MAY 2024

IPC Guidance: Privacy and Access in Public Sector Contracting with Third Party Service Providers

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

This guide by the Office of the Information and Privacy Commissioner of Ontario (IPC) is intended to enhance understanding of rights and obligations under Ontario's access and privacy laws and advance best practices when engaging third party services. It should not be relied upon as a substitute for the legislation itself or as legal advice. It does not bind the IPC's Tribunal, which may be called upon to independently investigate and decide upon an individual complaint or appeal based on the specific facts and unique circumstances of a given case. For the most up-to-date version of this guide, visit **www.ipc.on.ca**.

Acknowledgement

The IPC shared a draft of this guidance with interested parties in Ontario, including from:

- provincial government
- municipalities
- education
- law enforcement
- transportation
- gaming and alcohol

The IPC appreciates the thoughtful comments of the institutions and individuals representing these sectors. Feedback and inquiries about this guidance can be sent to **info@ipc.on.ca**.

Contents

Introduction

Ontario's public institutions increasingly rely upon third party service providers to help carry out their legal mandates.[1] These service providers often process institutional records and personal information which are subject to Ontario's access and privacy laws.

Outsourcing arrangements can challenge the traditional understanding of who has custody and control of records or personal information, blurring lines of accountability. As public-private partnerships become more common, they bring new privacy and security risks. These risks must be managed in a practical and trustworthy way.

Being an accountable institution requires addressing access and privacy considerations in outsourcing arrangements and maintaining effective control over records and personal information, even when they are in the custody of third-party service providers. Regardless of who processes data on their behalf, Ontario's public institutions remain accountable for protecting privacy and providing a right of access to records and personal information under their control.

About this guidance

This guidance sets out recommended best practices for exercising due diligence and ensuring accountability for privacy and access to information when planning for and entering into agreements with service providers.

This document is intended for use by Ontario institutions subject to the *Freedom of Information and Protection of Privacy Act* (FIPPA) or the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA). However, other public sector organizations may also benefit from these best practices and adapt them as necessary.

1 Examples of third-party arrangements with government include:

- delivering a program or service on behalf of government
- establishing and/or managing a database or IT system
- providing system support
- providing disaster recovery services
- providing consulting or research services
- administering a call centre
- providing records storage
- off-site shredding or recycling of information storage media

The recommendations in this document are intended to help institutions identify access and privacy considerations when entering into agreements with service providers in compliance with FIPPA and MFIPPA. However, there is no one-size-fits-all solution. Not all recommendations relate to all initiatives, records, or agreements. Institutions will need to assess the relevant and appropriate access and privacy requirements on a case-by-case basis.

This guidance focuses on access to information and privacy responsibilities related to outsourcing of services that involve the processing of records and/or personal information. For broader procurement considerations, institutions are encouraged to use this guidance with other requirements that apply to them, including, for example, the Ontario Management Board of Cabinet **Broader Public Sector Procurement Directive** (effective April 1, 2024) and the Ontario Public Service Procurement Directive (effective September 1, 2023).

While contracts are essential to managing third party risks, contracts alone are not enough. Institutions should exercise due diligence throughout all phases of procurement. Accordingly, the recommendations in this document are organized into a five-part checklist:

- **Part 1: Procurement planning** outlines considerations when you are identifying and evaluating your business needs and planning to engage a service provider.
- **Part 2: Tendering** outlines considerations when you are developing or reviewing tendering documents, such as requests for proposals.
- **Part 3: Vendor selection** outlines considerations for access and privacy during the evaluation and award stages of the procurement process.
- **Part 4: Agreement** outlines considerations when entering into an agreement with a service provider.
- **Part 5: Agreement management and termination** outlines considerations for the duration of your agreement related to its management, monitoring, and enforcement and termination.

This guidance will serve as a starting point for discussions between the business unit responsible for the records, the privacy office, procurement services, IT personnel, cyber security staff, legal counsel, and the project management team. It is intended to provide institutions with the necessary support they need to negotiate and develop agreement terms that comply with Ontario's access and privacy laws.

We encourage institutions to adapt these recommendations as may be relevant and applicable, and incorporate them into their established procurement processes.

General principles

- Each institution covered by FIPPA or MFIPPA is responsible for complying with the access and privacy requirements defined in the legislation.[2]

2 To learn more about your freedom of information and privacy responsibilities under FIPPA or MFIPPA, contact your institution's **freedom of information and privacy coordinator**.

- Institutions may also be subject to directives, trade agreements, policies, standards, and guidelines that define additional requirements relating to the transparency of institutional records and the protection of personal information.
- FIPPA and MFIPPA do not prohibit Ontario's public service and broader public service institutions from outsourcing the processing of records and personal information, nor do they prohibit the storage of this information outside of Ontario or Canada.
- Public institutions in Ontario are expected to maintain effective control over records and personal information even when these are in the custody of service providers for processing.[3]
- When Ontario's public service and broader public sector institutions outsource the processing of records and personal information, they remain accountable for complying with Ontario's privacy laws for records and personal information under their custody or control.[4]
- Service providers acting on behalf of an institution may not process personal information beyond what the institution itself is authorized to do. For example, service providers may not use personal information for secondary purposes such as marketing or product improvement[5] without the independent consent of the individual users of their services.
- To meet their safeguarding obligations under FIPPA or MFIPPA, institutions must ensure that any service providers that process records and personal information on their behalf are held to the same or equivalent requirements expected of the institutions themselves.
- Legal contracts are a critical requirement for ensuring that service providers comply with an institution's privacy and access obligations. Institutions cannot avoid their obligations under FIPPA or MFIPPA by failing to make appropriate contractual arrangements with service providers.
- While it is necessary for institutions to have a binding agreement with service providers, that alone is not sufficient. Institutions must also have sufficient oversight measures in place to ensure that service providers comply with their obligations under the agreement.
- Institutions must also be transparent to individuals when using a service provider to collect personal information on the institution's behalf, including by providing enhanced notices of collection.

3 The IPC's 2023 Interpretation Bulletin **Custody or Control** sets out a list of factors that may be relevant in assessing custody or control. This guidance builds upon the Supreme Court of Canada's two-part test in Canada (Information Commissioner) v. Canada (Minister of National Defence), **2011 SCC 25 (CanLII), [2011] 2 SCR 306** and past IPC orders to the same effect. See also Section 2.3 of this guide, "Records and personal information to be processed".

4 Ontario Criminal Code Review Board v. Hale, **1999 CanLII 3805 (ON CA)**, paragraphs 32 and 36-37.

5 Use of personal information to develop or improve services may be inconsistent with authorized purposes. See IPC Privacy Complaint Report **PI21-00001**.

Access and privacy checklist

Part 1: Procurement planning

This section outlines considerations relevant to identifying and evaluating the business needs of the institution and planning to engage a service provider.

Before tendering or engaging a service provider, institutions must consider and plan how to meet their privacy and access obligations under FIPPA or MFIPPA. An institution should recognize the potential risks to access and privacy that may arise when records or personal information move from that institution's protected custody to a service provider for processing on the institution's behalf. Before embarking on a procurement project or initiative, institutions should consider the following best practices:

1.1 Preliminary planning

- Add or integrate this checklist into any institutional planning documents, to help identify access and privacy matters that need to be addressed when procuring third party services.
- Engage relevant experts, including freedom of information and privacy staff, legal counsel, information security staff and other experts for advice on identifying and addressing access and privacy matters that may arise from the proposed procurement project or initiative.
- Confirm that the purpose of the procurement project or initiative to be outsourced is consistent with the institution's intended business or operational requirements.
- Confirm that lawful authority exists under FIPPA or MFIPPA for any collection, retention, use or disclosure of personal information that is being proposed under the initiative.
- Define the appropriate agreement or other instrument needed to govern the planned procurement activity and the processes to be followed.
- Clearly define any process requirements to seek, obtain and document necessary approvals.

1.2 Defining the records

- Develop a clear understanding whether institutional records or personal information will be involved in the procurement project or initiative.[6]

6 Employee personal information: if the outsourcing project involves processing personal information of an institution's employees, such as a human resources initiative, the institution should apply equivalent considerations and protections as for any other sensitive personal information under its custody or control. Unauthorized use or disclosure of employee information can create safety and financial risks for employees, and security, legal and financial risks for the institution.

- Identify and define the types of records or personal information that will be covered by the agreement, including the business owner responsible for the records or personal information.
- Confirm the requirements in privacy laws, regulations, agreements, directives, operating policies, standards, and other guidance that apply to the records or personal information.
- Establish that the records or personal information to be transferred to the service provider are limited to only those that are necessary and relevant for the service provider to provide the planned service. Clearly identify the minimum amount that needs to be transferred to meet the purpose.

1.3 Identifying and mitigating privacy and security risks

- Identify the privacy and security risks associated with the project or initiative before starting the procurement process or entering into an agreement and develop appropriate measures to mitigate them. This should be done by carrying out a privacy impact assessment (PIA) and, where relevant, a threat risk assessment (TRA).
- Consider whether the service provider should also undertake a PIA or TRA or other security assessment of its services, processes, or technology before entering into the agreement and/or at defined intervals during the project development or contract period.

1.4 Defining requirements for service providers

- Define the work to be carried out by the service provider related to the processing of records or personal information under the project or initiative.
- Establish clear lines of accountability between the institution and the service provider and define their respective roles and responsibilities.
- Define specific access, privacy and security requirements and prohibitions to be imposed on the service provider.[7]
- Define a process for monitoring and evaluating the service provider's compliance with the access, privacy and security requirements, including adherence to contractual obligations and security standards.
- Define the privacy or security qualifications, credentials, or certifications the service provider or subcontractors should have before undertaking the service being contemplated.

7 Defining specific privacy rules and responsibilities in your agreement provides greater clarity than a simple requirement to comply with legislation. This is particularly true when Ontario legislation would not usually apply to the service provider. Service providers may not be familiar with Ontario's access and privacy laws or understand how their provisions may apply in the context of the agreement. In such cases, defining the specific privacy protection requirements in your agreements may be necessary.

- Seek information on the service provider's corporate governance structures, such as where they carry out their data processing activities, and affiliations with foreign entities, and consider whether these raise any legal conflicts or other obstacles to fulfilling its contractual obligations.

1.5 Defining methods of evaluation

- Define how to assess and evaluate the prospective service provider's capacity to comply with the access, privacy, and security requirements, and what documentation will be required to support that assessment.[8]
- Consider the need for an on-site visit or inspection, preliminary assessment, compliance certification, or other means necessary to evaluate the prospective service provider's capacities.

Part 2: Tendering

This section outlines relevant access, privacy and security considerations when developing or reviewing tendering documents.

Building on the planning activities above, when institutions engage a service provider to process records or personal information on their behalf, they should define appropriate access, privacy and security responsibilities and prohibitions in their tendering documents and eventual agreement. These documents should define the rules related to the management of records and protection of personal information. Accordingly, institutions should proceed as follows:

2.1 Legislative framework

- Clearly define what privacy legislation or other relevant laws apply to the service provider's processing activities and where more than one law applies, how the requirements of Ontario's privacy laws will be met.

2.2 Compliance requirements

- Require the service provider to comply with the terms and conditions of the agreement and any applicable laws and regulations related to privacy and access to personal information.

8 For example, providing evidence of an information security management system meeting **ISO 27001** standards, or the American Institute of Chartered Public Accountants (AICPA) Statement of Controls (SOC) **SOC 2 Type II reports**. These are intended to provide detailed information and assurance about the controls at a service organization relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems. These reports can play an important role in oversight of the organization, vendor management programs and regulatory oversight.

- Require the service provider to limit the processing of records and personal information to only the purposes set out in the agreement.
- Prohibit any other activities involving records and personal information without obtaining prior written approval by the institution.
- Require the service provider to ensure that its employees, agents, and other representatives who will have access to the records or personal information comply with applicable legislation and the terms and conditions of the agreement.
- Determine whether criminal record checks are needed for persons with access to records or personal information and, if so, require the service provider to ensure these checks are conducted prior to allowing access to the records or personal information.
- Specify whether the service provider is permitted to use subcontractors to undertake work under the agreement. If so, require the service provider to identify the subcontractor(s) and ensure that the subcontractor(s) will be held to the same or equivalent standards as the service provider, as may be relevant.[9]
- Set out the governing law for interpreting and enforcing the agreement (for example, the law of Ontario) and the court or other forum in which disputes under the agreement will be resolved (for example, the Superior Court of Justice (Ontario)).

2.3 Records and personal information to be processed

- Define the terms "record" and "personal information" to ensure a common understanding among all parties to the agreement (for example, as defined by FIPPA and MFIPPA).
- Define the types of records and personal information the service provider will have access to and be responsible for processing, building upon Section 1.2 of this guide, "Defining the records."
- Define which records and personal information will be in the custody of each party under the terms of the agreement.
- Explicitly provide that any records and personal information transferred to or collected by the service provider for processing on behalf of the institution remain under the institution's control.
- Determine which activities or services, if any, must only be undertaken with de-identified or anonymized data and define the meaning of these terms.[10]
- If personal information is required to perform the processing activities, define the minimum amount necessary to perform them.

9 If your service provider is permitted to use subcontractors, then you will need to determine which elements of this checklist also apply to subcontractors, and how subcontractors' obligations to protect access and privacy are defined in your agreement.

10 For information to be considered "de-identified", details that either (i) directly identify an individual, or (ii) could be used, either alone or with other information, to identify an individual, must be removed.

2.4 Requests for access to records and personal information in service provider's custody

- Define which officials at the institution and the service provider will be designated as responsible for communications about requests for records or personal information in the service provider's custody.
- Define the service provider's responsibility to notify designated contacts at the institution whenever it receives formal or informal access requests for records or personal information in its custody.
- If the service provider receives an access request directly from the public, require the service provider to promptly advise the requester that any access request must be made in writing directly to the institution.[11]
- If the service provider receives an access request from law enforcement, require the service provider to promptly notify designated contacts at the institution of the request, refuse to provide access in the absence of a warrant, and direct law enforcement to make its request directly to the institution.

2.5 Collection of personal information by the service provider

- Define the service provider's responsibilities and prohibitions in respect of the collection of personal information, including:
    - Define the authority of the service provider to collect the personal information on behalf of the institution.
    - Limit the purposes for which personal information is to be collected by the service provider under the terms of the agreement.
    - Specify the personal information the service provider may collect,[12] and limit the permitted data elements to only those necessary to perform the activities defined in the agreement.
    - Specify the manner of collection (i.e., direct or indirect collection). If the collection is indirect, ensure that it is properly authorized.[13]
    - Require the appropriate notices of collection.[14]

11 Under FIPPA and MFIPPA's access procedures, requests for information under the custody or control of an institution must be made directly to the institution. Note that FIPPA, s 62(1) / MFIPPA, s. 49(1) do not permit institutions to delegate this authority to a service provider.

12 Note that collection also includes creation of new personal information by the service provider in undertaking its contracted activities. One example would be a service provider conducting analytics on individuals' personal information in a database, then creating and assigning the individuals to newly defined categories based on the analysis.

13 FIPPA, s 39(1) / MFIPPA, s 29(1).

14 In most circumstances this will involve reproducing the institution's notice of collection and pointing to where the notice can be found on the institution's website. Strictly speaking, the head of an institution may not delegate authority to the service provider to provide notices of collection: FIPPA, s 62(1) / MFIPPA 49(1).

2.6 Use and retention of records or personal information by the service provider

- Define the service provider's responsibilities and prohibitions related to the use and retention of records or personal information in its custody, including:
    - Define the service provider's retention responsibilities (such as following a defined retention schedule, returning or securely destroying records and personal information).
    - Prohibit the service provider from deleting or altering records and personal information, except as directed by the agreement or with prior written permission.
    - Define the service provider's responsibilities and prohibitions for managing backup copies of records and personal information.
- Where it is personal information being processed, further define the service provider's use and retention responsibilities and prohibitions, including:
    - Limit the permitted purposes for which the personal information may be used.
    - Require the service provider to take reasonable steps to ensure the personal information in its custody is accurately recorded, complete, and updated as necessary for its purpose.
    - Define the service provider's responsibilities related to the correction[15] of personal information at the request of the institution, including tracking disclosures of personal information to enable notification of correction or statement of disagreement.[16]

2.7 Disclosure of personal information by the service provider

- Define the service provider's responsibilities and prohibitions related to the disclosure of personal information in its custody, including:

15 This is the institution's responsibility. Under FIPPA, s 47 / MFIPPA, s 36, the right of correction or disagreement occurs only if a requester is given access in response to an access request.

16 As outlined in FIPPA, s 47(2)(c) / MFIPPA, s 36(2)(c)

- Define the service provider's confidentiality obligations.[17]
- Limit the purposes for which personal information may be transferred or disclosed to another party under the terms of the agreement, specifying to whom, and under what conditions, namely:
  - the purposes for which the other party may use or further disclose the personal information
  - how the personal information must be protected and disposed of
  - how the personal information-sharing activities will be monitored and enforced.
- Prohibit disclosure of personal information for any purposes not contemplated by the agreement.
- Require the service provider to de-identify personal information in defined circumstances (for example, before disclosure to certain parties) and specify what is understood by "de-identify."
- Require the service provider to immediately notify designated contacts at the institution of any request for disclosure of personal information for a purpose not authorized by the agreement.
- Require the service provider to immediately notify designated contacts at the institution of any unauthorized disclosure of personal information, in accordance with the agreement's privacy breach and complaint obligations.

2.8 Service provider's safeguarding obligations

- Define the minimum requirements for the service provider's privacy and security programs, including the name and contact information for the service provider's executive responsible for privacy and security, privacy and security policies and practices, and privacy and security training for employees and subcontractors.
- Define access controls for the records or personal information in the custody of the service provider, including restrictions on who may access personal information and for what purpose.

17 In Privacy Investigation Report **PC12-39**, the IPC reviewed the Ministry of Natural Resources' Licensing Automation System and noted that the ministry's contract had "robust provisions that protect the personal information under its control and restrict the use of that information by the Agent" including a confidentiality provision that defined confidential information to include "all personal information that the ministry is obliged, or has the discretion not to disclose under provincial or federal legislation or otherwise at law." The agent's contractual obligations for this information included:

- Keeping the information confidential and secure.
- Limiting the disclosure of confidential information to only those who have a need to know it for the purpose of the contract and who have been specifically authorized to receive such information.
- Not directly or indirectly disclosing, destroying, exploiting, or using any confidential information (except for the purpose of the contract, or except if required by order of a court or tribunal), without first obtaining the written consent of the ministry and in respect of any of the ministry's confidential information about any third party, the written consent of such third party.
- Not selling personal information without the consent of the ministry and relevant third party.

- Require the service provider to effectively secure records and personal information, whether hardcopy or electronic, at rest and in transit, including reasonable physical, technical, and administrative measures, commensurate with the sensitivity of the information, in order to prevent unauthorized access, use or disclosure, loss or theft, alteration, copying, damage, destruction or intermingling with other records.
- Define requirements to:
    - Monitor and audit access controls, including an audit trail to confirm access only by authorized parties.
    - Maintain up-to-date software applications, including security patches.
    - Test and verify security measures.
    - Provide documentation about the security program.
    - Monitor compliance with the agreement and any audit recommendations.
- Require the service provider to segregate personal information related to the agreement from other information in their custody.
- Define the service provider's responsibilities and prohibitions related to the location and movement of records and personal information, including backups.
- Define the service provider's and subcontractor's disaster recovery and business continuity requirements related to records and personal information in their custody.

2.9 Obligations in the event of a privacy breach or complaint

- Define what constitutes a privacy breach.
- Define the service provider's responsibilities to:
    - contain and assess the breach
    - immediately report the breach to designated contacts at the institution
    - report the breach to any regulators or other relevant parties as soon as reasonably feasible, or in accordance with any statutory timelines, format, and other requirements that may apply
    - communicate with the institution to coordinate who will notify the affected parties, as well as when and how
    - investigate the cause of the breach in cooperation with the institution and provide the institution with the outcomes of its investigation on a timely basis
    - take corrective or remedial action to prevent further breaches
- Set out the service provider's obligations to:
    - assume responsibility for any negligent or willful act or omission that caused the breach
    - compensate the institution for any damages in connection with a breach
    - pay or compensate for any costs incurred because of the breach (for example, notifying affected individuals)

- Require the service provider to manage questions and complaints about its privacy practices related to the personal information in its custody.
- Require the service provider to immediately notify designated contacts at the institution when it receives a complaint that could relate to the institution's obligations under FIPPA or MFIPPA, or other applicable legislation.

2.10 Monitoring the service provider's compliance with the agreement

- Define how access, privacy and security protections will be monitored to ensure the service provider's compliance with the agreement, including how and when compliance verification or audits should be done (such as on-site visits or inspections by the institution itself, or independent verification by an agreed-upon third party).
- Specify the reporting requirements and related documentation the service provider must provide to demonstrate its compliance with security and privacy policies and procedures, privacy and security audits, and other related privacy and security certifications.
- Require the service provider to provide prior notice of significant changes to security, privacy, business processes or sub-contracted work or services that could impact the service provider's obligations under the agreement, including but not limited to its ability to comply with those obligations.
- Define the service provider's responsibilities related to PIAs in the event of significant changes during the agreement period, including when a PIA is necessary and who will undertake the PIA (the institution, the service provider, or another designated party).
- Define the liabilities for violation of the agreement terms by the service provider, its employees, agents, other representatives, and subcontractors, including for any negligent or willful act or omission related to unauthorized collection, use, disclosure, retention, security, or disposal of records and personal information.
- Define the service provider's responsibility to notify the institution in the event of any change in ownership or control of all or part of the service provider's business and any proceedings for bankruptcy or insolvency brought by or against the service provider.
- Define requirements for the service provider to cooperate with and assist in any investigation related to compliance with the terms of the service agreement.
- Define requirements for the service provider to promptly facilitate the institution's compliance with IPC orders related to access to records or protection of personal information in the service provider's custody.
- Draw the service provider's attention to the offence provisions under FIPPA or MFIPPA.

Part 3: Vendor selection

This section outlines considerations relevant to access and privacy during the evaluation and awarding stages of the procurement process.

It is your institution's responsibility to select a service provider that has the capacity to comply with the terms and conditions of the agreement and other applicable requirements.

To accomplish this, your institution should:

- Vet potential service providers to determine that they both understand and can meet defined access and privacy requirements.
- Ensure someone with sufficient knowledge of access, privacy and security, including the terms and conditions defined in the procurement documents, is involved in the evaluation process, and is available to address issues and answer questions.
- Ensure that all appropriate documentation related to access, privacy and security requirements is submitted by prospective service providers before selection.
- Undertake any activities required to collect sufficient information to evaluate service providers (such as site visits or interviews).
- Ensure the access, privacy and security components of the evaluation are assigned appropriate criteria and weighting relative to the sensitivity, scope and scale of personal information that will be processed.
- Ensure the access, privacy and security components of the selection process receive thorough evaluation by subject-matter experts, based on the assigned criteria.
- Ensure that prospective service providers know that records they submit or share as part of the procurement process are subject to the freedom of information provisions of FIPPA or MFIPPA, and communicate that to them throughout the evaluation process.

Part 4: Agreement

This section outlines considerations related to establishing a contract arrangement with the service provider.

The service agreement should reflect the scope and deliverables of the procurement and cover all the requirements regarding access, privacy and security that were defined in your tendering documents.

Institutions are expected to have reasonable contractual and oversight measures in place to ensure access, privacy and security of the records and personal information under their control.[18]

18 In accordance with requirements set out in: FIPPA O Reg 460, s 4 and O Reg 459, ss 4 and 5; and MFIPPA O Reg 823, s 3.

The contractual provisions that may be necessary and relevant for ensuring that all reasonable steps are taken to protect the privacy and security of personal information under the institution's control include:[19]

- Ownership of data: The contract should establish that all records and personal information under the agreement belong exclusively to the institution.
- Confidential information: The contract should define confidential information to include all personal information that the institution is obliged to protect under provincial or federal legislation or otherwise at law, and the service provider should be required to keep such information confidential and secure and limit access to only those who have a need to know it for the purpose of performing their duties under the contract and who have been specifically authorized to receive the information.
- Collection, use, and disclosure: The contract should state that the service provider cannot directly or indirectly use, collect or disclose any records or personal information for any purposes not authorized by the institution. Unless the service provider obtains specific, written pre-authorization from the institution, any access to or use of the institution's property, technology or information that is not necessary for the performance of its contractual obligations with the institution should be prohibited.
- Notice of compelled disclosure: The contract should state that if the service provider is legally compelled to disclose any of the institution's confidential information, the service provider must provide the institution with prompt notice to allow the institution to seek a protective order or other appropriate remedy to prevent or limit such disclosure. Further, the service provider should disclose only that portion of the confidential information which the service provider is legally compelled to disclose.
- Subcontracting: The contract should state that the service provider is not permitted to subcontract the whole or any part of the contract without the prior written agreement of the institution. If the institution agrees to the service provider's subcontracting certain services, the subcontractor should be identified and contractually bound to the same or equivalent contractual obligations that were imposed on the service provider.
- Security: The contract should state that the service provider must ensure the security and integrity of all records and personal information in its custody. The service provider must keep the personal information and records in a secure and separate location, safe from loss, alteration, destruction or intermingling with other records and databases. Further, it must implement, and maintain the reasonable physical, administrative and technological measures and procedures to safeguard the information.

19 The basis for these contract provisions is IPC Privacy Complaint Report **PR16-40**. The report enumerated the contractual provisions that may be relevant to assessing whether an institution has met its obligations to ensure that all reasonable steps were taken to protect the privacy and security of personal information under its control. Similar contract provisions have served as an assessment framework the IPC has applied in investigations involving third party service providers. See, for example, **MC18-48**, **MC17-52**, **MC18-17**, and **PI21-00001**.

- Audits: The contract should state that the service provider will comply with annual audits for privacy and security compliance, for the duration of the contract. The agreement should specify who will conduct such audits, when and how. These audits may include reviews of PIAs, TRAs and other vulnerability assessments.
- Retention and destruction: The contract should state that the service provider must return all the institution's confidential information to the institution at or before the end of the term of the contract, with no copy or portion kept by the service provider. The contract should also establish a retention and destruction schedule for the service provider.

Note that these recommended contract provisions are neither authoritative nor exhaustive. You will need to consult with relevant experts at your institution (identified in Section 1.1 of this guide, "Preliminary planning"), including your legal counsel, to assess whether all reasonable steps have been taken to protect the records or personal information that are covered by the agreement in question.

Part 5: Agreement management and termination

This section outlines considerations for the duration of the agreement related to its management, monitoring, and enforcement of access, privacy and security requirements.

Consistent with defined policies, your institution should take specific action(s), including follow-ups as necessary to monitor service providers' performance to ensure compliance with requirements and prohibitions defined in the agreement, including:

- Establishing that the agreement or contract itself is covered by the access to information provisions of FIPPA or MFIPPA, subject to applicable exemptions.[20]
- Monitoring the service provider's performance against defined terms and conditions in the agreement.
- Ensuring the service provider meets defined requirements and processes in a timely and appropriate manner (training, confidentiality undertakings, reporting, privacy breach responses, etc.)
- Ensuring required assessments, evaluation, and agreement management activities (such as audits, PIAs or inspections) are undertaken by the institution or other designated party on a timely basis.
- Assessing the service provider's performance to determine whether corrective or preventive actions are needed and, if so, requiring the service provider to take these actions.
- Making sure that access, privacy, and security risks are being reported by the service provider in a timely manner, and that appropriate risk response plans are being executed.

20 See the IPC's 2024 **Third Party Information** Interpretation Bulletin.

- Enforcing contractual terms by taking appropriate remedial steps, including contract termination, in the event of a breach of contract by the service provider involving access, privacy or security violations.
- Ensuring appropriate delegation of these institutional roles and responsibilities, with adequate training and resources, to effectively carry out these monitoring actions for the duration of the contract or agreement with the service provider.

At the completion or termination of the contract term, institutions should:

- Define what actions related to the close-out or termination of the agreement (for example, return of records or secure disposal, including backups) will be undertaken and what required documentation must be received (for example, certificate of destruction).
- Identify and document the lessons learned related to access, privacy and security aspects of the agreement. This work can help inform the development, implementation, oversight or closing out of future agreements with the same service provider or other service providers.

Glossary

Agreement

"Agreement" for the purposes of this guidance means a contract, memorandum of understanding, service level agreement or other legal instrument between an institution and a service provider that processes records or personal information on behalf of the institution.

Business owner

"Business owner" means any program director or equivalent having authority and accountability under legislation, regulation, policy or other instrument for designated business activities of the institution and the business records relating to those activities. The business owner is accountable for complying with FIPPA or MFIPPA.

Control

"Control" over a record or personal information means being accountable for it, including ensuring the protection of privacy, and being able to make decisions about how it is to be managed. Regardless of who has been assigned custody of a record or personal information, it is considered to be under an institution's control when the institution has the duty and authority to manage it, including restricting, regulating, and administering its use, disclosure, or disposition.

Custody

"Custody" refers to having physical possession of a record or personal information. Custody does not equate to control. A service provider may have custody of a record or personal information, but it does not have control. In the context of an agreement with a service provider, control and responsibility for a record or personal information collected on behalf of an institution must be retained by the institution, even though it is processed or stored by a service provider.

Institution

An "institution" under FIPPA includes all ministries and any agency, board, commission, corporation, or other body designated in the regulations (FIPPA, s 2(1)).

An "institution" under MFIPPA includes municipalities, schools, police services, and any agency, board, commission, corporation, or other body designated as an institution in the regulations (MFIPPA, s 2(1)).

Outsourcing

"Outsourcing" is a means of delegating tasks or activities (including the processing of records or personal information) that an institution might have the capability to do, but outside parties may do better or cheaper. Outsourcing aims can include reducing costs, increasing efficiency, or improving quality.

Personal information

"Personal information" means recorded information about an identifiable individual, for example, name, home address and telephone number, sex, marital status, education, employment or criminal history, and medical information. Personal information may also include "any identifying number, symbol or other particular assigned to the individual" where "it is reasonable to expect that an individual can be identified from the information (either alone or by combining it with other information." (See FIPPA, s 2(1) / MFIPPA, s 2(1). See also the IPC's 2016 Fact Sheet **What is Personal Information?** and 2024 **Personal Information** Interpretation Bulletin.)

Privacy Impact Assessment

"Privacy impact assessment" or "PIA" refers to an analytical process involving several activities and deliverables. It is not a single document or end product. A PIA should help you identify, analyze, and address key privacy risks when changing or developing programs or systems, including those involving service providers. Understanding your privacy risks can help you take appropriate and timely action to ensure you and your

service provider comply with FIPPA or MFIPPA and other requirements. It also can help you make informed policy, business, procurement, architecture, and security decisions. (See the IPC's 2015 **Planning for Success: Privacy Impact Assessment Guide**).

Processing

"Processing" includes the collecting, using, disclosing, retaining, storing, securing, or disposing of records or personal information.

Procurement

"Procurement" is a process of finding, screening, and acquiring the necessary outside goods or services that can help an institution meet its business and operational requirements.

Record

A "record" means any record of information, however recorded, whether in printed form, on film, by electronic means or otherwise. (FIPPA, s 2(1) / MFIPPA, s 2(1)).

Service provider

A "service provider" is an entity that provides services to the institution. Service providers may be organizations, businesses, or individuals external to the institution, or a different program area within the same institution. The services may or may not be in exchange for payment.

Threat Risk Assessment

A "Threat Risk Assessment" (TRA) is a tool to assist in security risk management and the development of security plans. A TRA is used to assess the sensitivity of assets and information; identify and analyze potential threats and vulnerabilities; assess the level of risk, taking into consideration the effectiveness of current security measures; and recommend appropriate measures to protect assets and information from loss, theft, destruction, modification, or misuse.

IPC Guidance: Privacy and Access in Public Sector Contracting with Third Party Service Providers

Information and Privacy
Commissioner of Ontario

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

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

www.ipc.on.ca
416-326-3333
info@ipc.on.ca

May 2024