Improving Access and Privacy with Records and Information Management

November 2016

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

The IPC gratefully acknowledges the contributions of staff at the City of Toronto and the Ontario Ministry of Government and Consumer Services, whose suggestions and insights have greatly informed this paper.

CONTENTS

Where RIM Meets Access and Privacy 1

Basic RIM Concepts 1

Understanding Records 1

The Information Lifecycle 2

RIM Best Practices 3

Review and Understand Your Institution's Requirements 3

Develop File Classifications and Safeguards 4

Design With Access and Privacy in Mind 5

Designate Staff as Record Custodians 6

Develop and Implement Retention Schedules 7

Keep Up With Retention Schedules 7

Transitory Records 8

Email Management 9

Storage of Electronic Records 10

File Naming 11

Entry and Exit Protocols 11

Create a Duty to Document 12

Ongoing Training 13

Review and Audit 13

Conclusion 13

Developing and implementing effective records and information management (RIM) practices and policies are key to compliance with the ***Freedom of Information and Protection of Privacy Act*** *(FIPPA)* and the ***Municipal Freedom of Information and Protection of Privacy Act*** *(MFIPPA)* or the acts. The Office of the Information and Privacy Commissioner of Ontario (IPC) is issuing this guidance document to assist institutions and their staff in understanding the direct relationship between good RIM practices and institutions' ability to meet their responsibilities under the acts. This guidance will also provide heads of institutions with a basic understanding of RIM principles and best practices to facilitate conversations with information management professionals and staff.

WHERE RIM MEETS ACCESS AND PRIVACY

When a member of the public submits an access request, institutions must respond thoroughly and within the required time frame. Your institution's ability to do this, however, may be facilitated or hindered by its information management practices. By implementing strong RIM practices, you can prevent records from being lost or inappropriately deleted, reduce search times and fees associated with finding mishandled information and reduce the risk of privacy breaches. Poor RIM practices can negatively impact your ability to:

- respond to requests
- be transparent and accountable
- implement and maintain Open Data and Open Information programs
- ensure confidentiality and privacy of personal information

Our experience has shown that staff that process requests under the acts face situations where they are unable to locate responsive records or are burdened with extensive search times that return multiple copies of the same record or unresponsive records. In a number of recent appeals and orders, the IPC has found that institutions charged excessive fees or failed to conduct reasonable searches as a result of poor RIM practices.[1] In the special investigative report ***Deleting Accountability: Record Management Practices of Political Staff***, we found that email records had been inappropriately deleted under the misconception that emails did not qualify as records that needed to be retained. In each of these cases, a significant misunderstanding of or a failure to apply good RIM practices directly impacted an institution's ability to meet its obligations under the acts.

BASIC RIM CONCEPTS

UNDERSTANDING RECORDS

For the purposes of this paper, we will use the term 'record' as defined, in part, in section 2(1) of the acts:

1 See, for example, **PO-2964-I**, **PO-2423**, **MO-2959**, **PO-3177**, **MO-2733**

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

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

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

Records can be emails, visual representations such as photographs, illustrations or maps, audio or video recordings, and data in any form. Consequently, RIM practices must address records in all of their potential forms and media.

A challenge of introducing RIM practices in an institution is ensuring that staff understand the breadth of the term 'record.' Staff that deal solely with data, electronic files or other formats of materials must deal with their records in a similarly regimented way as staff dealing with traditional paper files.

THE INFORMATION LIFECYCLE

The 'information lifecycle' refers to the various stages that records go through from their creation or acquisition to their final destruction or archiving. It is important to remember that access and privacy laws apply to records at any stage of their lifecycle. As a result, it is necessary to ensure that your RIM practices address each stage to protect and preserve valuable information. Briefly, the information lifecycle is:

1. **Creation and collection:** This is the birth of a record. At this stage, a record is either created or collected. This can include a number of different types of records, such as drafts, research materials, final versions of documents, data or analytics.

2. **Use and Maintenance:** Once a record has been created or collected, it enters this stage. Here, the record may be actively used in any number of ways, such as publishing it or using it as a reference. Maintenance at this stage refers to the editing and updating that may occur to a record.

3. **Disposition:** When a record is no longer useful, it will either be retained permanently (archived) or destroyed. The decision to archive or destroy will be based on the applicable records retention schedule.

   Generally speaking, records with a shorter term value will be saved for a defined period of time before being destroyed, while records that have long-term value will

be archived. Records that are deemed to be of no lasting value, such as transitory records, will be destroyed.

The method of destruction will vary depending on the sensitivity of the information contained within the record. For example, a publically available newsletter may simply be recycled, whereas a document containing personal information would require secure destruction. The IPC has a number of resources providing additional information on secure destruction.[2]

RIM BEST PRACTICES

The following RIM practices are commonly accepted best practices but are not exhaustive. The intention of this section is to provide institutions with a high-level overview, rather than a detailed description of how to implement different RIM practices.

It must also be noted that no single approach will be appropriate for every institution. Some of these practices will need to be modified to meet specific needs, and some may not be appropriate at all.

The IPC highly recommends that you work closely with your institution's RIM staff in the development of practices that meet your institution's unique needs and situation. If your institution does not have dedicated RIM staff, consider designating a team or engaging with external consultants to investigate these options and develop an implementation plan.

REVIEW AND UNDERSTAND YOUR INSTITUTION'S REQUIREMENTS

Review all existing legal, policy and other requirements before developing and implementing RIM practices.

It is important to fully understand the recordkeeping rules that currently apply to your institution. For example, the ministries and designated agencies, boards and commissions of the Ontario Public Service (OPS) are required to meet the obligations of the ***Archives and Recordkeeping Act***, *2006* (*ARA*), and records retention schedules approved under that law. Many municipal institutions have by-laws that address records retention or management. Your institution may have additional requirements set out in policies or procedures that you will need to consider.

2 Fact Sheet #10 - Secure Destruction of Personal Information: **https://www.ipc.on.ca/wp-content/uploads/Resources/fact-10-e.pdf**

Get rid of it Securely to keep it Private - Best Practices for the Secure Destruction of Personal Health Information: **https://www.ipc.on.ca/wp-content/uploads/Resources/naid.pdf**

Practices No. 26: Safe and Secure Disposal Procedures for Municipal Institutions: **https://www.ipc.on.ca/wp-content/uploads/2016/08/Practices-No.-26-Safe-and-Secure-Disposal-Procedures-for-Municipal-Institutions.pdf**

Under *FIPPA* and *MFIPPA*, institutions must preserve records in accordance with the recordkeeping requirements established by their institution.[3] The acts also require that institutions retain personal information that has been used in order to allow people to access their personal information.[4]

In consultation with your legal and RIM staff, review all existing requirements and how they have been implemented within your institution, before considering new plans and RIM activities.

DEVELOP FILE CLASSIFICATIONS AND SAFEGUARDS

> **Classify files according to the sensitivity of their contents and apply safeguards to protect the records.**

The information maintained within records will vary significantly, and as a result, not all records require the same degree of protection. For example, consider personal information, which is defined by the acts as any information that is about an identifiable individual, and must be protected from unauthorized collection, use or disclosure. As a result of the requirements to protect personal information, records that contain such information may require greater safeguards than others.

Personal information, however, is only one form of information that may require special measures. Your institution may maintain records that are sensitive for other reasons. Consider, for example, law enforcement records that form part of an active investigation. The disclosure of this information may impede an investigation. Another example is location information for species at risk. The disclosure of this information could result in harm to an endangered species.

In order to effectively protect sensitive information, your institution must know where that information is held, who may access it and under what circumstances. You can start by developing sensitivity classifications for your records and assign appropriate safeguards for each sensitivity level. For example, the OPS has developed a system called the Information Security and Privacy Classification, which allows staff to apply a security level to each record.[5] The required safeguards for protecting records are then based on the security level of the individual record.

---

3 *FIPPA* 10.1 and *MFIPPA* 4.1. For further information, see ***New Recordkeeping Amendments in FIPPA and MFIPPA***

4 *FIPPA* 40(1) and *MFIPPA* 30(1)

5 For additional examples of information security classifications, see: British Columbia's Information Security Classification Framework: **http://www.cio.gov.bc.ca/cio/informationsecurity/classification/information_security_classification_framework.page**

Alberta's Information Security Classification: **http://www.im.gov.ab.ca/documents/publications/InfoSecurityClassification.pdf**

University of Western Ontario's Data Classification Standards: **https://security.uwo.ca/information_governance/standards/data_classification/index.html**

When implementing a classification, it is essential to develop accompanying safeguard requirements. Records that contain personal or other sensitive information require a number of security controls:

- **Administrative:** policies that reflect who is permitted access to sensitive records and what they may or may not do with that information. For example, information that is highly sensitive may only be viewed by specific individuals who need the information to conduct their work. Alternatively, information that is deemed non-sensitive may be accessed and used broadly.
- **Technical:** access controls that can be built into information systems. Some examples of technical access controls are password protection, encryption and secured shared drives.
- **Physical:** physical controls that can be implemented to protect records. These controls may be as simple as maintaining locks on file cabinets containing sensitive information, or more complex measures, such as key card access to specific locations within your office.

In addition to applying classifications and safeguards to your files, consider data minimization at all stages of personal or sensitive information handling. Data minimization refers to the practice of limiting the collection, use or disclosure of personal or sensitive information to only what is necessary. This practice can greatly assist institutions when responding to access requests. Where possible, your institution should avoid the unnecessary collection of any sensitive or personal information.

However, if it is necessary to collect or create records containing sensitive or personal information, design your records to ensure the specific information is easy to remove. For example, where feasible and appropriate, application forms that collect personal information should segregate personal information to one section of the form. Sensitive or personal data in databases can be kept in separate tables from other data, or documents that include personal information can keep that information to an appendix or separate section. This will make it easy to redact information should it be exempt from disclosure under the acts. This approach can be applied to any record containing personal or sensitive information.

DESIGN WITH ACCESS AND PRIVACY IN MIND

> **When building or acquiring new technologies, ensure that they are capable of meeting your access and privacy obligations.**

When institutions commission, acquire or build new technologies that can be used to manage information, it is essential that these tools be capable of functions that support access and privacy obligations under the acts. For example, databases that contain personal information must be capable of allowing users to access and correct that information to enable compliance with the acts. When a system is not capable of simple extraction, the costs associated with an

access or correction request may ultimately come at the expense of the institution. Likewise, the lack of extraction capability could prevent the appropriate destruction or archiving of records, leading to potential privacy and access issues.

Failure to address access and privacy issues at the system design stage may result in greater costs, in both time and resources. Information technology professionals, as well as procurement professionals involved in the acquisition of information technologies, must understand the RIM, access and privacy requirements for any new system.

DESIGNATE STAFF AS RECORD CUSTODIANS

> **Assign responsibility for maintaining specific records. Ensure that responsibility is transferred should designated staff members leave or organizational changes result in responsibilities changing hands.**

In large offices where many staff perform a variety of functions, it can be challenging to determine who is responsible for individual records. This challenge may grow over time, as staff change positions or leave institutions. This can become especially problematic when access requests are received. If records have been abandoned, it can be extremely difficult for staff to identify the appropriate individuals and offices to conduct a search. Designating staff as record custodians can help address this issue.

A record custodian is an individual or group that is responsible for maintaining specific records or types of records. Depending on the nature of the records and the size of the organization, a record custodian may be an individual, a work unit, or even a large branch. However, it is a best practice to identify a specific position or group that is most familiar with the records to be responsible for carrying out maintenance actions and responding to requests regarding the records.

When a record custodian has been identified, document the designation and make the document accessible to others in the institution that may need to know. This can be done in a number of ways, depending on the types of records. For example, consider using metadata. Metadata is descriptive information about a data set or record which can easily include contact information for the responsible record custodian. For some types of records, it may be appropriate to designate record custodians in job descriptions, file plan documentation or simply as a note on a shared drive. It is important to remember to keep this information up to date, changing designations and contact information as necessary. The key point in designating record custodians is to ensure that records are appropriately managed and maintained over time to prevent records from being mishandled, lost or forgotten.

DEVELOP AND IMPLEMENT RETENTION SCHEDULES

> **Develop specific retention schedules for all records in your institution.**

Records retention schedules outline the length of time records must be kept by an institution and what the ultimate disposition of those records will be after that time has elapsed. Generally, records retention schedules contain the following:

- A description of the records, including volume and format.
- The length of time that the records are to be retained by an institution.
- The length of time records may need to be retained in offsite storage.
- A decision as to whether they will be transferred to an archive or destroyed at the end of this retention period.

These schedules are an essential component of any RIM strategy and must form part of the policies and procedures used to implement that strategy. Many institutions, such as the OPS, have records retention schedules in place. For institutions that do not yet have them, they will need to be developed in order to maintain compliance with the acts.[6]

To begin, conduct an inventory of your institution's records to understand and document the full array of records created or collected by your institution. Once this has been completed, RIM and subject matter experts must work together to determine how long the record is needed by the institution. The ultimate disposition of the record, that is, whether it will be destroyed or archived, must then be decided. For institutions governed by the *ARA*, this decision will be made by the **Archivist of Ontario**. For other institutions, this decision will need to be made in consultation with RIM experts, librarians, archivists and/or subject matter experts, as appropriate.

KEEP UP WITH RETENTION SCHEDULES

> **Assign staff to conduct regular reviews to ensure that records are destroyed or archived in accordance with your retention schedules.**

Establishing records retention schedules is an excellent first step in developing a RIM strategy, but in order to be fully effective, the schedules must be implemented and followed. As a starting point, train all staff on how to apply retention schedules to their records. This is

6 For more information on the recordkeeping amendments to *FIPPA/MFIPPA*, see ***New Recordkeeping Amendments in FIPPA and MFIPPA***

particularly important for record custodians, who will be responsible for maintaining the records and ensuring that they are appropriately handled at the end of their lifecycle.

Once implemented, staff will need to periodically review holdings to find records that have exceeded their retention period. These records, if no longer useful on site, must be archived or destroyed in accordance with the applicable records retention schedule.

The following tips can help your institution keep up with retention schedules and ensure that records are destroyed or archived appropriately:

1. Document retention dates and disposition on or with the record. This will allow record custodians to quickly see which records have exceeded their retention period and what the next step will be. This information can be held within a metadata record, a separate note to file or a sticker on a paper document.
2. When large volumes of records are meeting their retention period at the same time, schedule reminders for staff.
3. Schedule regular record clean-up. This could be a large annual event or a smaller weekly task. Determine what kind of schedule works best and ensure that you keep up with the required schedule.

Remember that records may be responsive to access requests as long as they are in the custody or control of your institution. When staff are conducting reviews, it is important to remember that any records that are responsive to a request or subject to a litigation hold must not be destroyed. Ensure that staff consult with your institution's legal and access to information departments before destroying records.

TRANSITORY RECORDS

Develop clear guidance on what constitutes a transitory record and ensure that all staff can identify and handle transitory records appropriately.

Institutions create and collect a large variety of records, but not all of these records have ongoing value. Consider, for example, emails or posters about internal social events, or multiple copies of a report. While these records serve a short term purpose, such as informing staff of a bake sale, or distributing copies of a report to many people, they do not serve any significant business purpose to the institution or to the public. Records such as these are called 'transitory' and they have their own records retention schedule that allows them to be destroyed.[7]

7 For example, see the OPS' Common Record Series for transitory records: **http://www.archives.gov.on.ca/en/recordkeeping/documents/Transitory-Records-Common.pdf**

In developing and implementing RIM practices, it is vital that institutions clearly define the difference between transitory records and business records and establish protocols for deleting transitory records. When an access request is received, staff may need to search through a multitude of record holdings. This task can be made significantly easier if transitory records are destroyed appropriately.

The following considerations can help your institution define transitory records:

1. Was the record produced by your institution? If the record is a research resource, or copy of a published paper, it may not need to be kept after it is no longer useful.
2. Does the record document your institution's business? If the record contains information pertaining to your work, it is more likely to be a record that should be kept. If, however, the record pertains to internal social events, or external news clippings, it may not have a lasting value.
3. Are there multiple copies of the same record? It is important to save the official copy of a record, but duplicates may not be needed.

It is important to remember that transitory records do not have to be destroyed. If the record is still useful, keep it. There is no requirement to destroy these records. However, it is good practice to destroy transitory records that no longer have value to reduce the amount of material being stored and the resources associated with storing and searching through unnecessary records.

EMAIL MANAGEMENT

> **Emails are not transitory by default. Develop guidance on email management that helps staff manage and protect emails appropriately.**

As described above, records can be in any format. Despite the fact that email is one of the main forms of business communication, many people see emails as inherently transitory.[8] However, business decisions, key communications, and important information are regularly shared by email, and as a result, emails must be managed as any other record in accordance with the acts.

Managing email records can be challenging, especially given the volume of emails received and sent. The following tips can help institutions and their staff organize and manage their email records:

8 The inappropriate deletion of email records has been highlighted in ***Deleting Accountability*** and the BC report ***Access Denied: Record Retention and Disposal Practices of Government of BC***.

1. Email messages that qualify as business records should be saved to shared repositories or other storage associated with the file. Consider saving messages in .PDF format rather than .MSG format, as they are more stable and difficult to alter.
2. When possible, avoid sending attachments. Rather, send hyperlinks to records in shared repositories to ensure that recipients have the most up-to-date version and to prevent potential inadvertent disclosure.
3. Create folders within your email to organize emails into relevant subjects. This can help keep inboxes manageable and may assist with workflow. Try moving emails into subject folders when the issue has been dealt with. When the file is closed, those emails will be easy to find and to move into longer term storage.
4. Keep subject lines short and clear, using consistent naming conventions when possible. This will help both you and the recipient find information and quickly identify relevant emails.

STORAGE OF ELECTRONIC RECORDS

Use storage solutions that have automatic back-up and appropriate security controls.

While records are in active use, they should be stored in a secure manner that allows for ease of access by authorized individuals. This is essential for responding to access requests as it can significantly reduce search time and resources. Shared drives, electronic records management systems or other shared storage resources are recommended, as they allow institutions to set access controls and limit access to authorized individuals. When individuals save records on their personal computers or within their email, it is easy for those records to be lost should the computer break down or individuals leave the institution.

Shared storage resources should have automatic back-up to prevent inadvertent loss of information. In addition, they should have security controls that allow only authorized individuals to access information. For example, access to a shared drive may be appropriate for members of a work unit, but not for other members of the institution. Alternatively, sensitive or personal information may require that only specific individuals or management have access.

FILE NAMING

> **Apply meaningful names to files and apply them consistently.**

File names are an important tool to help staff find information, especially in the context of an access request. However, when working on materials that are familiar to us, we tend to use vague titles. While one staff member may easily recognize what "Letter.doc" is, other staff will have to open the file to determine what the file actually is. In the context of an access request, this can result in significant search time and associated fees.

Implementing file naming conventions throughout an institution can standardize the way that staff save files and help ensure that materials can be easily searched for and accessed. File naming conventions do not need to be complicated to be effective. Rather, they should capture the minimum amount of information necessary for staff unfamiliar with the file to access it using a standard search.

Institutions will need to consider the types of information that is necessary to easily identify files, but there are a few elements that are recommended:

- date the record was prepared
- a descriptive title, for example, rather than simply naming a document "New Practices," a more descriptive title could be "RIM Practice Guidelines"
- version number as it can be easy to become confused when there are many versions of a record. Adding a version number can help ensure that staff are accessing the most current materials

ENTRY AND EXIT PROTOCOLS

> **Train staff on RIM requirements when they join the institution. Ensure that all records are appropriately stored and managed before staff leave.**

As staff move between positions and institutions, it is easy for records to be lost, mishandled or destroyed inappropriately. Developing protocols for when staff start or leave positions can help prevent the loss of valuable information, as well as protect your institution from privacy breaches.

For staff entering a new position, ensure that they are made aware of the following:

- What records their position is responsible for maintaining.
- The RIM standards in place and how to apply them.

- Any mandatory or voluntary RIM training that is available.
- How to access and use shared storage resources.
- Who the contact is for questions about RIM.

For staff exiting a position, it is important to ensure that records created or maintained during the individual's tenure are appropriately saved, securely destroyed or transferred to a replacement. Have the departing staff member verify that the following is completed prior to their last day:

- Records have been stored, transferred to an archive or destroyed based on their retention schedules.
- Personal non-work related information that may have been stored on a computer or in paper files has been destroyed.
- Email records have been appropriately saved or destroyed.
- A list of all records that the individual is responsible for maintaining has been prepared for transfer to the new record custodian.
- Passwords for protected files or storage media have been reset and transferred to the new record custodian.

Managers are responsible for ensuring that departing staff have completed all RIM requirements and should take steps to verify their completion.

CREATE A DUTY TO DOCUMENT

> **Implement policy that requires staff to keep written records of decisions about your institution's business.**

As was seen above, records can be in any format. However, in some cases, important information is conveyed without the creation of a record at all. Business or policy decisions are sometimes made in meetings, over the phone or in other settings that do not automatically create a lasting record (such as over instant messaging programs). When these decisions or actions are not recorded, institutions may not be able to meet their access and privacy requirements under *FIPPA* and *MFIPPA.* As such, institutions should develop a policy requiring staff to document business-related activities, including a duty to accurately document key decisions.

In addition, it is important to ensure that staff use appropriate communication tools for business information. In our recent paper, **Instant Messaging and Personal Email Accounts: Meeting Your Access and Privacy Obligations**, we also recommend that institutions prohibit the use of non-institutional email accounts or instant messaging tools for conducting business.

Implementing a requirement to document decisions requires the development of policy and training for staff so that they will fully understand what information should be recorded.

Consider developing templates for use in specific situations, such as meeting notes. Training on how and when to appropriately use these templates may help ease the transition for staff accustomed to making decisions in meetings or hallway conversations.

ONGOING TRAINING

> **RIM training must be available to staff regularly.**

Initial training on RIM practices is essential. It will provide your staff with a strong basis upon which to build additional knowledge and skills. However, in order for long-term practice changes to take root, the lessons must be regularly refreshed and reinforced. Invest in a training program that allows staff to re-visit training materials and help them to understand RIM concepts and implement changes in their own work. Remember that the success of your RIM program is in the hands of your staff. Make sure that they have the resources and assistance that they need.

REVIEW AND AUDIT

> **Reinforce RIM practices by regularly reviewing practices and include records management commitments in performance plans.**

Implementing strong RIM practices should be a long-term goal. Do not expect quick and easy fixes. Staff are accustomed to their own filing and RIM practices, so changing habits can take a long time. As with any change, it will take time, patience and regular reinforcement.

In order to help keep staff accountable for maintaining RIM practices, it is highly recommended that institutions include regular reviews and monitoring of RIM practices in their ongoing plans. In addition, including RIM actions and targets in annual performance plans will help keep staff engaged and accountable.

CONCLUSION

By implementing RIM best practices, institutions can vastly improve conditions for accessing information. Information that is appropriately created, managed, stored and destroyed is eminently easier to find and use. Access requests can be processed with greater ease and efficiency. Staff time associated with record searches can be significantly reduced. Risks associated with failure to provide responsive records or with failing to meet the required response timelines can be avoided. Ultimately, a comprehensive RIM plan can help institutions to be more agile, efficient and accountable to the public.

Implementing RIM policies and practices can be challenging. Institutions, departments, and individuals develop their own ways of managing their records over time, so it can be difficult to get staff engaged and willing to change ingrained habits. When preparing to develop and implement new or improved RIM practices, remember the following:

1. **Be engaged**. Senior management should understand the importance of RIM practices to the legislated obligations of the acts and actively support the efforts to introduce or update RIM practices in your institution.

2. **Communicate often.** It is essential to keep RIM practices top of mind to ensure that staff don't slip into old practices.

3. **Communicate clearly.** Communication and training on RIM should be clear and straightforward, using plenty of examples and real world scenarios so that staff can fully understand their responsibilities and how to implement new practices.

4. **Commit to maintaining practices over time.** Implementing RIM practices is not a simple one-time event. It takes time and dedication to ensure that best practices become everyday practices.

ABOUT THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

The role of the Information and Privacy Commissioner of Ontario is set out in three statutes: the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act*. The Commissioner acts independently of government to uphold and promote open government and the protection of personal privacy.

Under the three *Acts*, the Commissioner:

- **Resolves access to information appeals and complaints when government or health care practitioners and organizations refuse to grant requests for access or correction**
- **Investigates complaints with respect to personal information held by government or health care practitioners and organizations**
- **Conducts research into access and privacy issues**
- **Comments on proposed government legislation and programs**
- **Educates the public about Ontario's access and privacy laws**

Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8

Web site: **www.ipc.on.ca**
Telephone: 416-326-3333
Email: **info@ipc.on.ca**

November 2016