contents of the original correspondence
- The personal opinions or view of the individual except where they relate to another individual
- The views or personal opinions of another individual about the individual

## Business Identity Information

FIPPA s. 2 (3), s. 2 (4) / MFIPPA s. 2 (2.1), s. 2 (2.2).

The legislation clarifies what is not personal information in a business context.

Business identity information includes the name, title, contact information or designation of an individual that identifies the individual in a business, professional, or official capacity.

Business identify information applies even if an individual carries out business, professional or official responsibilities from their home or dwelling, and the contact information relates to the dwelling.

## Customer Service Information

FIPPA s. 65.1 (2)

FIPPA authorizes a service provider organization to collect the customer service information of an individual with their consent. In the Ontario Government ServiceOntario is an example of a service provider organization.

Customer service information is a separate category of personal information that includes:

- The name, address, and telephone number or other contact information;
- The transaction or receipt number provided;
- Information relating to the payment of any fee; and
- Other prescribed information.

## Common Examples of Personal Information

A name by itself is not personal information by definition. A name is personal information, where it appears with other personal information relating to an individual or where the disclosure of the name would reveal other personal information about the individual.

Information that relates to an individual's characteristics, background and history are common examples of personal information. Examples include race, ethnicity, country of origin, gender, gender identity, employment history, educational history and more.

An identifying number is typically a unique number connected to an individual in a particular context. Examples include Health Card number, medical record numbers assigned by hospitals, Social Insurance Number (SIN), driver's licence number, student numbers, and address information. It may also include personal fax numbers or Internet Protocol addresses.

An identifying symbol is something that stands for, or suggests, something else by reason of relationship, association, convention, or accidental resemblance. Examples include a signature, a degree or professional designation, a tattoo, an emblem, or a scar.

Other identifying particulars may include biometrics such as a handprint, footprint, iris scan or DNA. Behavioural biometrics may include keystrokes and voiceprints.

## Privacy Rules

In order to deliver services and programs to the public, institutions need to collect, manage, disclose and dispose of personal information. Institutions should ensure that the manner of collection, use, disclosure and disposition of personal information is in compliance with the privacy rules outlined in the legislation.

As the privacy rules in the legislation are general, most institutions have other privacy policies, standards or procedures that assist in operationalizing these rules within the specific context of the institution. For instance, internal policies may outline roles and responsibilities within the institution for various privacy-related activities.

The privacy rules apply to all personal information held by institutions with the exception of public records of personal information discussed at the end of the chapter and certain employment-related and labour relations records.

The privacy rules and their main purpose are summarized below, followed by a more detailed discussion.

**Authority to collect:** Limits the collection of personal information by institutions to authorized activities.

**Manner of collection:** Ensures the collection of personal information is directly from the individual, except in limited circumstances.

**Notice requirements:** Informs the individual of the collection of personal information.

**Proper use and disclosure:** Limits use and controls sharing or distribution of personal information for authorized activities.

**Accuracy:** Ensures processes are in place to keep personal information accurate.

**Retention**: Ensures that an individual can obtain access to their own personal information for a certain period.

**Security:** Ensures the security and confidentiality of personal information.

**Disposal and destruction:** Ensures disposal and destruction of personal information is authorized and secure.

## Authority to Collect

FIPPA s. 38 / MFIPPA s. 28

An institution can only collect personal information under one of these conditions:

- The collection of personal information is expressly authorized by a statute;
- 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.

The phrase “expressly authorized by statute” requires that the specific types of personal information be described in a statute (i.e., law) or a general reference to the activity be set out in the statute.

“Purposes of law enforcement” refers to the definition of law enforcement that is outlined in section 2 of the legislation. Refer to the section on Law Enforcement in Chapter 5: Exemptions and Exclusions for more information on the definition of law enforcement.

“Necessary to administer a lawfully authorized activity” refers to instances where institutions need to collect personal information in order to deliver a service or program that is authorized by the government. For provincial ministries, authorization may include legislation, regulations or orders-in-council. For municipal institutions, authorization may include statute, by-law or regulation.

A key word in this provision is “necessary.” Institutions should be able to show that each element of personal information that is collected for the administration of a program is necessary in order to properly and effectively administer the program. Personal information that is merely helpful to the institution would not qualify for this collection authorization.

A collection occurs when an institution actively acquires the information or invites an individual or others to send personal information to the institution. When an institution collects personal information in a non-written form (i.e., verbally), this activity would also be considered a collection of personal information.

Where an individual submits personal information without being requested by an institution, a collection is deemed to occur only if the institution keeps or uses the information.

## Manner of Collection

FIPPA s. 39 (1) / MFIPPA s. 29 (1)

### Direct Collection

The legislation requires that personal information be collected directly from the individual to whom the information relates.

The legislation provides limited circumstances where personal information can be collected indirectly, which means from a source other than the individual to whom the personal information relates.

### Indirect Collection

Institutions may indirectly collect personal information when an individual consents to this manner of collection. Institutions should retain a record with the date and details of the authorization including the:

- Personal information to be collected;
- Source of the personal information; and

- Name of the collecting institution.

Other circumstances that permit indirect collection of personal information include:

- Where other statutes provide authority to collect in another manner; or
- Where institutions have legal authority to disclose personal information.
- For conducting a proceeding or a possible proceeding before a court or tribunal;
- For law enforcement purposes; and
- For determining suitability of an honour or award.

Examples of statutes that provide the authority for an institution to indirectly collect personal information include:

- The Assessment Act;
- The Family Responsibility and Support Arrears Enforcement Act,;
- The Municipal Health Services Act; and
- The Consumer Reporting Act.

Some examples of quasi-judicial proceedings or tribunals include the Ontario Municipal Board, Property Standards Committee, Social Assistance Review Board, and Committees of Adjustment.

In order to justify collecting personal information from another institution, an institution should be able to demonstrate that there is a common or shared purpose for the personal information.

## Authority of the Information and Privacy Commissioner

The legislation gives the IPC the authority to permit an indirect collection where:

- The collection is not specifically allowed under this section; or
- It is not possible or practical to collect the personal information directly or to obtain authorization directly from the individual concerned.

An institution must make an application for an exemption to the IPC.

## Notice Requirements

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

An institution must inform the individual to whom the information relates that a personal information collection has occurred. Whenever possible, the notice should be provided to an individual at the time of collection, or included on program forms and communications.

The notice to the individual must state:

- The legal authority for the collection;
- A reference to the specific law, section or by-law;
- The principal and any secondary uses of the personal information; and
- The title and business contact information of an official of the institution.

Notice must be provided each time there is a collection. The notice should address separate legal authorities or collections if a form is used for multiple purposes.

Notice should be stated or written clearly, and provide enough detail to inform the individual but not limit the institution unnecessarily. The needs of affected individuals and of the business should inform the manner in which notice is provided. There are many options available, such as providing the notice verbally, in writing, via mail outs, or through public advertisements.

Notice should be reviewed periodically to ensure the information is accurate and up to date. The designated official should be available and able to answer questions about privacy and how the personal information will be used and disclosed.

## Exception to Notice Requirements

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

The legislation allows the Responsible Minister to grant a waiver for a notice of collection based on the merits of the case. A waiver request should apply to a class or group of individuals rather than an individual.

A waiver may be warranted in circumstances where:

- There is legal authority for an indirect collection;
- Notice would interfere with an indirect collection for unique programs or investigations;
- It is impossible or very difficult to provide notice;

- The administrative burden and cost of providing notice is excessive compared to the need for notice; and
- Subsequent disclosures from an institution are inconsistent with the first notice.

Appendix 8 is a form institutions can use to apply for a waiver from the Responsible Minister and provides an outline of considerations for institutions contemplating requesting a waiver of notice from the Responsible Minister. Institutions should consult Legal Counsel when considering a waiver of notice application.

## Use and Disclosure of Personal Information

FIPPA s. 41, s. 42 / MFIPPA s. 31, s. 32

The legislation puts a number of conditions on the use and disclosure of personal information. In general, personal information can only be used or disclosed for the purpose for which it was collected.

There are circumstances where the use and disclosure of personal information is permitted for other purposes. These purposes are discussed in the sections below.

### Consistent Purpose

FIPPA s. 41 (1) (b), s. 42 (1) (c), s. 43 / MFIPPA s. 31 (b), s. 32 (c), s. 33

The legislation allows institutions to use and disclose personal information where it is consistent with the purpose indicated in the notice of collection. A purpose is consistent and compatible where an individual might reasonably have expected the use or disclosure of the personal information at the time of collection.

For example, disclosing the name and address of an individual to a courier company for the purpose of delivering a package would be considered a consistent purpose where the individual had requested new vehicle licence plates from the Ministry of Transportation.

In the context of an indirect collection from another institution, an institution must show compatibility with the original collection.

## Consent

FIPPA s. 41 (1) (a), s. 42 (1) (b) / MFIPPA s. 31 (a), s. 32 (b)

An individual can provide consent for an indirect collection or for a secondary use of personal information. An institution can also use and disclose personal information where the individual provides consent.

Consent should be in writing and the specific information for which consent is given must be identified. Where consent is not obtained in writing, institutions should document:

- The specific personal information to be disclosed;
- To whom the information may be disclosed and for what purpose it is to be used;
- The date of the consent; and
- The institution to which consent is given.

## Compliance with Other Laws

FIPPA s. 41 (1) (c), s. 42 (1) (e) / MFIPPA s. 31 (c), s. 32 (e)

An institution can use and disclose personal information for the purpose of complying with an Act of the Legislature or an Act of Parliament or a treaty, agreement or arrangement. The agreement or arrangement must be authorized by a federal or provincial law.

Some examples include:

- The Child, Youth and Family Services Act;
- The Highway Traffic Act; and
- The Ombudsman Act.

## Performance of Duties

FIPPA s. 41 (1) (c), s. 42 (1) (d) / MFIPPA s. 31 (c), s. 32 (d)

An institution may use or disclose personal information within an institution for purposes other than the purpose stated at collection where:

- The record is necessary for the proper discharge of an institution's functions; and

- Needed by an officer, employee, consultant or agent of an institution for the performance of their duties.

There must be sufficient need and necessity. Disclosures that are merely based on concern or convenience are not permitted under this section.

## Between Organizations

FIPPA s. 42 (1) (j) to (n) / MFIPPA s. 32 (j) to (l)

The legislation allows institutions to disclose personal information for reasons other than the reasons for which the information was collected in limited and defined circumstances. Institutions can disclose personal information to other organizations or representatives such as:

- The Responsible Minister;
- The IPC;
- A member of the Legislative Assembly who has been authorized by a constituent under FIPPA;
- A member of a bargaining agent who has been authorized by an employee under FIPPA; or
- The Government of Canada in order to facilitate the auditing of shared cost programs (e.g., General Welfare Assistance Act).

## Compassionate Circumstances

FIPPA s. 42 (1) (i) / MFIPPA s. 32 (i)

An institution may disclose personal information in compassionate circumstances to facilitate contact with a relative or a friend of an injured, ill or deceased individual. The personal information to be disclosed may relate to either party. Only the information necessary to facilitate contact should be disclosed.

This section is not relevant in deciding whether personal information may be disclosed under an access request. Compassionate circumstances considerations for processing requests are discussed in Chapter 5: Exemptions and Exclusions in the section regarding the personal privacy exemption.

## Fundraising

FIPPA s. 41 (1) (d), s. 42 (1) (o), s. 42 (2), s. 42 (3)

Educational institutions can use and disclose personal information from their alumni records and hospitals can use and disclose personal information from their hospital records for fundraising purposes provided that:

- Notice is given to an individual at first contact;
- Notice is given periodically to an individual; and
- A public notice is published periodically.

The purpose of the each type of notice is to inform and allow an individual to refuse or stop the use of their personal information for fundraising.

FIPPA requires that a fundraising agreement be in place between an educational institution or hospital with any person or associated organization that carries out fundraising activities.

Consult PHIPA for its fundraising provision for health information custodians and personal health information.

## Health and Safety

FIPPA s. 42 (1) (h) / MFIPPA s. 32 (h)

An institution can disclose personal information in compelling circumstances affecting the health and safety of an individual. The disclosure must be followed by notification mailed to the last known address of the individual to whom the information relates.

## Law Enforcement

FIPPA s. 42 (1) (f) to (g) / MFIPPA s. 32 (f) to (g)

An institution can disclose personal information for law enforcement purposes where disclosure is:

- By a law enforcement institution;
- To a law enforcement agency in a foreign country under an arrangement, a written agreement or treaty or legislative authority;
- To another law enforcement agency in Canada; and
- To an institution or law enforcement agency in Canada to aid an investigation that will likely result in a law enforcement proceeding.

Appropriate internal authorizations must be obtained prior to disclosure. Personal information should not be disclosed for general speculation or fact-finding and should only be disclosed for a specific law enforcement matter.

In some instances, the institution should insist on seeing an order or warrant before disclosing personal information to law enforcement.

## Accuracy

FIPPA s. 40 (2), s. 40 (3) / MFIPPA s. 30 (2), s. 30 (3)

An institution must take reasonable steps to ensure that personal information records used by the institution are accurate and up to date.

However, this standard of accuracy does not apply to personal information if collected for law enforcement purposes in the course of an investigation. For instance, witness statements collected by law enforcement officers do not need to be changed if others disagree with the accuracy of the contents of the witness statements.

## Retention

FIPPA s. 40 (1), Reg. 460 (5) / MFIPPA s. 30 (1), Reg. 823 (5)

Records retention schedules may be impacted by various legal requirements, business needs, or information management policies. The legislation requires that personal information must be retained for a minimum of one year after its use to ensure that an individual has a reasonable opportunity to obtain access.

The retention requirements are set out in the regulations and allow for four exceptions that permit a destruction to occur earlier than the one year retention rule. These exceptions are:

- An individual may consent to an earlier destruction;
- If information is credit or debit card payment data;
- When a different retention period is set out by a municipal by-law (MFIPPA institutions only); and
- Personal information stored on telecommunication logger tapes may be disposed after 45 days (FIPPA institutions only).

The use of the personal information is important in determining retention requirements. For instance, personal information collected on surveillance video cameras would not be considered used if the tapes are not reviewed for security incident investigations.

Therefore, institutions can develop shorter retention periods for surveillance tapes that are not used by the institution.

Further if institutions receive personal information in error that is not used by the institution, the institution is not required to retain the personal information for one year.

## Security

Reg. 460 (3), (4) / Reg. 823 (2), (3)

An institution must ensure the security and confidentiality of personal information records. Institutions must implement reasonable security measures such as policies, procedures, and standards to address various security requirements.

The security requirements set out in the regulations are summarized below:

- Access to an original record must ensure security;
- The identity of an individual seeking access to his or her personal information must be verified; and
- Unauthorized access must be prevented taking into account the nature of the records to be protected.

Additional security requirements are found in the disposal requirements set out in the next section.

## Disposal

Reg. 459 (4), (5), (6)

The regulations require that institutions only dispose of personal information with authorization of the head. Institutions must maintain a disposal record setting out what information has been transferred or destroyed, and the date of transfer or destruction.

The transfer and destruction of personal information must meet security requirements, and the reconstruction or retrieval of destroyed personal information must not be possible.

Under FIPPA, institutions may dispose of personal information by:

- Transferring it to the Archives of Ontario; or
- Destroying it.

Further to this, an educational institution may only dispose of personal information by:

- Transferring it to the archives of an educational institution with an agreement authorizing the transfer; or
- Transferring it to the Archives of Ontario with an agreement authorizing the transfer; or
- Destroying it.

There is no similar regulation for MFIPPA institutions. However, MFIPPA institutions should follow the principles of Regulation 459 and dispose of personal information in a similar manner. MFIPPA institutions should seek approval before disposing of personal information and maintain a similar record of disposal. In accordance with the principles in Regulation 459, MFIPPA institutions should dispose of personal information by:

- Transferring it to a municipal or local government archive; or
- Destroying it.

## Public Records of Personal Information

FIPPA s. 37 / MFIPPA s. 27

The legislation provides an exception to the privacy rules where personal information is maintained for the purpose of creating a record that is available to the public. However, the legislation does not include requirements for governing public records.

Public records of personal information are records to which access is given to all members of the public. Personal information that is only accessible to some members of the public and not others is not a public record.

Public records are maintained for some or all of the following reasons:

- Allow for the proper administration of programs, activities and services;
- Promote government accountability by providing information relating to the issuance of licenses, permits, government contracts, etc.;
- Promote informed choice and consumer protection; and
- Allow for the fair determination of rights.

A public record does not mean that there are no terms or conditions on public access. For example, access to public records may include fees.

Similar personal information may exist in multiple contexts. For instance, personal information may exist in one context for maintaining a public record, and another

context for the administration of a program. Despite the availability of the personal information in the public record context, the personal information maintained in the alternative context remains confidential.

The public records exception applies only if the institution maintains the information expressly for the purpose of creating a public record. Other institutions cannot claim the benefit of the public records exception unless they too have the same authority.

The following list includes examples of records containing personal information that are maintained for the purposes of making the information publicly available:

- Assessment rolls created under the Assessment Act.
- Some conviction related information subject to the Regulatory Modernization Act.
- Lists of electors created under the Municipal Elections Act.

## How Public Records Are Created

In Ontario, public records can be created either by statute or by a policy decision of the institution.

When a public record is created by statutes, regulations or by-laws they generally contain terms and conditions regarding the administration of the information such as the authority to charge fees, and the times and location of access.

When a public record is created by policy without statutory authority, the institution must establish a strong policy rationale that the public's right to access the information outweighs the privacy rights of individuals to whom the information relates.

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

- Does the public's "need to know" outweigh the privacy rights of the individuals concerned?
- Will the release of the information advance informed choice?
- Will the information be accessible to everyone?
- Does the public need the information to assist in the conduct of business?
- If the information is made publicly available, would the disclosure 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?

## Resources

IPC: Fact Sheet – What is Personal Information?

IPC: Collection, Use and Disclosure of Personal Information

# Chapter 8: Personal Information and Correction Requests

## Introduction

As discussed earlier in this manual, the legislation provides individuals with a right to request access to their own personal information in the custody and control of institutions. Like requests for general records, this right of access is subject to limited and defined exemptions. Individuals may also request institutions to correct their own personal information in the custody or control of the institution.

Requests for one's own personal information are referred to as a "personal information requests." Requests to correct one's own personal information are referred to as "correction requests."

This chapter outlines considerations specific to personal information requests and correction requests. For additional information on access request processing requirements, refer to Chapter 6: Managing the Request Process.

## Applying the Legislation for Personal Information Requests

As discussed in Chapter 6: Managing the Request Process, Coordinators must ensure requests contain enough information for an experienced employee to locate a record; coordinate a search for responsive records; and review responsive records to determine if relevant exemptions and exclusions apply to the records.

In personal information requests, there are some additional considerations. To assess how the legislation applies to responsive records within the context of a personal information request, the basic steps include:

1. Determine if any exclusions apply. If yes, do not go to the steps that follow.
2. Determine if the definition of personal information is met.
3. Determine if exemptions to an individual's right of access to one's own personal information may apply to the record.
    - Exemptions to the right of access are outlined in the legislation and discussed in greater detail in the sections below.
    - If yes, determine if the criteria and tests for each relevant exemption are met.
4. Determine if additional legal tests apply and the criteria are met.

5. Determine if the record has personal information of an individual other than the requester.
    - If yes, determine if disclosure would result in an unjustified invasion of privacy.
6. Complete the exercise of discretion if any discretionary exemptions have been considered to apply to a record.

The relevant factors and issues of each step are discussed further below.

## Exemptions to the Right of Access to One's Own Personal Information

FIPPA s. 49 (a) / MFIPPA s. 38 (a)

The legislation outlines that while individuals have a general right of access to their own personal information, there are limited and defined exemptions to this general right of access. The legislation sets out which specific exemptions apply to personal information requests. The majority of the exemptions apply to personal information requests. The exemptions that apply are:

- Draft by-laws and closed municipal meetings;
- Cabinet records;
- Advice to government/Advice or recommendations;
- Law enforcement;
- Civil Remedies Act;
- Prohibiting Profiting from Recounting Crimes Act;
- Relations with other governments;
- Relations with Aboriginal communities;
- Defence;
- Third party information;
- Economic and other interests
- Solicitor-client privilege;
- Danger to safety or health; and
- Information soon to be published.

See Chapter 5: Exemptions and Exclusions, for more information on how these exemptions are defined. Further discussions on any exceptions or legal tests that may apply to an exemption are also discussed in that chapter.

## Personal Information of Other Individuals

FIPPA s. 49 (b) / MFIPPA s. 38 (b)

In addition to the identified exemptions, the legislation specifies that an institution may withhold a record where disclosure might constitute an unjustified invasion of privacy of an individual other than the requester.

See Chapter 5: Exemptions and Exclusions for a detailed discussion on the personal privacy exemption and determining when the disclosure of information would constitute an unjustified invasion of privacy.

## Other Exemptions

FIPPA s. 49 (c) to (f) / MFIPPA s. 38 (c) to (e)

The legislation also identifies specific types of records or personal information that are exempt.

**Correctional records:** This exemption applies if the record is from a correctional facility and could reasonably be expected to reveal information supplied in confidence.

**Confidential evaluative or opinion material relating to awarding government contracts or other benefits:** This exemption applies to confidential evaluative or opinion material compiled solely for the purpose of awarding Government contracts or other benefits. This exemption applies where releasing the record would identify a source that provided information to the institution and where it was reasonably assumed that their identity was expected to be held in confidence.

**Other confidential and evaluative opinion material:** This exemption protects information that is evaluative or opinion material that is supplied explicitly or implicitly in confidence solely for the purpose of:

- Assessing teaching materials or research of an employee or associated person of an educational institution or hospital (FIPPA only);
- Determining admission to an academic program of an educational institution or hospital (FIPPA only); or
- Determining suitability for an honour or award (both FIPPA and MFIPPA).

**Medical information:** This exemption applies to personal information that could reasonably be expected to prejudice the mental or physical health of the requester.

## Correcting One's Own Personal Information

FIPPA s. 47 (2) / MFIPPA s. 36 (2)

The legislation provides an individual who is given access to their personal information through the access request process, the right to request correction of the information. The IPC has found that there are three factors to consider in a correction request:

- The information must be personal information;
- The information must be inexact, incomplete or ambiguous; and
- The information is not opinion material provided by another individual.

Opinion material that is provided by someone other than the individual requesting the correction is not usually subject to correction. Opinion material can be changed where it can be demonstrated that it was inaccurately recorded.

A head must determine whether the information submitted for correction can be verified and if so approve the correction. If the correction is made, the requester should be notified with a copy of the corrected record.

If the correction is not made, the individual can require the institution to attach a "statement of disagreement" to the information. The statement of disagreement identifies the correction was requested but was not made.

Further, the requester should be informed of the reasons the institution refused to make the correction and informed of the right to:

- Appeal the decision to the IPC;
- Require that a statement of disagreement be attached to the information; or
- Have the statement of disagreement provided to any person or body to whom the personal information was disclosed in the last 12 months.

## Comprehensible Form

FIPPA s. 48 (4) / MFIPPA s. 37 (4)

In a response to a request from an individual for their own personal information, institutions should ensure that the personal information is provided in a comprehensible form. Sometimes personal information may be stored or used in a way that is not easily understood by the requester.

For example, institutions may be required to translate the language used in personal information records; increase font sizes to assist individuals with visual impairments; or take other actions to make the record comprehensible to the requester.

## Resources

Ontario Central Forms Repository: Access or Corrections Request Form

Appendix 4.19 - Letter to Requester – Decision Approving Correction of Personal Information

Appendix 4.20 - Letter to Requester – Decision Denying Correction of Personal Information

# Chapter 9: Privacy Management

## Introduction

Chapter 7: Privacy Fundamentals outlined the rules that govern collection, use, disclosure, retention, accuracy, security and disposal of personal information. Institutions need to build a privacy management program that enables the institution to be compliant with these rules.

Each institution will have slightly different needs regarding the management of privacy depending on the volume of personal information within their custody, the sensitivity of the personal information they manage, and relationships with third parties, including vendors. The guidance in this chapter consists of best practices that may be adapted to each specific institution based on their needs.

This chapter outlines the importance of defining roles and responsibilities for privacy, building privacy into business practices, education and awareness; monitoring the effectiveness of a privacy program, and preventing and managing privacy breaches.

## Define Roles and Responsibilities

As discussed in Chapter 2: Government Roles and Responsibilities, the head of an institution is accountable for compliance with the legislation. In most institutions, some or all of the powers of a head are delegated to an officer or officers through a formal Delegation of Authority.

Senior level accountability for privacy protection must be established within an institution. This senior official should understand the personal information holdings of the institution, the safeguards that are in place to protect personal information, and act as a champion for privacy protection at the senior level.

Further, the management of privacy needs to be an institution-wide initiative, engaging employees at all levels. All employees who work with personal information are accountable for protecting the personal information in the custody and control of the institution.

Obligations to safeguard personal information should be outlined in job descriptions, codes of conduct, and in performance development plans for all institutional employees who collect, use, or disclose personal information as part of their official duties.

Education about privacy, as well as the legislation's requirements, will help employees understand why privacy is important, how to protect it, as well as employees' responsibilities with regards to safeguarding personal information. Coordinators should develop a privacy awareness training program that ensures employees can identify personal information and understand appropriate uses for the personal information.

Institutions should also make available to the public contact information where inquires can be made regarding the privacy practices of the institution. Providing this contact information supports transparency and accountability.

As discussed in Chapter 7: Privacy Fundamentals, this contact information should be included in any notice of collection. Additionally, this information should be generally available to the public on the institution's public website or other publicly available source.

## Privacy Policy

Institutions should develop a comprehensive privacy policy that outlines the institution's commitment to the protection of privacy and how the institution will be compliant with the privacy rules established in the legislation.

While the legislation has general requirements, an institution's policy can be more instructive to employees and outline how the institution will specifically address each privacy rule. The privacy policy translates abstract rules into concrete commitments that are relevant to the institution.

The privacy policy should outline mandatory requirements for managing privacy, steps to take in the event of a privacy breach, and outline when privacy impact assessments are required.

## Align Business Practices

Institutions should align business practices by integrating the protection of personal information into existing programs, systems, and policies.

It is easier and less expensive to build privacy protective measures into technology, contracts, programs, practices and business continuity plans from the beginning, than to retrofit them after privacy breaches occur. Therefore, institutions should consider privacy when identifying your strategic priorities, deliverables and performance measures. Privacy should not be an after-thought.

Areas that institutions should consider adding privacy considerations include:

- Assessment of potential vendors and partners;
- Contracts with vendors and partners;
- Information sharing agreements;
- Information technology planning;
- Policy development; and
- Program development.

## Privacy Impact Assessment

A privacy impact assessment (PIA) is an analytical process involving several activities and deliverables. It is not a single document or end-product.

A PIA process will support institutions in identifying and addressing privacy risks when planning, designing, acquiring and implementing any program, system, process, practice, service, technology, application or other deliverable that involves personal information. It is relevant to new initiatives, as well as changes to existing information management processes or systems.

The PIA is often described as an “early warning system” because it enables institutions to identify and understand potential privacy risks, to prevent or mitigate negative privacy consequences, and to enhance privacy protection. The PIA should be started as early in a project’s lifecycle as possible.

The following examples are the types of projects that may involve a substantial change to the collection, use or disclosure of personal information and, therefore, would be benefit from a PIA:

- New programs that will involve significant collection, use, or disclosure of personal information, particularly enterprise-wide initiatives or those involving multiple programs or partners;
- Major changes to existing programs that will involve a significant change in the collection, use and disclosure of personal information including those resulting from: an integration of programs; broadening of target population; change in service delivery channels; expansion of amount or type of data collection; constraining or eliminating opportunities for anonymity or pseudonymity; or major shift toward indirect collection of personal information;
- Use of new technology or one known to impact privacy that could raise significant privacy risks (e.g., biometrics, smart cards, drug testing, or technology with surveillance capabilities);

- Major changes to technology that will alter the functionality of information management, access to personal information (by program/system administrators, customers or third parties), or security features;
- Creation or modification of databases that will contain personal information, particularly where the data is sensitive or relates to a significant number of people, or that will link separate databases or create files that index or point to personal information on such databases; or
- Creation or modification of identification and authentication schemes that will involve multi-purpose identifiers, biometrics or identity cards.

## Privacy and Contracting Services

Institutions may contract with private sector organizations or enter into relationships with other types of organizations to provide services on behalf of the institution. These services may include:

- Delivering a program on behalf of government;
- Establishing and/or managing a database;
- Providing system support such as troubleshooting;
- Providing disaster recovery services;
- Conducting research;
- Administering a call centre;
- Providing records storage; or
- Supplying other services such as off-site shredding or recycling of information storage media.

Under these contracts it may be necessary for private sector organizations to handle personal information or other sensitive government information. However, the institution remains accountable for ensuring that the private sector organization manages the personal information in accordance with the legislation.

Institutions should take steps to assess the risk and develop mitigation strategies when contracting services that involve the collection, use, storage, retention, disclosure or disposal of personal information. The following steps provide guidance on how institutions can proactively protect personal information when contracting services:

**Assess risk:** Assess the sensitivity of the data and conduct a PIA and threat risk analysis when considering contracting services involving personal information.

**Develop an information protection plan:** Develop a plan to address control, accountability, security and mitigation strategies for any identified risks.

**Procurement and contractual requirements:** Work with procurement specialists and Legal Counsel to build privacy and security requirements into procurement and contracting process. Contractual requirements can address identified risks.

**Audit and monitor contract:** Conduct ongoing audit and consistently review contractor's performance in managing personal and sensitive information as documented in the contract.

## Monitor and Evaluate Privacy Program

Institutions should periodically review privacy policies and practices, and commit to ongoing improvements to ensure compliance with the legislation.

A privacy audit is a tool to support monitoring and evaluating a privacy program. A privacy audit is a self-assessment of the institution's practices to identify:

- The institution's personal information holdings;
- The information needs of a program areas or corporate functions; and
- Existing privacy and information management policies, practices, and procedures.

A privacy audit allows institutions to determine the extent to which personal information in the institution's custody and control is maintained in accordance with the legislation. A privacy audit will also help identify gaps in compliance and can help focus efforts to improve practices within the institution.

The basic steps to follow for a privacy audit include:

- Take inventory of the types of personal information that are collected, used, disclosed, retained or disposed of by the institution;
- Confirm the legal authority for collecting the personal information; and
- Describe the end-to-end business processes or activities that support the program in delivering those services.

Following the completion of the privacy audit, institutions should identify recommendations and next steps to fill in any gaps in compliance with the legislation. Some examples of next steps that could be identified from a privacy audit include:

- Updating notices of collection to include all necessary requirements under the legislation;
- Increased security on personal information stored within systems;

- Updates to an institution's personal information bank index in the Directory of Records; or
- Updated training for employees within the institution.

## Privacy Breaches

A privacy breach is an incident where personal information is collected, retained, used, disclosed or disposed of in ways that do not comply with the provisions of the legislation.

Common examples of a privacy breach include personal information being stolen, lost, or accessed by unauthorized persons. Circumstances that could lead to a privacy breach include:

- Personal information being mailed, faxed or emailed to a wrong address, email address or fax number;
- Loss or theft of equipment containing personal information, such as external hard drives, laptops, are memory sticks;
- Disposal of equipment or paper records without secure destruction of the personal information; or
- A malicious cyber-attack on an information system.

Addressing privacy breaches is an important part of an institution's privacy management program. When a privacy breach occurs, both the individuals affected by the breach and the institutions involved are potentially vulnerable to adverse consequences:

**Consequences for individuals:** Unauthorized disclosure of personal information violates an individual's privacy. It creates the potential for harm, including identity theft and other forms of fraud, physical safety issues such as stalking or harassment, financial loss, adverse impact on employment or business opportunities, and damage to reputation.

**Consequences for institutions:** In addition to not meeting the legal requirements of the legislation there are other consequences, including:

- Reduced productivity as staff respond to a breach or deal with a complaint;
- Lost public trust and confidence due to public disclosure of a major privacy breach;
- Cost of emergency measures necessary to control a breach; and
- Replacement costs of hardware, software and data affected by the breach.

## Privacy Breach Response Plan

Despite an institution's best efforts, privacy breaches will occur and the development of a privacy breach response plan will enable an institution to respond to a breach in a timely and effective manner.

Having such a plan enables institutions to respond to privacy breaches in a coordinated manner. As part of a privacy management program, institutions should evaluate the effectiveness of the institution's response plan annually and implement changes, as necessary. The creation of a response plan may involve documenting existing practices for dealing with privacy breaches.

Given the diversity of institutions and the varied nature of privacy breaches, no "one size fits all" response protocol is possible or practical. However, as a best practice, institutions should first assess whether a privacy breach has occurred and in the event of a breach, institutions may take the following actions:

- Respond and contain;
- Notify;
- Investigate; and
- Implement change.

These steps can take place simultaneously, or in rapid succession, depending upon the circumstances. Each step does not have to be completed before beginning the next step.

Each step of the protocol is described below and includes suggested roles and responsibilities for the key players.

Once an incident or suspected incident has occurred, it should be reported by the employee who discovered it immediately the employee's direct supervisor and the Coordinator. The Coordinator will work with the program area to determine if a privacy breach has occurred.

### Assessing a Suspected Breach

When an incident has been reported to the manager or the Coordinator within an institution, they must immediately determine if a privacy breach has occurred. In making this assessment, two important questions need to be answered:

- Is personal information involved?
- Has the personal information been collected, used, accessed or disclosed in an unauthorized manner?

Not all data in the custody or control of an institution is personal information. Therefore, the first part of your assessment is to identify the type of information affected by the incident. See Chapter 7: Privacy Fundamentals for a definition of personal information and examples.

If the answer to both questions is “yes”, a privacy breach has occurred.

## Respond and Contain

Coordinators or other employees should contain the privacy breach by taking corrective action. Corrective action may include retrieving personal information, or isolating or suspending activity on a system or website.

The privacy breach should be reported to key players within the institution including senior leadership and impacted program areas.

The institution should document the details of the privacy breach. Documentation should be as detailed as possible and address the “who, what, where, when and how” of the incident.

Finally, Coordinators should brief senior management on the privacy breach and how it is being managed and resolved, as appropriate.

## Notify

Coordinators should work with the program area and Legal Counsel to plan notification of the breach. Notifying the individuals impacted by the privacy breach should be the default course of action. The purpose of providing notice of a privacy breach to the individuals whose personal information was involved in the incident is to provide them with sufficient information about:

- What happened;
- The nature of potential or actual risks of harm;
- Appropriate action to take to protect themselves against harm; and
- A brief explanation of the individual’s right to complain to the IPC about your institution’s handling of their personal information.

Such notice supports the purposes of the legislation and the institution’s responsibility to protect the privacy of individuals with respect to personal information. It is also consistent with the fair information practices of openness and accountability.

Notice should take place at the earliest opportunity. However, institutions should not compound the potential harm caused by a privacy breach by providing premature notice

based on incomplete facts or taking any action that might make identity theft or other harm more likely to occur as a result.

Notice should be delayed if law enforcement determines immediate notice would impede a criminal investigation; or the breach resulted from a security or information system failure, restore and test the integrity of the system before disclosing details of the breach.

Notifying the individuals affected by a privacy breach may not be appropriate, reasonably possible, or necessary in the following limited circumstances:

- Law enforcement determines notice would impede a criminal investigation;
- Notice is not in the individual's interest (e.g., notice could potentially endanger an individual or result in greater harm to the individual); or
- Notice would serve no useful purpose (e.g., if all the personal information involved in the privacy breach is: already publicly available; recovered before an unauthorized party could possibly access it; or protected by technology, such as encryption, that would mean unauthorized access and use of the data is not reasonably possible).

Coordinators should consider consulting with the IPC when planning to provide notice to individuals impacted by privacy breaches.

See Chapter 12: Privacy Complaints, Breaches and Investigations for more information on institutions self-reporting privacy breaches to the IPC.

## Investigate

Institutions should investigate to:

- Identify and analyze the events that led to the privacy breach;
- Evaluate the institution's response and containment of the breach; and
- Recommend remedial action to help prevent future breaches.

Document the results of the internal investigation including:

- Background and scope of the investigation;
- Legislative implications;
- How the investigation was conducted (who did it, who was interviewed, what questions asked, what policies and practices considered, etc.);
- The source and cause of the privacy breach;
- An inventory of systems and programs affected by the breach;

- Determination of the adequacy of existing security and privacy policies, procedures and practices;
- Assessment of the effectiveness of the institution's response to the breach; and
- Findings including a chronology of events and recommendations for remedial actions.

Senior management should be informed of the results of the investigation to ensure recommendations are enacted.

## Implement Change

The final step of the response plan is to implement changes within the institution to prevent future privacy breaches. When determining what changes and remedial action needs to be implemented, Coordinators should consider if it is necessary to:

- Review relevant information management systems to enhance compliance with the legislation;
- Amend or reinforce your existing policies and practices for managing and safeguarding personal information;
- Develop and implement new security or privacy measures;
- Train staff on legislative requirements, security and privacy policies, practices and procedures to reduce the potential of future breaches; or
- Test and evaluate remedial actions to determine if they have been implemented correctly, and if your policies and practices need to be modified.

In addition, Coordinators should evaluate whether the notice individuals impacted by the privacy breach was done in a reasonably timely manner, whether the tone and content of the notice was appropriate, and whether there was sufficient support provided to individuals impacted by the breach.

## Resources

IPC: Planning for Success: Privacy Impact Assessment Guide

IPC: Privacy Breach Protocol Guidelines for Government Organizations

IPC: Thinking About Clouds? Privacy, Security, and Compliance Considerations for Ontario Public Sector institutions

IPC: Open Government and Protecting Privacy

IPC: Fact Sheet, Video Surveillance

# Part IV: The Office of the Information and Privacy Commissioner of Ontario

# Chapter 10: Interacting with the IPC

## Introduction

Chapter 2: Government Roles and Responsibilities introduced the IPC and the purpose and responsibilities of that office. This part of the manual will provide detailed information about the important role and powers of this independent Officer of the Legislature.

This chapter outlines expectations for institutional staff when interacting with the IPC and outlines when and how to seek advice or comments from the IPC on new initiatives.

Chapter 11: Appeals Process outlines in detail the IPC appeal process. Chapter 12: Privacy Complaints, Breaches and Investigations provides more information on privacy complaints and investigations.

## Guiding Principles

Below are guiding principles that employees of institutions should follow when interacting with the IPC:

**Independence:** The IPC is independent of the government. This independence enables the IPC to fulfil its role of independently reviewing the decisions and practices of government institutions concerning access to information and the protection of privacy when collecting, using and disclosing personal information under the legislation.

**Authority:** The IPC has specific powers under the legislation to ensure institutions comply with the provisions of the legislation. Employees dealing with the IPC should recognize the IPC's legal authority.

**Responsibility:** Employees involved with an IPC matter should ensure a positive and constructive approach to working with the IPC. In particular, Coordinators, managers and supervisors should ensure that this constructive relationship is maintained throughout the course of an appeal, privacy investigation or any matter related to the IPC's mandate.

**Cooperation:** It is the responsibility of employees to provide the IPC with timely access to information and records necessary for the IPC to perform its statutory responsibilities.

## Obligations and Best Practices for Staff

When involved with the IPC, employees of institutions subject to the legislation must:

- Comply with the law, with policies and any orders made by the IPC pursuant to the exercise of the IPC's powers under the legislation;
- Provide clear and full disclosure of requested information to the IPC;
- Subject to legal advice, permit access to the institution's employees for the purposes of interviews in the context of a privacy investigation or adjudication where possible;
- Respect that the IPC has the authority to decide the pertinence of information requested from institutions subject to the legislation;
- Not interfere with the IPC's exercise of powers under the legislation; and
- Act honestly, ethically, and with integrity and remember employee actions and comments always reflect on the institution.

In addition, employees of institutions are expected to:

- Provide timely and accurate responses and assistance and not limit or unreasonably delay the time required to provide information;
- Treat IPC staff with respect, courtesy and fairness;
- Exercise general diligence, care and attention in responding to the issues raised by the IPC; and
- Help foster and support a positive working relationship with the IPC.

In adopting the above best practices, employees of institutions must understand that access to information is fundamental to the IPC's role. Coordinators, managers and supervisors have a particular responsibility to ensure a positive working relationship with the IPC.

## Seeking Comments or Advice on New Initiatives

In addition to its important role as the oversight body for access and privacy legislation, the IPC is also a key government stakeholder for transparency and accountability. The legislation gives the IPC the authority to offer comment on the privacy protection implications of proposed legislative schemes or government programs.

The IPC provides feedback to government institutions that have consulted with the IPC on matters that have access and privacy implications. The IPC's Director of Policy is the point of contact for institutions who wish to consult with the IPC on access and privacy

matters. It is important to obtain IPC feedback early and address any concerns in the early stages of an initiative such as a new project, strategy or program.

Examples where consultation with the IPC may be appropriate include:

- When an initiative would involve new collections of personal information;
- On early drafts of legislation that impact access to government records and privacy; or
- When the institution is contemplating use of new technologies where impacts on privacy are not well known.

Providing background policy documents that support an initiative is important in enabling informed and meaningful IPC comment. For example, if a program area has completed a privacy impact assessment on a new initiative, it may be beneficial to provide this documentation to the IPC prior to meeting. Institutions may want to involve the IPC especially when the matter has significant impact on the public. The IPC will manage highly sensitive and confidential matters appropriately by restricting staff involvement and securing information appropriately.

It is best practice for institutions to include their Coordinator and Legal Counsel when contemplating consulting with the IPC.

## IPC Initiated Contact with Institutions

There may be situations where the IPC initiates contact with institutions on issues that are of public interest. The IPC may contact an institution directly, or the IPC may first contact MGCS, as the Minister of MGCS is the Responsible Minister for the legislation. In these cases, the IPC may request information through email or through letters to ministers' offices or senior employees, in order to fully understand the issue. It is important that institutions provide timely responses to these types of IPC inquiries. An institution's Legal Counsel and Coordinator may be able to assist with these matters.

The IPC may also appear before, or make submissions to, various Standing Committees. The purpose of these submissions is for the IPC to provide its views or recommendations to the Standing Committee on bills that have access and privacy implications. Employees should provide assistance and information to the IPC relating to these proceedings, when requested.

## Resources

Information and Privacy Commissioner of Ontario - Main Page

# Chapter 11: Appeals Process

## Introduction

Individuals may request a review of access decisions under the legislation to the IPC. This review is referred to as an appeal.

This chapter provides an overview of the appeals process, general requirements, and timelines. The IPC is responsible for developing and managing the appeals process and procedures. Institutions are required to follow the IPC's Code of Procedures and related practice directions.

It is important for Coordinators to work with Legal Counsel to establish roles and responsibilities in the appeals process.

## Reasons for an Appeal

FIPPA s. 50 / MFIPPA s. 39

The legislation provides a right of appeal to requesters and affected parties impacted by a request. The legal term for an individual who makes an appeal is an appellant. The IPC keeps the identity of the appellant confidential in public orders regarding the appeal. The IPC does disclose the identity of the appellant to the institution involved in the appeal.

An appeal can be triggered by different events and can occur at different stages of the request process. Fees, time extensions, and deemed refusals may all be appealed during the request process.

An individual does not have appeal rights when a request for information is handled informally or outside of the formal access request process.

The main reasons for an appeal include:

**Access denied:** Requester disagrees with an institution's decision to deny access to some or all of the information requested. This includes information that was determined to be subject to an exemption and information that was determined to be subject to an exclusion.

**Affected party:** Affected party objects to an institution's decision to provide access to personal or proprietary information of the affected party.

**Correction denied:** Requester disagrees with an institution's decision to deny correction of personal information.

**Deemed refusal:** Requester did not receive any response from the institution within 30 days of the institution's receipt of the request.

**Failure to disclose:** Requester received decision letter from the institution; however, the institution failed to disclose records after fee payment.

**Fees and fee waiver:** Requester disagrees with the amount of fees being charged or disagrees with the institution's decision not to grant a fee waiver.

**Reasonable search:** Requester disagrees with an institution's decision regarding the existence of records and believes efforts to locate records were inadequate.

**Time extension:** Requester disagrees with an institution's decision to extend the time limit to respond to a request.

## IPC Powers

The IPC manages the appeal process and coordinates the exchange of information, relevant to each stage of the appeal. Coordinators may deal with a number of individuals at the IPC on an appeal.

The scope and complexity of an appeal and the number of parties involved in an appeal are some of the factors the IPC takes into account in determining an approach to resolution. The IPC can depart from its Code of Procedure where it is appropriate, and as long as it does not prejudice the parties.

The IPC has authority to obtain and examine records. The IPC never releases records at issue to a requester or an affected party and is prohibited from disclosing information provided to the IPC as part of the appeal process.

Institutions do not waive solicitor-client privilege if legal advice is contained in a particular record. The same reasoning applies to confidentiality provisions contained in other statutes.

The IPC decides matters under appeal by issuing an order in the form of a report. An IPC order is binding on all parties to the appeal. An order is not subject to appeal; however it may be subject to a request for reconsideration or a judicial review. These processes will be discussed later in the chapter.

The IPC has broad order-making powers to:

- Uphold or overturn an institution's decisions related to the application of exclusions, exemptions, and fees;
- Order an institution exercise or re-exercise its discretion;
- Order an institution to conduct further searches for records;
- Order an institution to produce a record where certain machine readable records are requested;
- Issue an interim order on specific issues or records and defer a final decision; and
- Order an institution to produce the records to the IPC.

The IPC notifies all parties to the appeal that an order has been issued and sends a copy of the order to the parties.

## Stages of Appeal

The appeal process has four stages:

1. **Initiating an Appeal:** A requester files an application for an appeal.
2. **Intake:** The IPC screens appeals received and decides whether it can be resolved informally, dismissed or moved toward mediation or adjudication. Orders can be issued at this stage for "deemed refusals" and "failure to disclose" appeals.
3. **Mediation:** A mediator contacts the parties, investigates, attempts to effect settlement, and issues a report.
4. **Adjudication:** An adjudicator contacts the parties, begins the inquiry, receives representations, and issues an order.

## Timelines

The appeal process does not have an official start and end date. The length of time required for an appeal depends on the complexity of the issues within the appeal, number of parties involved, and how many appeals the IPC is managing.

However, within the appeal process there are specific time limits by which institutions must respond to the IPC. The table below summarizes the time limits and further discussion of the steps follows in the chapter.

| Appeal Stage | Action | Timeline |
|---|---|---|
| Initiating an appeal | Requester or affected party files an appeal | Requester or affected party must file an appeal within 30 days of date of institution's decision |

| Appeal Stage | Action | Timeline |
|---|---|---|
| Intake stage | Institution receives notice of appeal | The institution must identify affected parties for IPC as soon as possible upon receipt of notice of appeal |
| Intake stage | Institution receives Confirmation of Appeal from IPC | The institution has eight days to respond to the IPC and provide requested documentation |
| Intake stage | IPC may grant a time extension for providing records to IPC | When a time extension is granted, the institution has up to fourteen additional days to provide requested documentation |
| Mediation stage | IPC sends Notice of Mediation | The Notice of Mediation sets out a 35 day deadline for an institution to claim any additional discretionary exemptions |
| Mediation stage | IPC initiates mediation stage of appeal | The mediation process is generally four months; however, timelines can be flexible depending on the circumstances |
| Adjudication stage | IPC sends Notice of Inquiry | Institutions must submit representations within 21 days of receipt of Notice of Inquiry |
| Adjudication stage | IPC may grant extension of time in providing representations | Any request for a time extension exceeding one week must be made in writing, including an explanation for the delay, to the adjudicator |
| Adjudication stage | Institution may issue a new decision letter to appellant | The new decision letter must be sent to the appellant within 35 days of the Notice of Inquiry unless IPC specifies a date. The adjudicator should be copied on the letter |
| Adjudication stage | Institution may raise constitutional questions | Institutions may raise constitutional questions within 35 days after receiving the Notice of Inquiry |
| Adjudication stage | Appeal abandoned if IPC does not get a response from the appellant | The IPC will determine an appeal is abandoned after 21 days have passed where the IPC has been unable to contact or receive a response from the appellant |

| Appeal Stage | Action | Timeline |
|---|---|---|
| Adjudication stage | Comply with order – no affected parties | Institutions must comply with an order by the date that is specified in the order |
| Adjudication stage | Comply with Order – affected parties | Institutions must comply with an order within 35 days, but no earlier than 30 days of date of order, unless another date is specified in the order |
| Adjudication stage | Retain appeal records | 60 days from date of order |
| Review of IPC Order | Application for a reconsideration order | Within 21 days of date of order or before the first specified date or time period in the order |
| Review of IPC Order | Application for Judicial Review | Within 30 days of date of order |
| Review of IPC Order | Institution notifies IPC to return records | As soon as possible, by the end of the 3-month or 1-year period |

## Initiating an Appeal

Institutions are required to provide requesters information about their appeal rights and the appeal process. This information should be provided to the requester in fee estimate letters, time extension letters and decision letters.

An appellant must file a written notice with the IPC Registrar within 30 days of receiving a decision. The legislation allows counsel or an agent to appeal on behalf of an appellant with appropriate authorization.

The IPC asks the appellant to complete an appeal form including the following information:

- The appellant's contact information (name, address, telephone);
- The institution's name and file number assigned; and
- A brief explanation of the reason for the appeal.

In addition, the IPC requires a copy of the institution's decision letter and a copy of the original request. Where the appellant does not have a copy of the original request, the institution can provide this to the IPC.

The appellant is responsible for paying appeal fees to the IPC. However, there are no appeal fees for an affected party appealing an institution's decision, or for subsequent appeals arising from a decision.

Appeal fees cannot be waived.

The appeal fee for decisions (exemptions and exclusions applied), deemed refusals, fees, fee waivers and reasonableness of search for access requests for general records is $25.00.

The appeal fee for decisions (exemptions and exclusions applied), deemed refusals, fees, fee waivers and reasonableness of search for access requests for one's own personal information is $10.00.

## Intake Stage

During the intake stage, the IPC screens an appeal and either dismisses, resolves, or streams the appeal to a later stage of the process. Intake analysts have delegated authority to screen out files where:

- The matter, on its face, is not within the IPC's jurisdiction; or
- The matter falls within the IPC's jurisdiction, but the matter, on its face, is one that the IPC believes should not proceed through the appeal process.

Institutions may receive the following notices from the IPC during the intake stage:

**Notice of Appeal:** This notice informs the institution that an appeal has been filed and may also notify any affected parties that an appeal has been filed.

**Confirmation of Appeal:** This notice informs institutions that an appeal has been accepted. The letter will include the name of the requester, the appeal file number, the IPC contact, and IPC requirements.

**Notice of Inquiry:** The IPC may send a Notice of Inquiry during the intake stage for appeals regarding deemed refusals or where institutions have issued decisions, but have failed to disclose the records to the requester. This notice informs all parties about the nature of the appeal and requests representations from parties in the appeal.

During the intake stage, institutions may be contacted by the IPC to provide additional information including information about affected persons.

## Mediation Stage

A mediator will contact the parties to investigate the circumstances of an appeal and attempts to effect a settlement of the issues.

The mediator can review the records and provide an opinion to the parties on the likely outcome of the appeal at adjudication. The mediator can convene conference calls with the parties to canvass the issues, or engage in shuttle mediation by speaking separately with the appellant and the institution.

Mediators may request additional information from institutions, including information for the purpose of notifying affected persons. Institutions can issue revised decisions during mediation to disclose additional records to an appellant.

Most appeals are resolved through mediation. Even if an appeal is not settled in its entirety, mediation can result in streamlining the issues that need to be adjudicated.

The mediator issues a report to the parties. If the mediation is not successful in settling the dispute, the appeal moves on to the adjudication stage.

## Adjudication

The first step in the adjudication stage usually begins when an adjudicator sends a Notice of Inquiry to the parties bearing the initial onus. This notice informs parties to an appeal of the issues to be decided in the appeal and requests representations on those issues. The adjudicator also summarizes the background of the appeal and describes the records at issue. Once representations are received from the first party, the adjudicator usually sends a Notice of Inquiry to the other party or parties inviting representations.

### Making Representations

Representations are arguments or evidence presented to the adjudicator to persuade them to resolve the appeal in a particular way. The legislation places the burden of proof on different parties depending on the issue:

- The appellant when claiming that a record should to exist; and when claiming a public interest override in favour of disclosure;
- The institution when claiming an exemption or exclusion applies; and
- The affected party when claiming harms and arguing against disclosure.

When preparing representation an institution should consider:

- The type of appeal;
- Address each of the issues raised by the adjudicator;
- Provide detailed evidence and argument;
- Organize representations logically;
- Demonstrate the applicability of exemptions;
- Reference the most recent orders and decisions where possible;
- Indicate which information in the representations the institution regards as confidential and should be withheld from other parties and the reasons why;
- Provide copies of reference materials;
- Provide an index of appeal documents; and
- Use plain language.

## Written or Oral Submissions

The IPC'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 IPC believes that it would aid in an exploration of the issues.

In an inquiry, the IPC 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.

An inquiry must be conducted in a manner that protects the confidentiality of the records pending the IPC's decision. It is not a public hearing, witnesses are generally not cross-examined, and testimony may not be used in other proceedings.

## Sharing Representations

An adjudicator may share representations with other parties to the appeal, unless there are overriding confidentiality concerns. The adjudicator will consider if:

- Disclosure would reveal the substance of the record;
- The information would be exempt if it was in a record;
- The information was communicated to the IPC in confidence with the understanding that it would not be disclosed; and
    - Confidentiality is essential to maintaining relations with the IPC;
    - The relation is one which in the opinion of the community should be maintained; and
    - The injury to the relation would outweigh the benefit correctly determining the appeal.

Although a party is not entitled to access an opposing party's submissions, the IPC may decide to share submissions, in part or in whole, with other parties. The IPC gives parties the opportunity to object to the sharing of their submissions before deciding whether or not to share them. A party may also request a copy of the submission directly from the institution.

### Affidavit and Other Evidence

An affidavit is a statement of facts which is sworn to (or affirmed) before an officer who has authority to administer an oath. Affidavits are a common method of providing evidence. The IPC may request an affidavit be provided in mediation or adjudication. An affidavit may be shared with consent of the parties.

Institutions may decide that an affidavit is an effective way of providing evidence regarding searches, existence of records and contentious issues.

Affidavit evidence should be:

- Detailed enough for the parties to understand the contents; and
- Confined to facts within the personal knowledge of the person swearing.

It is a criminal offence under the Criminal Code to swear a false affidavit.

### Claiming Additional Exemptions

The IPC may allow an institution to claim additional discretionary exemptions at the inquiry stage. This requires that an institution send a new decision letter to the appellant. In these circumstances, further representations may need to be submitted by the parties.

The adjudicator may at any stage request supplementary representations by the parties.

## Providing Records to the IPC

Once an appeal is received by the IPC, institutions will be required to:

- Notify the IPC if the records are voluminous (e.g., 500 pages plus and more than three exemptions);
- Provide relevant records;
- Advise the IPC if the institution plans to claim additional discretionary exemptions; and
- Notify the IPC if records are to be returned to the institution.

Only the documents in the appeal should be sent to the IPC. The relevant documents include:

- 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;
- A severed copy of the records under appeal where severances have been made, and
- Unsevered copy of the records.

The severed and unsevered copies of records do not need to be provided to the IPC in appeals related to fee estimates, time extensions or reasonableness of search.

Institutions should provide the IPC with a well-organized, legible, and complete package of records. The IPC may agree to on-site inspection of records in special circumstances such as highly voluminous requests or fragile records.

Records should be sent securely to the IPC. Records should be sent by bonded courier or may be delivered by an employee of the institution.

## On Hold and Abandoned Appeals

The IPC may place an appeal “on hold” for later resolution. The IPC may treat an appeal as abandoned if an appellant has not responded to the IPC within a time period specified by the IPC.

## Reconsideration of Orders

A reconsideration of an order is not an appeal of an order on its merits. An adjudicator may reconsider a decision where there is:

- A fundamental defect in the adjudication process;
- Some other jurisdictional defect in the decision; or
- A clerical error, accidental error or omission or other similar error in the decision.

A request for reconsideration must comply with the criteria above and be made within 21 days or before the first specified date or time period in the order. An institution must still comply with the terms of an order unless otherwise directed by the IPC. A request

for reconsideration does not preclude a party from seeking other legal remedies for review that may be available.

## Constitutional Issues

A constitutional question may be raised by one of the parties in an appeal or by the IPC for one of the parties to address. A constitutional question raises issues relating to:

- The constitutional validity or applicability of the legislation, a regulation or a by-law, or a rule of common law; or
- A claim for a remedy under the Canadian Charter of Rights and Freedoms.

The IPC must be served notice of a constitutional question using the IPC's form along with written submissions.

## Judicial Review

Judicial review proceedings are governed by the Judicial Review Procedure Act. The criteria for a judicial review by a party to an appeal include where it is alleged that the IPC's decision was patently unreasonable or otherwise outside the IPC's jurisdiction.

Applications for judicial review are made to the Divisional Court and must be made within 30 days of the order or reconsideration order. Appellants and institutions may file judicial review applications. If an appellant or institution does not file an application for judicial review within 30 days, the institution must comply with the IPC's order.

## Resources

IPC: Appeals Process

IPC: Filing an Appeal

IPC: Code of Procedures

IPC: Mediation Tips for Institutions

IPC: Best Practices for Institutions in Mediating Appeals

IPC: Practice Direction #1 – Providing Records to the IPC During an Appeal

IPC: Practice Direction # 2 – Participating in a Written FIPPA or MFIPPA Inquiry

IPC: Practice Direction #3 – Guidelines for Individuals Whose Personal Information is at Issue in an Appeal

IPC: Practice Direction #4 – Guidelines for Parties Whose Commercial or Business Information is at Issue in an Appeal

IPC: Practice Direction #5 – Guidelines for Institutions in Making Representations

IPC: Practice Direction #6 – Affidavit and Other Evidence

IPC: Practice Direction #7 – Sharing of Representations

IPC: Practice Direction #8 – Reasonable Search Appeals and Fee Appeals

IPC: Practice Direction #9 – Constitutional Questions

IPC: Practice Direction #10 – Appeal fees

IPC: Practice Direction #11 – Appeal Form

# Chapter 12: Privacy Complaints, Breaches and Investigations

## Introduction

The IPC has authority under the legislation to investigate matters related to an institution's collection, use, disclosure, retention, security, disposal and destruction of personal information.

When an individual believes an institution has collected, used or disclosed personal information in a manner not consistent with the legislation, they may file a privacy complaint with the IPC.

Institutions may also self-report privacy breaches where the institution has discovered personal information has been accessed by an unauthorized individual or was disclosed in a manner not consistent with the legislation, either intentionally or in error.

In rare cases, an IPC initiated privacy complaint may be opened. This could involve a matter that the IPC considers worthy of investigation but where there is no complainant.

This chapter outlines the IPC's approach to investigating privacy complaints and breaches.

## Privacy Complaints

Individuals have the right to complain to the IPC when they believe that an institution has not complied with the privacy rules on the collection, use, disclosure, retention, security, disposal and destruction of their personal information.

Privacy complaints are usually the result of a privacy breach, which is an incident where personal information is collected, retained, used, disclosed or disposed of in ways that do not comply with the provisions of the legislation.

Individuals are encouraged to attempt to resolve privacy complaints directly with institutions. Institutions have an obligation to work with individuals in addressing privacy concerns.

If an individual believes an institution has not adequately addressed their concerns, the individual may file a privacy complaint with the IPC. The IPC requires the individual to complete a form outlining the following information:

- The individual's own contact information (name, address, telephone);
- The institution's name;
- Details of the nature of the complaint; and
- Details of how the complaint should be resolved.

The privacy complaint form should be filed with the IPC's Registrar.

## Institution Reported Privacy Breaches

Institutions may also self-report privacy breaches and incidents to the IPC. While the legislation does not require institutions to report privacy breaches to the IPC, it is best practice for institutions to self-report substantial breaches to the IPC.

Reporting substantial privacy breaches allows the IPC to understand the nature of the breach and steps being taken to contain and respond to the breach. Proactively sharing information gathered from the institution's own internal investigation and details about how the institution is responding to the breach assists the IPC in determining if further investigation or remedial action is required.

## Privacy Investigation Process

The IPC has broader authority in the context of privacy investigations. A privacy breach is likely the most common reason for an investigation. In addition, the IPC may also comment on the privacy protection implications of proposed legislative schemes or government programs.

As a result of an investigation, the IPC can order an institution to cease a collection of personal information practice, and destroy a collection of personal information that contravenes the legislation.

The IPC can handle privacy investigations informally and formally. In either case, the institution needs to provide information and participate in discussions and meetings with the IPC.

A privacy complaint can be handled informally when the complainant and institution can agree on an approach to resolve the issue. This usually involves information sharing to achieve an understanding of what happened or why the information was used in a certain way.

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 a

mutually satisfactory way, a formal privacy investigation will follow. There are also times when the individual who submitted the complaint is not satisfied, but the IPC dismisses the complaint at an early stage based on the information presented to it. If the complaint is not resolved or dismissed at an early stage, a formal investigation may proceed.

In a formal privacy investigation, the IPC follows the main steps outlined below:

**Notice and request for information:** The IPC notifies the institution that a complaint has been received and requests information relating to the institution's position on the matter.

**Investigation:** The investigation may require a personal visit to the institution by the investigator and/or meetings with key program staff. Copies of relevant documents must be provided.

**Draft report:** The IPC may conclude with a letter in straightforward matters. In other cases, the matter will proceed with a draft report. Where a privacy breach has occurred, the draft report may include recommendations to prevent future breaches.

Both the institution and the individual who submitted the complaint are asked to comment on errors or omissions in the draft report.

**Final report:** Formal investigations may result in a formal public report, usually if the matter is of interest to the public. Where recommendations have been made, the IPC will request evidence of implementation of the recommendations within six months of the date of the final report.

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:** Within six months, the IPC will contact the institution to find out the status of recommendations, and if nothing has been done, the reason why.

## Resources

IPC: Filing a Privacy Complaint

IPC: The Privacy Complaint Process

IPC: Privacy Complaint Form

# Part V: Appendices

# Appendix 1: Sample Draft By-Law Designating Head Under MFIPPA

THE CORPORATION OF THE [**insert name of Municipal Corporation**]

BY-LAW NO. [**Insert by-law number**]

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 (here after the 'Act'), 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 [**insert name/position of member of council or committee of council**] be designated as head for the purposes of the Act.

2. That this by-law come into force and effect on [**insert date**].

Read a first and second time this **[insert day]** day of [**insert month**], [**insert year**].

[**Insert signature of Clerk and head of Council**]

Read a third time and passed this **[insert day]** day of [**insert month**], [**insert year**].

[**Insert signature of Clerk and head of Council**]

[**Insert seal of the municipal corporation**]

# Appendix 2: Sample Resolution Designating Head Under MFIPPA

RESOLUTION

FOR [**insert board commission or other body name**]

MOVED BY: [**insert name of individual**]

SECONDED BY: [**insert name of individual**]

Whereas, under Section 3, subsection (2) of the Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990 c.M.56 (here after the 'Act') 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 [**insert name of board, commission or other body**] deems it necessary and expedient to designate a head for the purposes of the Act:

Now, therefore, the [**insert name of board, commission or other body**] resolves as follows:

1. That the [**insert name of board, commission or other body**] hereby designates [**insert the name or position of individual or committee**] as head for the purposes of the Act.
2. That this resolution come into force and effect on [**insert date here**].

[**Insert signature of Secretary or Chairperson]**

# Appendix 3: Sample Delegation of Authority

## 3.1 – Detailed Delegation of Authority

[**Insert institution name**]

DELEGATION OF POWERS AND DUTIES OF THE HEAD UNDER THE [MUNICIPAL FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT ([M]FIPPA)

**1.0 Delegation**

1.1 Pursuant to subsection [**62 (1) of the Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31** OR **49 (1) of the Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56**] and subject to section 2.0 below, I hereby delegate the powers and duties of the [**insert title of head**] as head of the [**insert institution name**] to the following officers of the institution:

(a) [**Insert title of delegated position**]; and

(b) [**Insert additional title of delegated positions as needed**];

**2.0 Limitations, restrictions, conditions and requirements**

2.1 The officers of the institution listed in section 1.1 above shall exercise the delegated powers and perform the delegated duties as outlined in Schedules A, B, and C.

2.2 The powers and duties delegated to each of the delegates named herein may also be exercised by such persons who hold the position in an acting capacity to which he or she has been duly appointed, or by such persons who are duly authorized to act for the delegate in his or her absence.

**3.0 Effect on previous delegations**

3.1 The previous delegations under the Act by the [**insert title of head of institution**] are hereby revoked.

**4.0 Term of delegation**

4.1 This delegation is effective from the date set out below and shall remain in effect until such date as it is revoked by the [**insert title of head of institution**].

[**Insert signature of head**] [**Insert date**]

| Section | Decision | Delegated Decision-Maker | Alternate Delegated Decision-Maker |
|---|---|---|---|
| **FIPPA:** 10<br>**MFIPPA:** 4 | Grant access in whole to general information. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 10 (1), 25<br>**MFIPPA:** 4 (1), 18 | Determine whether the institution has custody or control of a record. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 10 (1)(a), 12 to 22<br>**MFIPPA:** 4 (1)(a), 6 to 15 | Determine whether exemptions apply in whole or in part to a record. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 10 (1)(b), 24 (1.1), Reg. 460 (5.1)<br>**MFIPPA:** 4 (1)(b), 20.1, Reg. 823 (5.1) | Determine whether a request is frivolous or vexatious. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 10 (2)<br>**MFIPPA:** 4 (2) | Refuse access in whole to general information or grant access in part. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 11<br>**MFIPPA:** 5 | Disclose a record in the public interest where the record reveals a grave environmental, health or | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if** |

| Section | Decision | Delegated Decision-Maker | Alternate Delegated Decision-Maker |
|---|---|---|---|
| | safety hazard and if practicable, give notice to any person to whom the information relates. | | **applicable**] |
| **FIPPA:** 23<br>**MFIPPA:** 16 | Determine whether a compelling public interest outweighs the exemptions under sections [**13, 15, 15.1, 17, 18, 20, 21 or 21.1** OR **7, 9, 9.1, 10, 11, 13 or 14**]. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 28 (7)<br>**MFIPPA:** 21 (7) | Decide whether to grant or refuse access to whole record or part of record; give notice of decision to affected person and requester. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 47 (1)<br>**MFIPPA:** 36 (1) | Grant access in whole to personal information to the individual to whom it relates. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 49<br>**MFIPPA:** 38 | Refuse an individual access in whole or in part to their own personal information. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 47 (2)<br>**MFIPPA:** 36 (2) | Grant or refuse an individual's request for correction of their personal information. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |

| Section | Decision | Delegated Decision-Maker | Alternate Delegated-Decision Maker |
|---|---|---|---|
| **FIPPA:** 24 (2)<br>**MFIPPA:** 17 (2) | Offer assistance to requester in reformulating request when it is unclear (clarifying a request). | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 24 (4)<br>**MFIPPA:** 17 (4) | Provide requester with schedule of dates for continuing access requests. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 25 (1)<br>**MFIPPA:** 18 (2) | Determine which institution has custody or control of the requested records, forward request and notify requester. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 25 (2)<br>**MFIPPA:** 18 (3) | Determine if another institution has a greater interest in the record and transfer the request and, if necessary, the record. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 26, 27.1, 29, 30<br>**MFIPPA:** 19, 20.1, 22, 23 | Give notice of access to a record or notice of refusal to give access to a record. If access is given, provide access to record or cause record to be produced; allow examination of original record. If access is | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |

| Section | Decision | Delegated Decision-Maker | Alternate Delegated-Decision Maker |
|---|---|---|---|
| | denied, provide explanation. | | |
| **FIPPA:** 27<br><br>**MFIPPA:** 20 | Extend time limit and give notice of time extension to requester. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 28<br><br>**MFIPPA:** 21 | Give notice to affected persons; give notice of delay to requester. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 33<br><br>**MFIPPA:** N/A | Make manuals, directives and guidelines available on the internet or in a reading room. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 34<br><br>**MFIPPA:** 26 | Produce Annual Report. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 36<br><br>**MFIPPA:** 25 | **FIPPA:** Information to be made available to responsible Minister for Directory of Records.<br><br>**MFIPPA:** Information to be made available to the public for Directory of Records. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 24 (1)(c), 57, Reg. 460 | Fee administration (including application fee), calculation of fees | [**insert position of delegated** | [**insert position of alternate delegated** |

| Section | Decision | Delegated Decision-Maker | Alternate Delegated-Decision Maker |
|---|---|---|---|
| (5.2), (6), (6.1) (7), (9)<br><br>**MFIPPA:** 14 (1)(c), 57, Reg. 823 (5.2), (6), (6.1) (7), (9) | and deposits. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 57 (4), Reg. 460 (8)<br><br>**MFIPPA:** 45 (4), Reg. 823 (8) | If it is determined to be fair and equitable, grant a fee waiver | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 63 (1)<br><br>**MFIPPA:** 50 (1) | Grant access in the absence of a written request. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |

## Schedule C to Sample Delegation of Authority – Privacy and Security Responsibilities

| Section | Decision | Delegated Decision-Maker | Alternate Delegated-Decision Maker |
|---|---|---|---|
| **FIPPA:** 38 (2)<br><br>**MFIPPA:** 28 (2) | Ensure personal information is collected with lawful authority | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 39 (2)<br><br>**MFIPPA:** 29 (2) | Provide a proper notice when personal information is collected. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 40 (1), Reg. 460(5)<br><br>**MFIPPA:** 30 (1), Reg. 823 (5) | Ensure personal information is retained for a period of one year after use (or a lesser time frame with consent). | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 40 (2)<br><br>**MFIPPA:** 30 (2) | Ensure personal information used is accurate and up-to-date. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 41, 43<br><br>**MFIPPA:** 31, 33 | Ensure personal information is used with lawful authority. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 42, 43<br><br>**MFIPPA:** 32, 33 | Ensure personal information is disclosed with lawful authority. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |

| Section | Decision | Delegated Decision-Maker | Alternate Delegated-Decision Maker |
|---|---|---|---|
| **FIPPA:** 21 (1)(e), Reg. 460 (10)<br><br>**MFIPPA:** 14 (1)(e), Reg. 823 (10) | Approve the disclosure of personal information for a research purpose. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 40 (4), Reg. 459 (3)<br><br>**MFIPPA:** 40(4) | Authorization to destroy personal information. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 40 (4), Reg. 459 (4)<br><br>**MFIPPA:** 40 (4) | Take steps to ensure the security and confidentiality of personal information transferred to the Archives or destroyed. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 10.1<br><br>**MFIPPA:** 4.1 | Ensure recordkeeping polices are put in place and records are managed in accordance with polices and requirements. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** Reg. 460 (4)<br><br>**MFIPPA:** Reg. 823 (3) | Prevent unauthorized access to records. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** Reg. 460 (4)<br><br>**MFIPPA:** Reg. | Protect records from inadvertent destruction and damage. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker** |

| Section | Decision | Delegated Decision-Maker | Alternate Delegated-Decision Maker |
|---|---|---|---|
| 823 (3) | | | **if applicable**] |
| **FIPPA:** 44<br><br>**MFIPPA:** 34 | Developing personal information banks. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |
| **FIPPA:** 46<br><br>**MFIPPA:** 35 | Record and notification of inconsistent uses or disclosures of personal information. | [**insert position of delegated decision-maker**] | [**insert position of alternate delegated decision maker if applicable**] |

## 3.2 – Simplified Delegation of Authority for Small Institutions

[**Insert institution name**]

DELEGATION OF POWERS AND DUTIES OF THE HEAD UNDER THE [MUNICIPAL FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT ([M]FIPPA)

[**I** OR **We**] [**Insert name of 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 [**insert position title of delegated decision maker**] effective on [**insert date**].

[**Insert signature and title of head**]

[**Insert date**]

# Appendix 4: Template Letters for Request Processing

## 4.1 – Letter to Requester Acknowledging Request - Standard

[I**nsert date**]

[**Insert name and address of requester**]

**Access Request**: [**insert access request number**]

Dear [**insert name of requester**]:

I am writing to inform you that your access request under the [Municipal] Freedom of Information and Protection of Privacy Act, along with your $5.00 application fee, was received in our office on [**insert date**] and is being processed.

Your request is for the following information:

[**Insert details of records requested**]

Should you have any questions, please contact [**insert name, title and phone number of person responsible**]. We would appreciate you using the above listed access request number in any further correspondence.

Sincerely,

[**Insert signature**]

## 4.2 – Letter to Requester Acknowledging Request – Application Fee Missing

[**Insert date**]

[**Insert name and address of requester**]

**Access Request**: [**insert access request number**]

Dear [**insert name of requester**]:

I am writing to inform you that your access request under the [Municipal] Freedom of Information and Protection of Privacy Act was received in our office on [**insert date**].

Your request is for the following information:

[**Insert details of records requested**]

In order to proceed with your request, we require a $5.00 application fee. If paying by cheque or money order, please make the application fee payable to **[insert payee information**]. Once we have received payment, we will proceed with processing your request.

If we do not hear from you within 30 days of this letter's date, we will close your file.

Should you have any questions, please contact [**insert name, title and phone number of person responsible**]. We would appreciate you using the above listed access request number in any further correspondence.

Sincerely,

[**Insert signature**]

## 4.3 – Letter to Requester Acknowledging Request – Clarification Required

[**Insert date**]

[**Insert name and address of requester**]

**Access Request**: [**insert access request number**]

Dear [**insert name of requester**]:

I am writing to inform you that your access request under the [Municipal] Freedom of Information and Protection of Privacy Act, along with your $5.00 application fee, was received in our office on [**insert date**].

Your request is for the following information:

[**Insert details of records requested**]

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.

Should you have any questions, please contact [**insert name, title and phone number of person responsible**]. We would appreciate you using the above listed access request number in any further correspondence.

Sincerely,

[**Insert signature**]

## 4.4 – Letter to Requester Acknowledging Request – Proof of Identity Required

[**Insert date**]

[**Insert name and address of requester**]

**Access Request**: [**insert access request number**]

Dear [**insert name of requester**]:

I am writing to inform you that your access request under the [Municipal] Freedom of Information and Protection of Privacy Act was received in our office on [**insert date**].

Your request is for the following information:

[**Insert details of records requested**]

Pursuant to paragraph 3 (3) of Regulation 460, we are required to verify the identity of individuals seeking access to their own personal information. Please provide our office with a photocopy of one piece of valid government issued photograph identification.

Once we have received verification of your identity, we will proceed with processing your request.

Should you have any questions or require an alternate method to verify your identity, please contact [**insert name, title and phone number of person responsible**]. We would appreciate you using the above listed access request number in any further correspondence.

Sincerely,

[**Insert signature**]

## 4.5 – Letter to Requester when Transferring of Forwarding a Request

[**Insert date**]

[**Insert name and address of requester**]

**Access Request**: [**insert access request number**]

Dear [**insert name of requester**]:

I am writing to inform you that your access request under the [Municipal] Freedom of Information and Protection of Privacy Act (hereafter 'the 'Act'), along with your $5.00 application fee, was received in our office on [**insert date**].

[**Insert name and address of other institution**] has [**custody and control of** OR **a greater interest in**] the records you seek. Under section [**25** OR **18**] of the Act, we [**forwarded** OR **transferred**] your access request to them. We have enclosed a copy of section [**25** OR **18**] for your review.

[If receiving institution is a different payee, add: **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**.]

[If the receiving institution is the same payee (ie: the Minister of Finance), add: **We have forwarded your $5.00 application fee along with your request.** OR **We have processed your $5.00 application fee on behalf of the receiving institution.**]

Should you have any questions, please contact [**insert name, title and phone number of person responsible**]. We would appreciate you using the above listed access request number in any further correspondence.

Sincerely,

[**Insert signature**]

## 4.6 – Letter to Receiving Institution when Transferring or Forwarding a Request

[**Insert date**]

[I**nsert name and address of receiving institution**]

Dear [**insert name of requester**]:

The enclosed request for access was received by our office on [**insert date request was received**].

This request is [**transferred** OR **forwarded**] to you under section [**25 of the Freedom of Information and Protection of Privacy Act** OR **18 of the Municipal Freedom of Information and Protection of Privacy Act**] as we believe your institution has [**custody or control of** OR **a greater interest in**] the record.

[If receiving institution is a different payee, add: **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**.]

[If the receiving institution is the same payee (ie: the Minister of Finance), add: **We have forwarded your $5.00 application fee along with your request.** OR **We have processed your $5.00 application fee on behalf of the receiving institution.**]

Should you have any questions, please contact [**insert name, title and phone number of person responsible**].

Sincerely,

[**Insert signature**]

## 4.7 – Letter to Requester – Notice of Time Extension

[**Insert date**]

[**Insert name and address of requester**]

**Access Request:** [**insert access request number**]

Dear [**insert name of requester**]:

I am writing regarding your access request under the [Municipal] Freedom of Information and Protection of Privacy Act (hereafter, 'the Act') received by our office on [**insert date request was received**].

A request under the Act usually must be answered within 30 calendar days; however, section [**27** OR **20**] allows for time extensions under certain circumstances. The time limit for answering your request has been extended for an additional [**insert number of days**] days to [**insert new due date**].

The reason for the time extension is [**due to a large volume of records that must be searched in order to respond to your request** OR **due to a large volume of records that must be reviewed in order to respond to your request** OR **to conduct consultations with external parties**].

A copy of section [**27** OR **20**] of the Act is enclosed for your information.

You may request the Information and Privacy Commissioner to review this decision to extend the timeline to response within thirty days from the date of this letter. The Commissioner's address is Suite 1400, 2 Bloor Street East, Toronto, Ontario, M4W 1A8. The appeal fee is [**$25.00** (for general record requests) OR **$10.00** (for personal information requests)], payable by cheque or money order to the Minister of Finance and must be included with your correspondence.

Should you have any questions, please contact [**insert name, title and phone number of person responsible**]. We would appreciate you using the above listed access request number in any further correspondence.

Sincerely,

[**Insert signature**]

## 4.8 – Letter to Requester – Fee Estimate and Interim Decision - $25 to $99 Fee

[**Insert date**]

[**Insert name and address of requester**]

**Access Request:** [**insert access request number**]

Dear [**insert name of requester**]:

I am writing regarding your access request under the [Municipal] Freedom of Information and Protection of Privacy Act (hereafter, 'the Act') received by our office on [**insert date request was received**].

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**].

Section [**57** or **45**] of the Act requires fees to be charged for processing a request. The fee estimate for processing this request is [**insert total fee estimate**]. The breakdown for your fee estimate is as follows:

- [**$XX**] for search time based on [**insert time]** hours of time @ $7.50 per quarter hour;
- [**$XX**] for records preparation based on [**insert time**] hours of time @ $7.50 per quarter hour; and
- [**$XX**] for photocopying based on [**insert page numbers**] pages @ 20 cents per page.

Please note: this represents an estimate of fees based on preliminary work. The final fee calculation may vary. Please do not provide any fee payment at this time.

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. 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.

You may request the Information and Privacy Commissioner to review this fee estimate within thirty days from the date of this letter. The Commissioner's address is Suite 1400, 2 Bloor Street East, Toronto, Ontario, M4W 1A8. The appeal fee is [**$25.00** (for general record requests) OR **$10.00** (for personal information requests)], payable by cheque or money order to the Minister of Finance and must be included with your correspondence.

Copies of section [**insert sections of exemptions that may be claimed in interim decision**] and [**57** OR **45**] of the Act are enclosed for your information.

Should you have any questions, please contact [**insert name, title and phone number of person responsible**]. We would appreciate you using the above listed access request number in any further correspondence.

Sincerely,

[**Insert signature**]

## 4.9 – Letter to Requester – Fee Estimate and Interim Decision – Over $100 Fee

[**Insert date**]

[**Insert name and address of requester**]

**Access Request:** [**insert access request number**]

Dear [**insert name of requester**]:

I am writing regarding your access request under the [Municipal] Freedom of Information and Protection of Privacy Act (hereafter, 'the Act') received by our office on [**insert date request was received**].

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**].

Section [**57** or **45**] of the Act requires fees to be charged for processing a request. The fee estimate for processing this request is [**insert total fee estimate**]. The breakdown for your fee estimate is as follows:

- [**$XX**] for search time based on [**insert time]** hours of time @ $7.50 per quarter hour;
- [**$XX**] for records preparation based on [**insert time**] hours of time @ $7.50 per quarter hour; and
- [**$XX**] for photocopying based on [**insert page numbers**] pages @ 20 cents per page.

Subsection 7(1) of Regulation [**460** OR **823**] under the Act provides that when an estimate is over $100.00 the institution may collect 50% of the estimated fee prior to the completion of the request. Please make your cheque or money order for [**insert 50% of total fee estimate**] payable to the [**insert payee information**] and forward it to my attention. Receipt of the fee deposit is requested prior to completing your request. Please do not send the full estimate at this time. We will calculate the actual fee and include the balance owing when you are notified of the decision regarding your access 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. 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.

You may request the Information and Privacy Commissioner to review this fee estimate within thirty days from the date of this letter. The Commissioner's address is Suite 1400, 2 Bloor Street East, Toronto, Ontario, M4W 1A8. The appeal fee is [**$25.00** (for general record requests) OR **$10.00** (for personal information requests)], payable by cheque or money order to the Minister of Finance and must be included with your correspondence.

Copies of section [**insert sections of exemptions that may be claimed in interim decision**] and [**57** OR **45**] of the Act are enclosed for your information.

Should you have any questions, please contact [**insert name, title and phone number of person responsible**]. We would appreciate you using the above listed access request number in any further correspondence.

Sincerely,

[**Insert signature**]

## 4.10 – Notice to Affected Person for Third Party Information

[**Insert date**]

[I**nsert name and address of third party**]

**Access Request:** [**insert access request number**]

Dear [**insert name of third party**]:

[**Insert name of institution**] has received a request for access to records under the [Municipal] Freedom of Information and Protection of Privacy Act (hereafter 'the Act') to disclose [**describe in detail the records as they relate to the affected third party**].

According to section [**28** OR **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 or 10] of the Act, we must release these records unless the above conditions are met. Copies of sections [**17 and 28** OR **10 and 21**] of the Act are enclosed along with the impacted records. 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.

Should you have any questions, please contact [**insert name, title and phone number of person responsible**]. We would appreciate you using the above listed access request number in any further correspondence.

Sincerely,

[**Insert signature**]

## 4.11 – Notice to Affected Person for Personal Privacy

[**Insert date**]

[**Insert name and address of affected party**]

**Access Request:** [**insert access request number**]

Dear [**insert name of affected party**]:

[**Insert name of institution**] has received a request for access to records under the [Municipal] Freedom of Information and Protection of Privacy Act (hereafter 'the Act') to disclose [**describe in detail the records as they relate to the s affected individual**].

Section [**28** OR **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 would be 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** OR **14**] of the Act outlines circumstances where the disclosure of personal information may be an unjustified invasion of personal privacy.

Copies of sections [21 and 28 OR 14 and 21] are enclosed for your review.

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.

Should you have any questions, please contact [**insert name, title and phone number of person responsible**]. We would appreciate you using the above listed access request number in any further correspondence.

Sincerely,

[**Insert signature**]

## 4.12 – Letter to Requester – Notice of Delay Where a Third Party's Interests are Impacted

[**Insert date**]

[**Insert name and address of requester**]

**Access Request:** [**insert access request number**]

Dear [**insert name of requester**]:

I am writing regarding your access request under the [Municipal] Freedom of Information and Protection of Privacy Act (hereafter, 'the Act') received by our office on [**insert date request was received**].

The disclosure of the records may affect the interests of a third party.

Under section [28 OR 21], we are required to notify third parties whose interest may be affected by the disclosure of records. Third parties then have an opportunity to make representations about the release of the record(s).

This process requires the timelines for response to be adjusted. A decision on whether or not the record(s) will be disclosed will be made by [**insert date**].

A copy of section [28 OR 21] of the Act is enclosed for your information.

Should you have any questions, please contact [**insert name, title and phone number of person responsible**]. We would appreciate you using the above listed access request number in any further correspondence.

Sincerely,

[**Insert signature**]

## 4.13 – Letter to Affected Person – Notice to Disclose Information

[**Insert date**]

[I**nsert name and address of affected party**]

**Access Request:** [**insert access request number**]

Dear [**insert name of affected party**]:

Thank you for your representations dated **[insert date on representations]** concerning disclosure to [**insert description or details of records**]. A decision has been made to grant access [OR **partial access**] to the requester.

The official responsible for making the access decision on your request is [**insert name and title of delegated decision maker**].

You may request the Information and Privacy Commissioner to review this decision within thirty days from the date of this letter. The Commissioner's address is Suite 1400, 2 Bloor Street East, Toronto, Ontario, M4W 1A8.

If no appeal is filed with the Information and Privacy Commissioner, full access to these records will be provided to the requester after [**insert date**].

Should you have any questions, please contact [**insert name, title and phone number of person responsible**]. We would appreciate you using the above listed access request number in any further correspondence.

Sincerely,

[**Insert signature**]

## 4.14 – Letter to Affected Person – Notice to Withhold Information

[**Insert date**]

[**Insert name and address of affected party**]

**Access Request:** [**insert access request number**]

Dear [**insert name of affected party**]:

Thank you for your representations dated [**insert date on representations**] concerning disclosure to [**insert description or details of records**].

After consideration of these representations, [**insert name of institution**] agrees with your submissions. Pursuant to section [17 OR 21 OR 10 OR 14] of the [Municipal Freedom of Information and Protection of Privacy Act, a decision has been made to deny the requester access to [**insert description or details of records**] in their entirety.

The official responsible for making the access decision on your request is [**insert name and title of delegated decision maker**].

Please be advised that the requester may appeal this decision to the Information and Privacy Commissioner of Ontario.

Should you have any questions, please contact [**insert name, title and phone number of person responsible**]. We would appreciate you using the above listed access request number in any further correspondence.

Sincerely,

[I**nsert signature**]

## 4.15 – Letter to Requester – Decision to Disclose All Records

[**Insert date**]

[**Insert name and address of requester**]

**Access Request:** [**insert access request number**]

Dear [**insert name of requester**]:

I am writing regarding your access request under the [Municipal] Freedom of Information and Protection of Privacy Act (hereafter, 'the Act') received by our office on [**insert date request was received**].

A search has been conducted and the responsive records have been reviewed. A decision has been made to grant access to the records in full. [If no fee required add: **The responsive records are enclosed.**]

[If some records were subject to a notice under section 28/21 add: **Some of the responsive records impacted the interests of other parties. As a result, we cannot disclose these records for an additional 30 days, to allow the affected parties an opportunity to appeal this decision. If no notice of appeal is received by our office within 30 days, we can proceed with disclosing these records.**]

The official responsible for making the access decision on your request is [**insert name and title of delegated decision maker**].

The estimated fee for processing your request was [**insert estimated total].** The actual fee for processing your request is [**insert actual total].** The breakdown for your fee is as follows:

- [**$XX**] for search time based on [**insert time]** hours of time @ $7.50 per quarter hour;
- [**$XX**] for records preparation based on [**insert time**] hours of time @ $7.50 per quarter hour; and
- [**$XX**] for photocopying based on [**insert page numbers**] pages @ 20 cents per page.

[If fee deposit was paid, add: **Your deposit of $XX will be deducted from this total fee**.] The records will be prepared and made available to you upon receipt of the outstanding balance of [**insert fee total** OR **fee total minus fee deposit**]. Please note, if we do not receive your fee payment within 30 days of the date on this letter, we will consider your request abandoned and close the file.

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. 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.

You may request the Information and Privacy Commissioner to review this decision and fee within thirty days from the date of this letter. The Commissioner's address is Suite 1400, 2 Bloor Street East, Toronto, Ontario, M4W 1A8. The appeal fee is [**$25.00** (for general record requests) OR **$10.00** (for personal information requests)], payable by cheque or money order to the Minister of Finance and must be included with your correspondence.

A copy of section [**57** OR **45**] of the Act is enclosed for your information.

Should you have any questions, please contact [**insert name, title and phone number of person responsible**]. We would appreciate you using the above listed access request number in any further correspondence.

Sincerely,

[**Insert signature**]

## 4.16 – Letter to Requester – Decision to Deny Access in Full or in Part

[**Insert date**]

[**Insert name and address of requester**]

**Access Request:** [**insert access request number**]

Dear [**insert name of requester**]:

I am writing regarding your access request under the [Municipal] Freedom of Information and Protection of Privacy Act (hereafter, 'the Act') received by our office on [**insert date request was received**].

A search has been conducted and the responsive records have been reviewed. A decision has been made to [**grant access in part** OR **deny access in full**]. Information on [**XX**] of records will be severed and [**XX**] of pages will be withheld in full pursuant to sections [**insert relevant exceptions**] of the Act.

[If some records were subject to a notice under section 28/21 add: **Some of the responsive records impacted the interests of other parties. As a result, we cannot disclose these records for an additional 30 days, to allow the affected parties an opportunity to appeal this decision. If no notice of appeal is received by our office within 30 days, we can proceed with disclosing these records.**]

The official responsible for making the access decision on your request is [**insert name and title of delegated decision maker**].

The estimated fee for processing your request was [**insert estimated total].** The actual fee for processing your request is [**insert actual total].** The breakdown for your fee is as follows:

- [**$XX**] for search time based on [**insert time]** hours of time @ $7.50 per quarter hour;
- [**$XX**] for records preparation based on [**insert time**] hours of time @ $7.50 per quarter hour; and
- [**$XX**] for photocopying based on [**insert page numbers**] pages @ 20 cents per page.

[If fee deposit was paid, add: **Your deposit of $XX will be deducted from this total fee**.] The records will be prepared and made available to you upon receipt of the outstanding balance of [**insert fee total** OR **fee total minus fee deposit**]. Please note,

if we do not receive your fee payment within 30 days of the date on this letter, we will consider your request abandoned and close the file.

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. 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.

You may request the Information and Privacy Commissioner to review this decision and fee within thirty days from the date of this letter. The Commissioner's address is Suite 1400, 2 Bloor Street East, Toronto, Ontario, M4W 1A8. The appeal fee is [**$25.00** (for general record requests) OR **$10.00** (for personal information requests)], payable by cheque or money order to the Minister of Finance and must be included with your correspondence.

Copies sections [**insert relevant sections for exemptions claimed**] and [**57** OR **45**] of the Act are enclosed for your information.

Should you have any questions, please contact [**insert name, title and phone number of person responsible**]. We would appreciate you using the above listed access request number in any further correspondence.

Sincerely,

[**Insert signature**]

## 4.17 – Letter to Requester – Decision to Refuse to Confirm or Deny Existence of Record

[**Insert date**]

[**Insert name and address of requester**]

**Access Request:** [**insert access request number**]

Dear [**insert name of requester**]:

I am writing regarding your access request under the [Municipal] Freedom of Information and Protection of Privacy Act (hereafter, 'the Act') received by our office on [**insert date request was received**].

Pursuant to section [**21(5)/14(5)** OR **14(3)/8(3)**], we cannot confirm or deny the existence of the record, as the disclosure of the existence of a record would [**constitute an unjustified invasion of privacy** OR **compromise a law enforcement matter**].

The official responsible for making the access decision on your request is [**insert name and title of delegated decision maker**].

You may request the Information and Privacy Commissioner to review this decision within thirty days from the date of this letter. The Commissioner's address is Suite 1400, 2 Bloor Street East, Toronto, Ontario, M4W 1A8. The appeal fee is [**$25.00** (for general record requests) OR **$10.00** (for personal information requests)], payable by cheque or money order to the Minister of Finance and must be included with your correspondence.

Copies sections [**insert relevant sections for exemptions claimed**] of the Act are enclosed for your information.

Should you have any questions, please contact [**insert name, title and phone number of person responsible**]. We would appreciate you using the above listed access request number in any further correspondence.

Sincerely,

[**Insert signature**]

## 4.18 – Letter to Requester – Decision of No Responsive Records Exist

[**Insert date**]

[**Insert name and address of requester**]

**Access Request:** [**insert access request number**]

Dear [**insert name of requester**]:

I am writing regarding your access request under the [Municipal] Freedom of Information and Protection of Privacy Act (hereafter, 'the Act') received by our office on [**insert date request was received**].

A search has been conducted and the responsive records and no responsive records were located.

The official responsible for making the access decision on your request is [**insert name and title of delegated decision maker**].

You may request the Information and Privacy Commissioner to review the sufficiency of our institution's search for records within thirty days from the date of this letter. The Commissioner's address is Suite 1400, 2 Bloor Street East, Toronto, Ontario, M4W 1A8. The appeal fee is [**$25.00** (for general record requests) OR **$10.00** (for personal information requests)], payable by cheque or money order to the Minister of Finance and must be included with your correspondence.

Should you have any questions, please contact [**insert name, title and phone number of person responsible**]. We would appreciate you using the above listed access request number in any further correspondence.

Sincerely,

[**Insert signature**]

## 4.19 – Letter to Requester – Decision Approving Correction of Personal Information Request

[**Insert date**]

[**Insert name and address of requester**]

Access Request: [**insert access request number**]

Dear [**insert name of requester**]:

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.

[**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. The personal information of individuals acting in a personal capacity should not be included on the list.]

The official responsible for making the access decision on your request is [**insert name and title of delegated decision maker**].

Should you have any questions, please contact [**insert name, title and phone number of person responsible**]. We would appreciate you using the above listed access request number in any further correspondence.

Sincerely,

[**Insert signature**]

## 4.20 – Letter to Requester – Decision Denying Correction of Personal Information Request

[**Insert date**]

[**Insert name and address of requester**]

**Access Request:** [**insert access request number**]

Dear [**insert name of requester**]:

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 not made to the personal information. [Insert reason why request was refused consider including discussion of three part test: 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 OR whether it is a law enforcement record.]

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.

[**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. The personal information of individuals acting in a personal capacity should not be included on the list.]

The official responsible for making the access decision on your request is [**insert name and title of delegated decision maker**].

You may request the Information and Privacy Commissioner to review this decision within thirty days from the date of this letter. The Commissioner's address is Suite 1400, 2 Bloor Street East, Toronto, Ontario, M4W 1A8. The appeal fee is $10.00, payable by cheque or money order to the Minister of Finance, and must be included with your correspondence.

Should you have any questions, please contact [**insert name, title and phone number of person responsible**]. We would appreciate you using the above listed access request number in any further correspondence.

Sincerely,

[**Insert signature**]

## 4.21 – Letter to Requester Advising Request will be Considered Abandoned

[**Insert date**]

[**Insert name and address of requester**]

**Access Request:** [**insert access request number**]

Dear [**insert name of requester**]:

I am writing regarding your access request under the [Municipal] Freedom of Information and Protection of Privacy Act (hereafter, 'the Act') received by our office on [**insert date request was received**].

On [**insert date**] our office contacted you regarding [**a fee estimate** OR **clarifying your request**]. We have not yet received your reply.

In absence of a response, we will consider your request abandoned and close the file on [**insert date**].

Should you have any questions, please contact [**insert name, title and phone number of person responsible**]. We would appreciate you using the above listed access request number in any further correspondence.

Sincerely,

[**Insert signature**]

# Appendix 5: Sample Record Search Form

**Instructions to Program Area:**

Complete this form if the total search time amounts to less than 3 hours or if you have been expressly asked to complete a full retrieval.

This form documents the search activities of the program area and is used to calculate fees for searching and retrieving records. Note: additional fees may be applied for records preparation or other administrative actions.

Please complete this form and return it electronically. If you are mailing your retrieved records, please include a copy of this form.

Before sending digital records or digitally scanning any records, please contact the FOI Coordinator for instructions.

If your search time will be more than 3 hours, use Fee Estimate Form.

**Reference #:** [insert access request number]

**Program Area Contact:** [insert program area contact including responsible for conducting or coordinating search - one form per program area is requested – include name, position and office telephone number]

**Program Area:** [insert name of program area or office conducting search]

**Date(s) of search:** [insert dates of search]

1. Indicate the information banks that were searched [whose computer, which files (hard copy and shared drives)], which offices or file rooms.

---

2. Name(s) and position title(s) of staff contacted during the search.

---

3. Methods/processes used to conduct the search and types of files searched (searching emails, other electronic files, paper files, file lists, off-site file lists, microfiche, etc.)

---

4. Were responsive records located? If no, is there another location where they may be? If responsive records once existed but were destroyed, or have gone missing, please explain.

---

5. Do any responsive records contain personal information of the requester? If yes, search time and severing should not be included in the search fee.

---

6. Are there any issues/sensitivities around these records or this request? If yes, please explain. Please keep in mind that our staff may have no familiarity with your records.

---

7. **Number of hours required to complete search (to the nearest ¼ hour, do not include photocopy time):_____hrs.**

8. **Was a computer programmer required to write code to retrieve any of the records for this request? Yes/No**

# Appendix 6: Sample Fee Estimate Form

**Instructions to Program Area:**

Complete this form if the total search is estimated to take more than 3 hours (do not retrieve records).

This information will be used to create a fee estimate for the requester, and to inform them of the general nature of the responsive records. Other staff's search time should be considered when determining whether more than 3 hours will be required (if multiple program areas are impacted).

Please complete this form and return it electronically.

If your search time will be less than 3 hours, use Record Search Form.

**Reference #:** [insert access request number]

**Program Area Contact:** [insert program area contact including responsible for conducting or coordinating search - one form per program area is requested – include name, position and office telephone number]

**Program Area:** [insert name of program area or office conducting search]

**Date(s) of search:** [insert dates of search]

1. Indicate which locations will require searching (whose computer, which files, which offices or file rooms).

---

2. Name(s) of all staff contacted.

---

3. Methods/processes used to arrive at the estimate and the types of files searched (emails, paper files, etc.)

---

4. Was a representative sample utilized? If so, describe locations searched, sample size, the number of hours used to search the sample, the number of pages of responsive records found in the sample and any other costs incurred in searching the sample etc.

---

5. Do any responsive records contain personal information of the requester? If yes, search time and severing should not be included in the search fee.

---

6. Estimate hours required to complete search (to the nearest ¼ hour, do not include photocopy time):_____hrs.

7. Estimated number of pages of responsive records:_____pgs.

**8. Estimated number of pages which may require partial or full MFIPPA severances (third party or personal information, legal advice, etc.)_____pgs.**

**9. Will a computer programmer be required to write code to retrieve any of the records for this request? Yes/No**

10. Is there likely to be any third party information in the responsive records, if so, please explain.

---

11. Types of records likely to be retrieved (emails, correspondence, spreadsheets, maps, briefing notes etc.).

---

# Appendix 7: Sample Index of Records

| Document Number | Document Description | Number of Pages | Decision to Release | Exemptions Applied | Comments |
|---|---|---|---|---|---|
| [number each document] | [briefly describe each document, include date] | [calculate number of pages in document] | [enter decision: release in full, withhold in full, or withhold in part] | [enter exemptions applied to withheld information] | [enter relevant comments including IPC orders or case law supporting application of exemptions] |
| [add more rows as needed] | | | | | |

# Appendix 8: Request for Waiver of Notice to Individual of Collection of Personal Information

**Instructions to Institution:**

Pursuant to section 39 (2) of the Freedom of Information and Protection of Privacy Act (FIPPA) and section 29 (3) (b) of the Municipal Freedom of Information and Privacy Act institutions may request a waiver of notice to individual of collection of personal information.

Complete the following form and attach any relevant background material and submit your request for waiver to the Information, Privacy and Archives Division of the Ministry of Government and Consumer Services by email to Web.Foi.MGCS@ontario.ca.

1. Institution: **[Insert Name of Institution]**

2. Description of information to be collected: **[Describe personal information to be collected.]**

3. Authority for collection: **[Describe legal authority for collection of personal information.]**

4. Manner of collection: **[e.g.: directly from the individual to whom the information relates for indirectly. If the collection is indirect, indicate the authority to do so.]**

5. Anticipated number of individuals in respect of whom waiver is sought: **[Insert anticipated number of individuals.]**

6: Use of personal information collected: **[Describe the purpose for collection and include any FIPPA/MFIPPA section authorizing additional uses or disclosure.]**

7. Personal Information Bank: **[Is personal information maintained in a personal information bank and is this described in the Directory of Records.]**

8. Reason for Waiver: **[Identify reason for waiver from list below.]**

- 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)

9. Explain why notification cannot be given: **[Give detailed explanation.]**

10. Other material attached: **[List additional material provided with this application.]**

Date: **[Insert date]**

Head of Institution: **[Insert name and signature of the Head of the Institution for the purposes of FIPPA or MFIPPA.]**