foip | Freedom of Information and Protection of Privacy Act

Managing Contracts under the FOIP Act

A Guide for Government of Alberta Contract Managers and FOIP Coordinators

Revised September 2010

Government of Alberta

ISBN 978-0-7785-6102-6

Produced by

Access and Privacy
Service Alberta
3rd Floor, 10155 – 102 Street
Edmonton, Alberta, Canada T5J 4L4

Office Phone: 780-422-2657
Fax: 780-427-1120

FOIP Help Desk: 780-427-5848
Toll free dial 310-0000 first
Email: foiphelpdesk@gov.ab.ca

Websites:
foip.alberta.ca
pipa.alberta.ca

Preface

Alberta Government departments, agencies, boards and commissions use a variety of contracts to operate their programs. When these public bodies enter into contracts and other agreements, they must take into consideration their duties and functions under the *Freedom of Information and Protection of Privacy Act* (the FOIP Act), as well as the Records Management Regulation (RMR) established under the *Government Organization Act*.

The FOIP Act provides a right of access to information in the custody or under the control of public bodies. When a government body enters into a contract, it must ensure that records created by or for the public body will continue to be accessible to the public body for its own use and in response to a request for information by the public. These records must continue to be accessible to enable the government body to fulfil its mandate and functions, as well as its duty of accountability. The FOIP Act further requires public bodies to protect personal information. When a government department or other government body enters into a contract, it must ensure that its responsibility for the protection of personal information will be fulfilled by the contractor on its behalf.

The RMR requires the deputy head of a government department to ensure that department records are managed in accordance with the Regulation. Records management is of critical importance for many reasons; however, it is particularly important in enabling government to meet its obligations under the FOIP Act.

A large number of contracts that public bodies enter into are relatively straightforward, and the application of the FOIP Act and the RMR to the information and records involved is well understood. However, a number of recent trends have resulted in a need for attention to the management of information that is collected, used, disclosed and retained under different types of agreements.

For example, public bodies have entered into an increasing number of agreements relating to shared services, common or integrated programs, and cooperative arrangements such as "public–private partnerships." Some of these agreements involve the sharing of sensitive personal information and new information technology, which may raise concerns about the protection of personal privacy. In other cases, agreements involve the transfer to the private sector of certain functions that have traditionally been carried out in the public sector; this may raise concerns about access to information and continued accountability for public services. In addition, new privacy legislation relating to personal information in the private sector and to health information has, in some cases, led to new obligations on the part of contracting parties. This can arise, for example, when an individual receives services from an organization that is acting under contract to a public body and also acting on its own behalf.

This Guide is designed to assist employees involved in contract management in understanding the implications of the FOIP Act and the RMR for the various aspects and stages of the contracting process. Although the Guide has been designed to meet the needs of provincial government employees, many of the suggestions offered here are likely to be applicable to local public bodies subject to the FOIP Act.

- Chapter 1 provides a summary of some of the key concepts in the FOIP Act and the RMR that are of particular relevance to contracting.
- Chapter 2 outlines different types of agreement that public bodies may enter into, including purchase agreements, fee-for-service contracts, and agreements relating to common or integrated programs.
- Chapter 3 provides an overview of access to information and privacy legislation in Alberta and other jurisdictions that may affect an agreement between a public body subject to the FOIP Act and a body that is subject to other legislation.
- Chapter 4 considers some issues that may arise in relation to different kinds of agreements, such as the processing or storage of personal information outside Alberta, the processing of sensitive personal information, the use of client information by contractors after the end of the contract, and the restructuring of a contractor organization during the life of a contract.
- Chapter 5 covers some business processes that may require consideration of access, privacy and records management issues at the pre-contracting stage of a project. This chapter also discusses records management, access and privacy issues relating to the tendering process. It offers model provisions for inclusion in tendering documents, such as requests for proposals.
- Chapter 6 discusses contract preparation and suggests various model clauses for inclusion in a contract.
- The Checklist in Appendix 1 provides an alternative approach to accessing the content of the Guide.

Throughout the Guide, there are a number of references to the FOIP Act and Regulation and to Orders and Investigation Reports of the Alberta Information and Privacy Commissioner. The Orders and Investigation Reports relate to cases in which various provisions of the FOIP Act have been considered. The Act and Regulation can be found on the FOIP website at foip.alberta.ca. The RMR appears in Appendix 3 of this Guide. The Orders and Investigation Reports are available in full text on the Commissioner's website at www.oipc.ab.ca. Summaries produced by Access and Privacy, Service Alberta are available at foip.alberta.ca.

This publication replaces the *FOIP Contract Manager's Guide*. This revised and expanded version of the Guide aims to provide more comprehensive coverage of issues and examples, while maintaining ease of use through the use of a range of navigational aids, including a detailed table of contents and extensive links between related sections of the publication.

The information provided in this Guide is intended to assist public bodies in understanding how the FOIP Act applies to the contracting process. The Guide is not intended to provide legal advice. The sample contract clauses are provided as examples only and may not be appropriate in all circumstances. Public bodies should obtain legal advice on contract wording when establishing specific contracts.

Visit the FOIP website for information about the *Managing Contracts under the FOIP Act* course that is offered by Service Alberta.

Contents

1.
Fundamentals

1.1 Overview

The Government is constantly seeking ways to increase efficiencies and improve the quality of service through innovative forms of service delivery. Whatever the form of service delivery, however, the Government remains accountable for services delivered in fulfilment of its mandate and functions. When, for example, a government department enters into a contract with a private-sector organization to provide services to the public on the Government's behalf, it is the government department, not the contractor, that is accountable to the public for those services.

It is important, therefore, that the contracting process provides for the clear communication of the obligations of the government body and the contractor respectively, and that the contract ensures that the Government can meet its duty of accountability. This publication is concerned with ensuring accountability in relation to information and records, areas governed by the FOIP Act and the Records Management Regulation (RMR) under the *Government Organization Act*.

With respect to the FOIP Act, ensuring accountability means that the government body can provide a right of access to information relating to the contracted services, and that the government body can demonstrate that personal information is protected in accordance with the privacy provisions of the Act. With respect to the RMR, accountability for contracted services means that the government body can meet its legal requirements regarding the management of records collected, created, maintained or stored by a contractor on behalf of the government body.

Within government, responsibility for contract management resides in a range of different business units, including legal services, program areas, FOIP offices and records management units. Administrative responsibilities may be determined by the volume of contracts to be managed, their value or complexity, the nature of services provided under the contract, or the stage in the life-cycle of the contract. Regardless of where the responsibility for managing contracts resides within the government body, the FOIP Act and the RMR must be taken into consideration in the contracting process.

The following example will highlight some of the concepts that will be addressed throughout the Guide.

> Let us say that a government department created a pilot project to increase the amount of green space in the province. After a three-month trial period in one of the province's main cities, the Department has decided to conduct a survey of the city residents to determine the success of the pilot project. The Department is contracting with a third party organization that specializes in surveys, to perform the service. This organization, Dialling@DinnerTime, will collect the names and telephone numbers of city residents from the Department, collect the survey results from the residents, analyze the data, and

deliver the aggregate, anonymized results to the Department.

There are two distinct issues under the FOIP Act that the Department must address when entering into the contractual arrangement. The first issue is a *right of access* to records in the custody or control of public bodies.

When drafting the contract for this service, the following are some issues or situations the Department should consider:

- Will the Department or Dialling@DinnerTime handle a request to update residents' phone numbers? (For example, an individual may make an informal request along the following lines: "Jimmy Lee no longer lives here, can you please note that in your records?")
- What records does Dialling@DinnerTime have to give the Department if there is a *FOIP request* for records about the survey? (For example, an applicant may make a request for records indicating how many residents were called, how many residents actually participated in the survey, etc.)

The second issue is *protecting personal information* in the custody or control of a public body. The following are some issues or situations the Department should consider:

- What privacy legislation applies to Dialling@DinnerTime?
- Where does Dialling@DinnerTime store the personal information it collects from the surveys?
- What *security measures* does Dialling@DinnerTime have in place to ensure that personal information in its custody is protected? How will the Department determine whether these security measures are sufficient to meet the Department's obligations under the FOIP Act?
- How much information does the Department need from Dialling@DinnerTime? (For example, does the Department need just the aggregate, anonymous results, or additional information?)
- What will Dialling@DinnerTime do with the personal information collected about the city residents after it has completed the contract?

The Guide will discuss these and other issues in more detail, to help public bodies determine what steps are necessary to ensure that their obligations under the FOIP Act are met. This chapter will review some of the key concepts in the FOIP Act and the RMR that are of particular relevance to contracting, including

- definitions of "record" and "personal information,"
- determining custody and control,
- the application of the FOIP Act to contractors,
- excluded categories of information and records, and
- transfer of responsibility for a program within government.

1.2 Key Concepts

Who is subject to the legislation

The FOIP Act and the RMR apply to all records in the custody or under the control of a public body. The term *public body* is defined in section 1(p) of the FOIP Act and includes

- a department, branch or office of the Government of Alberta,
- an agency, board, commission, corporation, office or other body designated as a public body in Schedule 1 of the FOIP Regulation, and
- the offices of Officers of the Legislature.

The RMR uses the word "department" as defined in the *Government Organization Act*, meaning a department of the Government administered by a member of the Executive Council. A "department" is a category of public body under the FOIP Act. In this Guide the terms "public body" and "government body" are used, as applicable within the context.

What is subject to the legislation

The term *record* is defined in the FOIP Act as a record of information in any form. See the glossary in Appendix 4 for the complete definition.

The FOIP Act contains special provisions for *personal information*, which is defined in the Act as recorded information about an identifiable individual. Personal information includes information that can *identify* an individual, such as an identifying number or biometric information, as well as information *about* an individual, such as educational, financial and employment history. See the glossary in Appendix 4 for the complete definition.

The FOIP Act applies to all records in the custody or under the control of a public body, subject to certain exclusions, which are set out in section 4 of the FOIP Act. Exclusions are discussed further below.

Custody and control

A public body has *custody* of a record when the record is in the possession of the public body. A record is in the custody of a public body when, for example, it is on the premises of the public body, in active files or in a central filing facility, or in off-site storage. A record is also in the custody of a public body when the record is in use by an employee in an office, at a work site or in a home or vehicle.

A record is under the *control* of a public body when the public body has the authority to manage the record, including restricting, regulating and administering its use, disclosure or disposition. The concept of control has been considered in several Orders of the Information and Privacy Commissioner. *Order 99-032* provides the most detailed general discussion. For the purposes of managing contracts, the following list of questions, which is not exhaustive, will help in deciding whether records involved in a contracting situation are under the control of the public body.

- Were records that have been transferred to the contractor created by an officer, employee or member of the public body?
- Did the contractor create the records for the public body?
- Does the public body have an irrevocable right to take custody of the records from the contractor?
- Do records that have been physically or electronically transferred to the contractor remain the property of the Crown?
- Does the contract specify that the records are under the control of the public body?
- Does the public body need to create and maintain specific records that it can access either during or beyond the life of the contract?
- Does the public body have authority to direct the use of the records?
- Does information collected or created under the contract have to be maintained as a record under the RMR or another enactment?
- Is the public body bound by its own legislation to maintain the types of records required by the contract, or by other requirements (such as requirements imposed by the Auditor General or law enforcement)?
- Does the public body have authority to dispose of the records?
- Does the contract permit the public body to inspect, review, or copy records produced, received, or acquired by a contractor as a result of the contract?
- Does the public body have copyright in the records?

A public body would normally have control of records relating to the conduct or administration of a program or service under a contract. For example, a public body may have a contract in place for providing particular services to individuals. If the contract requires the contractor to make records available to the public body to audit services provided, the records used by the public body to monitor or inspect the delivery of the services would likely be under its control.

When making a determination as to whether a record is under the control of a public body, the Commissioner is likely to consider the factors listed above in relation to the specific records and make a finding of fact. A contract that addresses the matter of control of records relating to services provided under the contract would be considered, but may not be determinative.

For example, the Commissioner found that a public body had control of a record relating to a report provided to a public body under a contract even though the public body did not have the report in its custody. The Commissioner considered the criteria for control set out in *Order 99-032* and observed that the right to demand possession of a record, or to authorize or forbid access to a record, indicates that a public body has control of a record (*Order F2002-014*).

In another case, the Commissioner found that a record that was in the possession of a public body under conditions of trust imposed by an affected party (prior to

the coming into force of the FOIP Act) was in the custody of the public body and subject to the FOIP Act. The Commissioner rejected the argument that, to have custody of the record for the purposes of the Act, a public body must have a legal right of control. He also found that the public body had control of the record if it had the authority to manage, even partially, what is done with a record (*Order 2000-003*).

Since custody and control are critical to the administration of the FOIP Act and the RMR, public bodies should establish contracts that are consistent with their duties with respect to records and information, and that make the contractor's responsibilities very clear. As long as records are in the custody or under the control of a public body, the legal requirements of the FOIP Act and the RMR apply. The extent to which the contract deals with the specific requirements of this legislation will depend on the nature of the contract.

Application of the FOIP Act to contractors

The FOIP Act includes a number of provisions that expressly apply to individuals and organizations that perform services for a public body under contract. These provisions arise from the definition of the word "employee" (section 1(e)).

Employee, in relation to a public body, includes a person who performs a service for the public body as an appointee, volunteer or student or under a contract or agency relationship with the public body. The Commissioner has defined the term "for" in other provisions of the FOIP Act to mean "on behalf of" (*Order 97-007*).

Wherever the Act refers to an "employee," it is referring not only to an employee in the traditional sense, but also to a person providing services for or on behalf of the public body. For example, the Act permits a public body to disclose personal information to an employee of a public body if the disclosure is necessary for the performance of the duties of the employee (section 40(1)(h)). This provision allows the public body to provide services involving personal information through a contractor; it does so by permitting the public body to disclose personal information to the service provider for the purpose of providing the contracted services.

In most cases, the Act does not specifically refer to the "employees" of a public body. For this reason, public bodies must limit the actions of contractors providing services on behalf of the public body through the contract. For example, the Act permits a public body to use personal information under specified circumstances and for specified purposes (section 39). A public body that enters into a contract with a service provider must limit the contractor's use of personal information to uses necessary to provide the services or carry out the contract.

Since the FOIP Act defines the term "employee" very broadly, an employee of a service provider or a person under contract to a service provider may be considered an "employee" of the public body for certain purposes of the FOIP Act. This would be the case wherever the Act expressly refers to an "employee." Where the Act does *not* expressly refer to "employees," it may be understood that

the duties of a person that has a contractual relationship with a contractor are governed by that contract. To enable a public body to comply with its obligations under the FOIP Act, it may be necessary to require that a service provider's employees and subcontractors are obliged to act in accordance with the applicable provisions of the FOIP Act. The public body should include clauses in the contract with the service provider that require the service provider to require its employees and subcontractors to act in a manner consistent with the applicable provisions of the Act.

The contract between the public body and the service provider should specify which records and information relating to the contracted services remain within the control of the public body. If the contract permits the service provider to subcontract, the contract should also require the service provider to specify in the subcontract which records relating to services performed for the public body remain within the control of the public body. The contract must enable the reader to determine which records are under the control of the public body and which are under the control of the contractor, subject to the public body's right of access for audit purposes.

A public body cannot contract out of its obligations under the FOIP Act or the RMR. For example, section 33 of the FOIP Act states that no personal information may be collected by or for a public body except under certain circumstances. A public body can not enter into a contract for the collection of personal information except as authorized by the FOIP Act or another enactment.

Exclusions

The FOIP Act does not apply to certain categories of records listed in section 4 of the Act. For example, the Act does not apply to records created by or for, or in the custody or under the control of, an officer of the Legislature that relate to the exercise of that officer's functions under an Act of Alberta. If a public body has in its custody a record created by the Auditor General for the purpose of an audit under Alberta's *Auditor General Act*, the FOIP Act does not apply to that record. The same applies to a record that is in the custody of a contractor to that public body.

Exclusions in the Act may apply differently with respect to Part 1 of the Act (access to information) and Part 2 of the Act (protection of privacy). For example, the Act does not apply to a record made from information in a registry specified in section 4(1)(l). A person may not request such a record under Part 1. However, Part 2 limits the collection of personal information for the purpose of creating a registry record. A contractor may collect personal information only as permitted by section 33 of the Act.

Transfer of responsibility for a program within government

A program may be transferred from one ministry to another, for example, during a government reorganization. The formal transfer is effected through an amendment to the Designation and Transfer of Responsibility Regulation under the *Government Organization Act*. The successor public body assumes responsibility for the program when the amendment regulation comes into force.

This includes assuming custody and control of the related records, even though it may take some time to complete the physical transfer of the records to the successor public body.

For further information on the effect of reorganization within government, see *Records Management Activities Checklist for Government Reorganization and Changes in Ministers or Deputy Ministers*, published by the Records and Information Management Branch, Service Alberta. The Access and Privacy unit also provides guidance on managing FOIP requests after reorganization. Contact the unit for further information.

2.
Contracts and Agreements

2.1 Overview

Alberta Government departments, agencies, boards and commissions enter into a variety of contractual arrangements to carry out their functions. These contractual arrangements can vary from a simple agreement between the public body and a contractor for the supply of goods or services, to a multi-year cooperative arrangement where the roles, participation and contributions of each party will change over the term of the contract. A public body may also enter into an arrangement with another public body or private-sector organization to implement a program or project of mutual interest. For any formal arrangement, there is likely to be some form of written agreement or contract (in the case of agencies of the Crown, this agreement is likely to be a Memorandum of Understanding).

The complexity and term of the arrangement will dictate the amount of detail the contractual document will contain. The roles and responsibilities of each party must be set out in the body of the contract, and may be detailed in a schedule to the contract or in an ancillary agreement, such as an information-sharing agreement.

It is up to the public body, with the help of its legal advisors, to decide on the structure of its contractual arrangements. Whatever the arrangement entered into and the documentation used to record it, the public body must, in each situation, take into consideration the issues relating to access to information and protection of personal information that may be exchanged with the contractor or generated as a result of the contractual arrangement.

This chapter provides an overview of the more common types of contractual arrangements entered into by government departments and other government bodies, and some of the access and privacy considerations that typically arise in contracts and agreements. The contractual arrangements discussed are:

- purchase agreements for the acquisition of goods,
- rental agreements and leases for business equipment,
- software licensing agreements,
- fee-for-service contracts,
- contracting for service delivery,
- privatization arrangements,
- public–private partnerships (P3s),
- agreements relating to common or integrated programs or services,
- information-sharing agreements,
- grant agreements, and

- agreements where the public body is the service provider.

Throughout this Guide the terms "contract" and "agreement" are used in accordance with common practice; no legal distinction should be implied.

2.2 Purchase Agreements for the Acquisition of Goods

A public body will generally use a purchase order to acquire goods from a private-sector vendor. The purchase order is a binding commitment when the purchase order is issued. A public body may also have ongoing contracts with specific vendors (for example, Standing Offer Agreements) for the supply of certain goods over a period of time at an agreed price. In either situation, the public body will have custody of the records it creates or receives in the course of the transaction. These would include a written contract, copies of purchase orders, invoices, and payment records.

Access and privacy considerations

Generally speaking, no specific terms relating to the FOIP Act and the RMR are required for a simple contract to purchase goods. Any personal information that may appear in such a contract is typically business contact information, which can be disclosed in accordance with section 40(1)(bb.1) of the FOIP Act. This provision permits the disclosure of an individual's name and business contact information (business title, address, telephone number, facsimile number, and email address), provided that the disclosure does not reveal other personal information about the individual or personal information about another individual.

If a department is dealing with a new supplier, it may be helpful to advise the supplier that government purchasing may be subject to review, including public review on the part of elected officials and media exercising the right of access under the FOIP Act, but that the Act does not permit the disclosure of confidential business information of a third party if disclosure would cause significant harm to the business.

Related sections of this Guide	Chapter
▪ Drafting the contract: FOIP access to information requests	6.4; esp. cl. Nn

2.3 Rental Agreements and Leases for Business Machines

Public bodies regularly rent or lease business machines, partly to facilitate the upgrading of these machines as newer models become available. Many newer-model business machines, such as digital photocopiers and fax machines, have the ability to record and store information – memory chips and hard drives are not limited to computers.

Access and privacy considerations

While newer business machines may have additional features and enhanced capability for processing information, they may also pose a risk to the security of government information. For example, an unauthorized person may be able to retrieve information from a previous transaction, or be able to remove the storage

device. These risks apply whether the equipment is purchased or obtained under a rental agreement or lease. However, government standards for the protection of information on the hard drives of equipment that is being disposed of (*Security Policy for Disk Wiping Surplus Computers,* produced by Service Alberta) do not apply in the context of rental agreements and leases unless specified in the agreement or lease. This means there is a risk of unauthorized access to stored information when a machine is returned to the vendor at the end of the lease or rental period.

Alberta's Information and Privacy Commissioner addressed these concerns in a news release and backgrounder ("Photocopiers and Fax Machines Latest Security Risk," March 15, 2005) and specifically recommended consideration of service contracts and lease agreements to ensure appropriate security for data contained in a storage device and provisions for the protection of stored information when the machine is returned to the supplier.

2.4 Software Licensing Agreements

Under a software licensing agreement, a licensee acquires from the publisher the right to use a piece of software. Title to or ownership of the underlying intellectual property in the software is not typically transferred to the licensee.

The purpose of a licensing agreement is to limit the licensee's use of the software, and to protect the software publishers from loss of revenue due to unauthorized use or exploitation of the software. Licensing agreements also offer a contractual remedy against the user for failing to comply with the terms of the licensing agreement.

Software licensing agreements typically offer users little choice when they enter into the agreement. For example, users may become bound to the terms of the licensing agreement as a condition of opening the software packaging, or software may not be available for use or downloading unless the user agrees to be bound by the terms of the licensing agreement.

Some software licensing agreements contain a jurisdiction clause identifying where the contract was formed and which system of law will apply in the event of a dispute. Where the law of more than one jurisdiction could apply, in the absence of an express selection by the parties as to which law governs, Canadian law dictates that the contract will be governed by the system of law with which the transaction had its most substantial and real connection.

In most cases involving the licensing of software, the user's data is processed and stored locally. However, there are cases where the licence provides for processing and storage by the software distributor. A clear example is where Apple Computers offers .Mac users the ability to store, publish and share their files online, rather than keeping files such as documents, music files and photographs on their local hard drives. The iDisk program allows users to put the contents of their hard drives onto the Internet for remote storage via Apple's servers.

To use iDisk, users must agree to the terms and conditions located within the .Mac Use Agreement and Acceptable Use Policy. The agreement offers users a

non-exclusive, limited licence to use the software for the sole purpose of connecting to the .Mac system. The agreement also contains clauses allowing Apple to conduct investigations into any .Mac account, and authorizing Apple to remove any content from the .Mac system.

Access and privacy considerations

By entering into software licensing agreement, personal information about the user may be stored with the software publishers, who may be located outside Alberta, or outside Canada. Any software licensing agreement that involves the transfer of personal information outside Alberta requires consideration of the interaction between the FOIP Act and other applicable legislation. Consideration must also be given to government policy on transborder data processing and storage.

Related sections of this Guide	Chapter
▪ Interaction between the FOIP Act and other legislation	3
▪ Processing or storage of personal information outside Alberta	4.2

2.5 Fee-for-Service Contracts

A "fee-for-service contract" is used when the Government retains an individual or a company to provide a specific service. This is commonly the case when, for example, a department engages a consultant to provide professional services for a relatively short period of time, or on an ad hoc basis. The contractor may enter into the contract as an individual, a corporation or as a professional corporation. Some of the more common services performed under a fee-for-service contract include conducting research and preparing reports, project management, training, and organizing conferences and events.

The contract typically establishes the services to be provided, who may provide those services, time lines, fees, payment, insurance, and indemnification. The contract may also contain provisions relating to the custody and control of records, ownership of and copyright in the records created under the contract, and the confidentiality of information transferred, collected or created by the contractor.

Access and privacy considerations

The *Public Service Act* distinguishes between a "fee-for-service" contract and employment. This distinction is the subject of a Corporate Human Resources directive (available on the Corporate Human Resources website), which sets out the tests used to determine whether an employment relationship exists. This is significant for matters such as income tax and liability. The *Financial Administration Act* uses the term "personal service contractor" to refer to a person providing services under a fee-for-service kind of contractual relationship. Each of these Acts provides for persons other than government employees to perform services for or on behalf of the Government, and establishes certain powers, duties and functions with respect to these persons.

The FOIP Act adopts a more extensive definition of the term "employee" than either of these other Acts; the definition includes persons other than persons appointed under the *Public Service Act* to perform services for or on behalf of government. This is because the FOIP Act is concerned with establishing accountability for information in the custody or control of a public body.

Section 1(e) of the FOIP Act defines "employee" as including a person who performs a service for or on behalf of the public body under a contract or agency relationship with the public body. This means that the provisions in the FOIP Act that limit the actions of a public body employee may also limit the actions of a contractor providing services on behalf of the public body. For greater certainty, a fee-for-service contract must limit the actions of the contractor by specifically stating rules the contractor must follow regarding collection, use, disclosure, protection, retention and destruction of the relevant records. The contract should also specify that the relevant records are under the control of the public body and establish the responsibilities of the contractor regarding access requests and correction of personal information requests.

Particular care should be taken in defining the contractor's responsibilities and obligations when the contractor will be handling personal information on behalf of the public body. These contracts require a greater level of detail than contracts that do not involve personal information, including specification of the type of physical protection to be used in the contractor's office (including a home office), the methods for transmitting data between the contractor and the public body and the limitations on use and disclosure of the information by the contractor. If a contractor is providing professional services to individuals, such as psychological, counselling or mediation services, the contract should make it very clear which records created by the contractor will be considered to be under the control of the public body.

Subcontractors of the contractor may be considered "employees" within the definition of the FOIP Act for certain purposes (for example, the "whistleblower" protection provisions in section 82). However, if the public body wishes to ensure that the subcontractor performs in accordance with the access and privacy rules that apply to the contractor, the public body must provide for this in its contract with the primary contractor.

The subcontractor may also be subject to private-sector privacy legislation in respect of records containing personal information that are in its custody or under its control. It is important, therefore, that the subcontractor clearly understand which records remain within the control of the public body and are subject to the FOIP Act.

Related sections of this Guide	Chapter
▪ Key concepts: Application of the FOIP Act to contractors	1.2
▪ Contracts involving sensitive personal information	4.4
▪ Assessing privacy capabilities of smaller contractors	5.5

Related sections of this Guide	Chapter
▪ Tendering process	5.7
▪ Drafting the contract: Protection of privacy	6.3; esp. cl. R–S

2.6 Contracting for Service Delivery

Contracting with non-governmental third parties is a common method of service delivery used by public bodies. All or a portion of an existing service previously delivered by government, or a new government service, may be "outsourced" for delivery by a private-sector or non-profit organization. The public body generally pays the service provider a contracted sum for the delivery of the services; however, in some cases, the public body authorizes the service provider to charge a user fee for providing the service.

Outsourcing has been used for the delivery of various services, including information technology services, safety and technical inspections, highway maintenance, registry services, government licensing functions, and the operation of programs and facilities. The public body remains accountable for the program and the performance of the service provider.

Access and privacy considerations

The outsourcing agreement should state whether the public body maintains control over the records. Where the control is to remain with the public body, the agreement should address access to information, protection of personal information and records management.

Outsourcing agreements often require the service provider to store and process information under the control of the public body off-site. These contracts usually require a significant level of detail, especially with regard to records management and, if personal information is involved, the protection of privacy.

The Government's draft *Policy for Protection of Personal Information in Information Technology Outsource Contracts* requires personal information to be processed and stored in Canada, preferably in Alberta.

Any outsourcing agreement that involves the transfer of personal information outside Alberta requires consideration of the interaction between the FOIP Act and other legislation that may be applicable to the contractor, as well as government policy on transborder data processing and storage.

Related sections of this Guide	Chapter
▪ Key concepts: Application of the FOIP Act to contractors; custody and control	1.2
▪ Processing or storage of personal information outside Alberta	4.2
▪ IT outsourcing contracts	4.3
▪ Business case	5.2
▪ Privacy Impact Assessment (PIA)	5.4

Related sections of this Guide	Chapter
▪ Organization of records for alternative service delivery	5.6
▪ Tendering process	5.7
▪ Drafting the contract: Protection of privacy	6.3; esp. cl. Ff

2.7 Privatization

A public body may choose to stop delivering certain services and offer non-government organizations the opportunity to move into the service field. These organizations may be private-sector organizations, non-profit organizations, or a combination of the two. In these instances, the public body may continue to carry on an inspection or auditing role, or undertake licensing and set standards of operations. However, the public body's control over records transferred to, or created in, a privatized service environment would normally end. The records and personal information would no longer be subject to the FOIP Act. This would include personal information that was originally collected by the public body under conditions that imposed statutory requirements on the public body to protect the privacy of the individuals involved with the service.

It is imperative that a public body obtain legal advice at the concept stage of a proposal for privatization.

Access and privacy considerations

The best way to effect the transfer of records and eliminate control by the public body is through legislation supported by an agreement. It is important to define clearly which records or functions will remain within the control of the public body, and which records or functions will be transferred to the control of the private service operator. The agreement should clearly identify the authority under which the transfer takes place and the records that are no longer in the custody or under control of the public body and therefore no longer subject to the FOIP Act.

The implementation strategy to effect the privatization should include a record retention and disposition schedule for the alienation of records transferred to the contractor. The schedule should be authorized by the Alberta Records Management Committee before the agreement is signed. The Provincial Archives of Alberta should also be consulted during the contract negotiations, since the Archives may wish to establish procedures for preserving any archival records.

If the transferred records include personal information, the public body should satisfy itself that the private service operator has the ability to protect the personal information in compliance with Alberta's *Personal Information Protection Act* (PIPA) and, where applicable, the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA).

Special consideration is required where the service provider is a non-profit organization as defined in PIPA. The personal information in the custody or under the control of these organizations is subject to PIPA only when the

information is collected, used or disclosed by the organization in connection with a commercial activity. Wherever possible, the public body should negotiate a clause in the agreement under which the private service operator agrees to establish a privacy policy designed to ensure protection of personal information equivalent to the protection provided under either Part 2 of the FOIP Act or PIPA.

Related sections of this Guide	Chapter
▪ Other Alberta legislation: PIPA	3.2
▪ Business case	5.2
▪ Privacy Impact Assessment (PIA)	5.4
▪ Organization of records for alternative service delivery	5.6

2.8 Public–Private Partnerships (P3s)

Concerns about public debt and fiscal responsibility, growing demands for public services, and the opportunities for innovative approaches to financing of long-term projects have led government to consider providing and financing public programs and services through "public–private partnerships" (P3s).

A *public–private partnership* is a contractual agreement between one or more public bodies and one or more private or non-profit parties for the provision of goods or services with resources, risks and rewards allocated among the parties. P3s have been attributed with the following general characteristics:

- a long-term contractual arrangement,
- a sharing of risks and rewards,
- a joint investment,
- clearly assigned responsibilities, and
- a model of delegated authority and control.

The P3 arrangement is most likely to be used for new, large-scale, complex projects involving a high level of risk, when service delivery lends itself to open, joint management and when service requirements are complicated or constantly changing. A P3 may require a significant financial investment in the project by the non-government parties. The Government of Alberta has entered into P3 arrangements as an alternative for funding certain capital projects, such as the building and maintenance of a major roadway.

A P3 arrangement can take a variety of forms, each varying in the degree to which the public and private sectors are involved. Some P3 arrangements have become very complicated in recent years, involving, for example, multiple parties in an arrangement where services would be delivered to a public body as well as other clients. It is therefore critical that a P3 agreement define the parties' responsibilities, investments, risks, and rewards.

It is imperative that a public body obtain legal advice at the concept stage of a P3.

Access and privacy considerations

Generally speaking, the access and privacy considerations that arise in a P3 agreement are similar to those that arise in other contracts involving non-government bodies. The key issues of control and custody of records, protection of personal information, requests for access to information, and records management need to be addressed in the agreement. There may be a risk of overlooking these fundamentals in an agreement involving other complexities. A P3 may, for example, be a multi-lateral agreement extending over a long period, with multiple schedules and clauses addressing a range of contingencies, such as corporate restructuring over the term of the agreement.

Many of the P3s in Canada and abroad that have attracted public attention have been established for the purpose of large-scale construction projects or for the operation of public utilities. Because of the public interest in these projects, special consideration needs to be given to ensuring access to information. Since P3 arrangements are relatively new and tend to have unique features, it is particularly important to clarify expectations respecting access to information. For example, non-government parties may expect confidentiality with respect to many, if not all, of the elements of the P3 agreement and records relating to the project. Government and non-government parties should recognize some factors that apply especially to P3s.

- There is greater likelihood that records relating to a P3 project may be subject to an access to information request under the FOIP Act because P3 projects usually generate a higher level of public and media interest.
- The agreement and records relating to the P3 project may be withheld under an access request only if one or more of the exceptions to disclosure under the FOIP Act apply. For example, the public body that has custody or control of the records must withhold the records if the disclosure would be harmful to the business interests of a third party in a P3 arrangement (section 16(1) of the FOIP Act). This exception to disclosure does not apply if the information relates to a non-arm's length transaction between a public body and another party (section 16(3)(c)).

Although P3 arrangements relating to construction projects tend not to involve significant amounts of personal information, there have been cases where P3s have been established to operate programs in which the protection of personal information is a major consideration, for example, where a private-sector organization cooperates with an educational institution to build a special facility or to develop a program in a field that is of interest to the organization but is currently under-served by the public education system. A P3 agreement of this kind would require close attention to the protection of personal information.

Since the private-sector party or parties would be governed by private-sector privacy legislation with respect to activities that are not provided for or on behalf of the public body, careful consideration needs to be given to the interaction between the FOIP Act and the privacy legislation that applies to the private-sector party or parties.

TIP The Commissioner has determined that a partnership can be a third party under the FOIP Act, even where one of the partners is a public body (*Order 2000-005*).

Related sections of this Guide	Chapter
▪ Key concepts: Custody and control	1.2
▪ Interaction between the FOIP Act and other legislation	3
▪ Processing or storage of personal information outside Alberta	4.2
▪ Use and retention of information about common clients	4.6
▪ Corporate restructuring, mergers and buy-outs	4.7
▪ Confidential business information	4.9

2.9 Information-Sharing Agreements

A public body may need to share personal information with another party when the public body has a legal obligation or other interest in contributing to a particular program or activity, but is not itself responsible for all aspects of that program or activity. Information sharing can occur on a one-time, time-limited, or ongoing basis. It may involve the sharing of a small number of data elements about one individual, or a large number of data elements about a number of individuals, client groups, or populations.

Where personal information will be shared on an ongoing basis, the public body should enter into an information-sharing agreement with the other party to set out the particulars for the information transfer. The agreement should state the objectives to be achieved under the information-sharing agreement and include provisions specifying

- the specific personal information involved (i.e. the data elements),
- the purpose for which the information may be used by the recipient,
- to whom the recipient may disclose the information,
- the method of transmission,
    - requirements for the protection, retention and disposal of the information, and
    - measures to audit or monitor compliance with the agreement.

For a more detailed discussion of explanation on the preparation of an information-sharing agreement, see the *Guide for Developing Personal Information Sharing Agreements*, published by Access and Privacy, Service Alberta.

Access and privacy considerations

The public body that provides the information under the information-sharing agreement must have the authority to disclose the information under section 40(1) of the FOIP Act. Section 40(1)(e) permits disclosure of personal information for the purposes of complying with an agreement made under an enactment of Alberta or Canada. If a government body's own legislation does not provide for the execution of an information-sharing agreement, section 10 of the *Government Organization Act* may do so (see section 3.3 of this Guide for a more detailed discussion of the power to enter into an agreement under section 10 of the *Government Organization Act*, as well as requirements for intergovernmental agreements under section 11 of the *Government Organization Act*). If a government body is proposing to enter into an agreement with a local public body, the local public body must have the power under its own legislation to enter into an agreement for the purpose in question.

The public body that provides the information should satisfy itself that the recipient has the authority to collect and use the information and is capable of protecting the privacy and security of the information at a level equal to or better than that required of the public body.

If the recipient is allowed to further disclose the information to another party, the information-sharing agreement should state that the recipient is responsible for verifying that the other party is authorized to collect the information and for ensuring that the other party will be subject to the same restrictions regarding use, disclosure and security.

Related sections of this Guide	Chapter
▪ Interaction between the FOIP Act and other legislation	3
▪ Use and retention of information about common clients	4.6
▪ Privacy Impact Assessment (PIA)	5.4
▪ Drafting the contract: protection of privacy	6.3

2.10 Joint Service Delivery Agreements

Government programs and services may be delivered by various levels of government or by two or more public bodies working in a collaborative manner. It has been a longstanding practice for provincial, federal and municipal governments to share in the delivery of services, for example, in the area of social benefits. Common service centres have also been established for the public to go "one-stop shopping" for related programs or services. In some cases, centres provide access in a single venue to services offered by different levels of government. Examples include programs and services relating to economic development, skills development and student financing.

These collaborative program and service initiatives vary in approach and scope. The business and program objectives that a public body wishes to accomplish

through the initiative will dictate the extent of control over pre-existing records and over any records collected or created during the new service delivery process.

Access and privacy considerations

Joint service delivery initiatives may relate to a range of services, including services to businesses that do not involve a significant amount of personal information, and services to individuals, which may involve considerable amounts of sensitive personal information. Whatever the nature of the service, it will be important that the agreement address the question of custody and control, since this will determine the extent to which the FOIP Act and RMR will apply in particular circumstances, and what conditions and standards apply to the records.

The agreement should state the types of records each party is providing, whether records transferred to another body remain under the control of the public body, whether the records should be segregated, and whether the records should be returned to the contributing body on the expiry or termination of the agreement.

In cases where a joint service delivery agreement involves services to individuals, it will be particularly important to work out the flow of personal information for the purposes of operating the program and to ensure that each of the participants in the program can collect or disclose personal information, as applicable, under its governing legislation.

The situation is most straightforward where the parties are subject to the FOIP Act with respect to the information collected, used or disclosed under the joint service delivery arrangement. The FOIP Act includes a provision for the disclosure of personal information to an employee of a public body if the disclosure is necessary for the delivery of a common or integrated program or service and for the performance of the duties of the employee to whom the information is disclosed (section 40(1)(i)). This provision enables public bodies to share personal information for the purpose of delivering a joint program.

Each public body must have its own authority to collect the personal information. Section 40(1)(i) then allows for indirect collection from the other public body; use of the personal information by each public body to perform its functions; and disclosure to the other public body as required to enable that body to perform its functions. Where a public body relies on section 40(1)(i), any indirect collection, use or disclosure must be limited to the purposes of the joint program.

The purpose of this provision is to eliminate the need for each public body to collect the same information from the client or for one public body to obtain the client's consent to disclose information to the other public body. The intent is not to permit indirect collection, use or disclosure of personal information for administrative convenience, simply because public bodies have common clients. For more information on this subject, see *FOIP Bulletin No. 8, Common Programs and Services*, published by Access and Privacy, Service Alberta.

The joint service delivery agreement, or a separate information-sharing agreement, should address access to and correction of personal information by clients of the program or service, and protection of personal information,

including requirements for recording the disclosure of personal information by one public body to another, as well as safeguards for the transmission of personal information. Each public body will be responsible for recording any personal information bank created as a result of the agreement in the public body's directory of personal information banks.

The situation may be more complicated where one or more parties are not subject to the FOIP Act with respect to the information collected, used or disclosed under the agreement (including public bodies with respect to health information subject to the *Health Information Act*). In that case, it will be necessary to consider the effect of other party's governing privacy legislation on the terms of the agreement. It may be necessary to obtain the consent of the individuals who will be participating in the program, to use or disclose their personal information. If that is the case, the agreement should address all aspects of the consent process.

Related sections of this Guide	Chapter
▪ Key concepts: Custody and control	1.2
▪ Information-sharing agreements	2.9
▪ Interaction between the FOIP Act and other legislation	3
▪ Use and retention of information about common clients	4.6
▪ Business case	5.2
▪ Privacy Impact Assessment (PIA)	5.4
▪ Organization of records for alternative service delivery	5.6
▪ Drafting the contract	6

2.11 Grant Agreements

A public body may, if authorized by its own governing legislation or by a regulation under the *Government Organization Act*, provide a grant to an individual or an organization.

A grant is a disbursement of money made by the Government as a gift, transfer or payment with no exchange of goods or services. The purpose and terms and conditions of the grant may be set out in the regulation or in a written grant agreement.

The public body normally has very little control of the day-to-day operations of the person or program funded by the grant. The grant recipient may be subject to reporting and auditing requirements, as specified in the regulation or the grant agreement.

Access and privacy implications

A grant is a payment for which goods or services are not normally received by the public body. Any intellectual property developed under the grant would not normally be provided to the granting body. If the public body wishes to retain a

right to use, to publish, or to collect revenue on the intellectual property, this should be specified in the grant agreement. If the public body asserts a right to intellectual property, the agreement should indicate the terms under which it will exercise that right (for example, the public body may assume control over the intellectual property once it has indicated, in writing, that it will exercise the right).

The regulation or grant agreement may provide that the Minister responsible for the public body or the Auditor General has the right to examine and take copies of any records necessary for accountability within the grant program. This would typically include reports, financial statements, receipts, invoices, and other records that are required to be submitted to the Minister or Auditor General.

The grant recipient should acknowledge that the FOIP Act applies to records submitted by the recipient to the public body, including the grant application, and that the records may be disclosed in response to an access request under the FOIP Act, subject to any applicable exceptions to disclosure under the Act.

A public body may provide a grant to a person to purchase goods or services from a private-sector provider approved by the public body. In these cases, records relating to payments made by the public body to the provider that are in the control of the public body would be subject to the FOIP Act. Transactions between the private-sector provider and the grant recipient would not be subject to the FOIP Act (unless for some reason the information was in the custody of the public body). Personal information collected, used or disclosed for the purpose of providing the services may be subject to private-sector legislation. The public body should clarify its responsibilities in this regard in its notice to the grant recipient.

2.12 Agreements Where the Public Body is the Service Provider

In recent years, some public bodies have taken on the role of providing services to other public bodies within the Government (for example, Service Alberta). The goals of these arrangements include cost and administrative efficiencies, standardization, and a one-window approach for users. The public body providing the service will be required to protect the privacy and security of personal information that it handles on behalf of the client public bodies.

Access and privacy considerations

The contract for the provision of services should specify which public body has control of the records and the parties' responsibilities in relation to an access request. In most cases, the control will remain with the client public body.

The public body providing the service will handle records on behalf of the client public bodies. The public body providing the service may use the information only in accordance with the contract. The public body providing the service may need to segregate that information from its own operating records and from the information and records of its other clients.

In some situations, the client public body may access the electronic information system of the public body providing the service in order to input, view, or retrieve

data. The client public body should be required to use a secure form of access, with the necessary safeguards (for example, passwords, firewall and virus protection) to ensure the integrity of the information system.

TIP Private-sector privacy legislation requires organizations to assume responsibility for the contractor's compliance with the legislation. This does not apply in situations where a public body provides services under a contract with an organization. The public body remains subject to the FOIP Act.

Related sections of this Guide	Chapter
▪ Key concepts: Custody and control	1.2
▪ Use and retention of information about common clients	4.6
▪ Drafting the contract	6; esp. cl. C, E, H, L, Bb–Gg.1

3.
Interaction between the FOIP Act and Other Legislation

3.1 Overview

Alberta Government departments and other public bodies subject to the FOIP Act enter into agreements with a range of government bodies, as well as organizations in the private sector that are subject to other legislation. When entering into these agreements, public bodies should aim to ensure that the rights and powers conferred by the FOIP Act are not diminished.

The most important general points to bear in mind when entering into an agreement with a body that is not subject to the FOIP Act are as follows.

- Each party to the agreement must comply with the legislation that governs that party *with respect to the transaction* – parties cannot "contract out" of their governing legislation.
- Where the legislation that governs the other party provides for a lower standard than the FOIP Act with respect to access or the protection of personal information (as applicable), the agreement should, if possible, include clauses that require the other party to meet the higher standard.
- The contracting process should provide clarity regarding the obligations of the parties; it is generally preferable to state what those obligations are rather than to include clauses that merely require the parties to comply with legislation that would not otherwise apply.

There is a broad range of access to information and privacy legislation in Canada. The federal government and all of Canada's provinces and territories have access to information and privacy legislation that applies to the public sector. In addition, some provinces, including Alberta, have separate legislation for health information.

Since January 1, 2004, all private-sector organizations in Canada have also been subject to privacy legislation. The federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies to the collection, use and disclosure of personal information by federally regulated organizations regardless of where the collection, use or disclosure occurs within Canada. PIPEDA also applies to the collection, use and disclosure of personal information by organizations in provinces that do not have their own provincial legislation. In Alberta, British Columbia and Quebec, all of which have legislation that is substantially similar to the federal Act, PIPEDA applies only to an organization's disclosure of personal information *outside* the province.

Although this range of legislation may appear complex, the various Acts are largely based on common principles. This chapter will provide a brief overview of how Alberta's FOIP Act interacts with some of this other legislation. Topics covered include:

- the paramountcy of the FOIP Act over other Alberta legislation,
- Alberta's *Health Information Act* (HIA),
- Alberta's *Personal Information Protection Act* (PIPA),
- the paramountcy of federal legislation over provincial legislation,
- the federal *Access to Information Act* and *Privacy Act*,
- the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA),
- United States legislation,
- extra-territorial application of foreign law, and
- jurisdictions with no privacy legislation.

For each Act covered in this chapter, the discussion will briefly explain the purposes of the Act, provide key definitions, highlight the most significant differences between the FOIP Act and the Act in question, and provide examples of situations in which the other Act is relevant to an agreement between a public body and another party. Some tips are offered, as well as references to other resources. Public bodies may need to seek legal advice when entering into agreements that involve the interaction between different Acts with respect to new situations.

3.2 Other Alberta Legislation

Paramountcy of the FOIP Act

The FOIP Act is an Act of general application and it is paramount over most other Alberta Acts and regulations. If a provision of the FOIP Act is inconsistent or in conflict with a provision of another enactment, the provision of the FOIP Act prevails unless another Act, or a regulation under the FOIP Act, expressly provides that the other Act or regulation, or a provision of it, prevails over the FOIP Act (section 5). Section 5 of the FOIP Act provides the means for resolving a conflict or inconsistency in situations where other legislation states that it prevails over the FOIP Act, or where compliance with one law would involve a breach of the other (see *Orders 99-034* and *F2005-007*).

For the most part, paramountcy comes into play when another Act or regulation restricts access to information. The most common case is where another Act or regulation contains a confidentiality provision. If a confidentiality provision expressly states that it prevails despite the FOIP Act, then, if there is a request for access to that information, that confidentiality provision may limit the ability of a public body to provide access.

TIP If there is a possibility of a misunderstanding as to which of two enactments will govern a transaction under a contract, it may be helpful to address the issue of which law applies in situations where a conflict may be anticipated.

For further information about paramountcy, see *FOIP Bulletin No. 11, Paramountcy*, produced by Access and Privacy, Service Alberta.

Health Information Act (HIA)

The FOIP Act does not apply to health information, as defined in the *Health Information Act* (HIA), that is in the custody or under the control of a public body that is a custodian as defined in HIA.

Health information, as defined in HIA, means diagnostic, treatment and care information, and/or registration information that is collected, used or disclosed by custodians.

Custodian is defined in HIA to include bodies such as a regional health authority, provincial health boards, the Minister and department of Alberta Health and Wellness, licensed pharmacies, pharmacists, physicians and other health professionals designated as custodians in the Health Information Regulation.

For custodians that are also public bodies under the FOIP Act, such as Alberta Health and Wellness and Alberta Health Services, HIA applies to *health information*, as defined in HIA, and the FOIP Act applies to *personal information*, as defined in the FOIP Act.

HIA is based on a concept that is considered important for the delivery of health services. This is the concept of a "controlled arena" in which custodians operate. Health information can move from one custodian to another within the controlled arena for purposes authorized in the Act. Outside this arena, the movement of individually identifying health information is more restricted. The general rule is that an individual's consent is required before individually identifying information is disclosed. Another general rule is that a custodian may disclose only the least amount of information at the highest degree of anonymity for the purpose of the disclosure.

Since the FOIP Act and HIA apply to categories of information that are mutually exclusive, there is no conflict between the two Acts and the question of paramountcy does not arise.

However, there are aspects of HIA that need to be taken into consideration in agreements between public bodies and custodians. Some key points to bear in mind are as follows.

- The FOIP Act applies to personal information, including medical information, that is in the custody or under the control of a public body. The FOIP Act applies, for example, to records created by a custodian under contract to a public body that are unrelated to providing a health service (as defined in HIA). However, if a public body transfers medical information to a custodian (including a custodian that is a public body), the information may become health information subject to HIA when it is in the hands of the custodian. The rules that apply to the information may be different.
- The FOIP Act permits a public body to disclose personal information to an officer or employee of a public body if the disclosure is necessary for the delivery of a common or integrated program or service (section 40(1)(i)). However, HIA does not permit disclosure by a custodian to a public body

without consent for the purpose of a common or integrated program or service. Section 40(1)(i) of the FOIP Act does not allow for disclosure to a custodian that is not a public body. A public body would normally require an individual's consent for such a disclosure unless the disclosure is authorized by some other provision of section 40.

Example A **A public body enters into a fee-for-service contract with a person who is a custodian under HIA**

The Workers' Compensation Board (WCB) requires a claimant to undergo an independent medical assessment performed by a physician under contract to the WCB. Since the service is not a health service the information is not subject to HIA. WCB is a public body subject to the FOIP Act and not a custodian under HIA. When it engages the services of the physician, the records must remain within the control of the public body, in such a manner that the information relating to the contract is subject to the FOIP Act.

TIP Since, in some cases, the physician is likely to be more familiar with the requirements of HIA than the FOIP Act, it may be helpful to include clauses in the contract, or a schedule to the contract, setting out how the FOIP Act applies to the information, where this would be different from HIA.

Example B **A public body enters into an agreement with a custodian with respect to a service delivery**

Alberta's Student Health Initiative is a collaborative program intended to build cooperative relationships that strengthen the province's collective capacity to support students with special health needs. When each party is acting on its own behalf under an agreement concerning the program, that party is subject to its own governing legislation. Alberta Children and Youth Services and Alberta Education are subject to the FOIP Act with respect to all personal information, including medical information. Alberta Health and Wellness and Alberta Health Services and those health professionals designated as custodians under the Health Information Regulation are subject to HIA for personal health information.

TIP As a practical consideration, it may be advisable to include a clause in the agreement requiring specified personal information, as opposed to health information, to be collected, used or disclosed in accordance with the FOIP Act.

TIP In the case of a common or integrated program, it may be advisable to include a clause in the agreement regarding the consent of individuals to collection, use and disclosure of their personal information. This could be important where the public body obtains consent to disclosure by the public body and consent to the collection by the custodian at the same time. Including such a clause will ensure that there is certainty as to how each of the parties to the agreement will meet their legal obligations under their own governing legislation.

A public body that provides records management or IT services for a custodian may become an Information Manager under HIA. For further information on information manager agreements and other issues relating to HIA, the Alberta Health and Wellness HIA Help Desk can be contacted at (780) 427-8089.

Personal Information Protection Act (PIPA)

The *Personal Information Protection Act (*PIPA) governs the collection, use and disclosure of personal information by organizations within Alberta.

Organization is defined in the Act (section 1(i)) to include

- a corporation,
- an unincorporated association,
- a trade union as defined in the *Labour Relations Code*,
- a partnership as defined in the *Partnership Act*, and
- an individual acting in a commercial capacity,

but not an individual acting in a personal or domestic capacity.

If an organization is providing services for a public body, personal information relating to the contracted services will remain under the control of the public body and the FOIP Act will apply to the information. PIPA (or other applicable privacy legislation) will govern the protection of other personal information in the custody or under the control of the organization (for example, the personal information of the organization's employees).

PIPA contains two provisions that are critical to determining which Act applies to information relating to contracted services. First, PIPA does not apply to a public body or any personal information that is in the custody or under the control of a public body (section 4(2)), with the exception of Alberta Treasury Branches (Regulation, section 3). In addition, PIPA does not apply to personal information that is in the custody of an organization if the FOIP Act applies to that information (section 4(3)(e)).

PIPA is based on the principle of consent. The Act requires organizations to obtain the consent of individuals for the collection, use and disclosure of their personal information, except in a limited number of circumstances specified in the Act. Consent may be express, implied or opt-out, depending on the sensitivity of the personal information. The standard that applies for most provisions of PIPA is *reasonableness*, an objective standard as to what a reasonable person would think appropriate in the circumstances (section 2). PIPA contains special provisions for personal employee information.

Since the FOIP Act and PIPA apply to different bodies, and since PIPA does not apply to information to which the FOIP Act applies, there should be no conflict between the two Acts and the question of paramountcy should not arise.

Some key points to bear in mind when negotiating agreements between public bodies and organizations are as follows.

- PIPA contains general provisions concerning the transfer of personal information between public bodies and organizations. PIPA expressly allows an organization to collect personal information from a public body if the public body is authorized to disclose the information to the organization

(section 14(c)). Similarly, an organization can disclose personal information to a public body if the public body is authorized to collect the information from the organization (section 21(c)).

- The FOIP Act permits a public body to disclose personal information to an officer or employee of a public body if the disclosure is necessary for the delivery of a common or integrated program or service (section 40(1)(i)). This provision does not allow a public body to disclose personal information to an organization that is not a public body for the purpose of a common or integrated program or service, unless that organization is providing a service on behalf of a participating public body under a contract.
- PIPA applies to non-profit organizations, as defined in the Act, only with respect to personal information that is collected, used or disclosed in connection with a commercial activity carried out by the non-profit organization (section 56). When a public body enters into a fee-for-service contract with a non-profit organization, the contracted service would likely constitute a commercial activity. Some other agreements between a public body and non-profit organization may not constitute a commercial activity. If a public body discloses personal information to a non-profit organization for a purpose that does not meet the definition of a commercial activity, that information has no legislated protection.
- PIPA does not apply to health information, as defined in the *Health Information Act* (HIA), to which that Act applies (section 4(1)(f) of PIPA).
- PIPA provides a right of access to an individual's own personal information. If a public body discloses information that is not personal information to an organization, there is no right of access to that information through the organization. The right of access is through the public body, which may, therefore, need to retain control of the records containing the information.

Example C **A public body enters into a contract with an organization to provide services for the public body**

This is the clearest case involving the interaction between the FOIP Act and PIPA. The FOIP Act, not PIPA, applies to the information relating to the services provided under the contract. For example, a service provider enters into a contract to deliver a training program on behalf of a public body. The public body provides personal information regarding the individuals registered in the program. The personal information remains within the control of the public body and the FOIP Act applies to that information. The public body should provide for the protection of the information in the contract with the service provider. Any request under the Act for personal information must be submitted to the public body.

TIP It would be advisable to make the obligations of the service provider clear in the contract, especially where these obligations may differ from those that the contractor has in contracts with private-sector clients. If the contract permits the service provider to use subcontractors, the contract between the public body and the service provider should specify that personal information relating to

subcontracted services remains within the control of the public body, and require the subcontractor to protect that information in accordance with the FOIP Act.

Example D **A public body enters into an agreement with an organization to provide a service to the public body that entails collection, use and disclosure of personal information by the organization for its own purposes.**

Alberta Employment and Immigration operates Training on the Job programs. The department enters into an agreement with the employer organization to train a client and provides a partial wage subsidy to the employer. The employer is required to report to the department on the individual's progress. The organization's collection, use and disclosure by the employer of personal information within the control of the department are subject to the FOIP Act. As an employer, the organization also has to meet its own obligations with respect to the individual. The employer organization's collection, use and disclosure of personal information for those purposes are subject to PIPA.

For further information about PIPA, see the Service Alberta website on Private-Sector Privacy at pipa.alberta.ca.

3.3 Federal Legislation

Paramountcy of federal legislation

In an area where federal and provincial governments both have a constitutional right to legislate, federal legislation prevails over provincial legislation where there is a conflict. The FOIP Act is a provincial act of general application governing access to records and information. Federal legislation that deals specifically with restrictions on disclosure would override the more general provincial access legislation. For example, the *Youth Criminal Justice Act* (Canada) prohibits the disclosure of information regarding a young person which may identify him or her as a young person involved in proceedings under that Act. This prohibition prevails over any right of access under the FOIP Act.

For the most part, the paramountcy of federal legislation comes into play when a federal Act restricts access to information, usually through a confidentiality provision. If a public body receives a request for access to that information, that confidentiality provision may limit the ability of a public body to provide access.

The issue of federal paramountcy does not arise under the disclosure provisions in Part 2 of the FOIP Act because compliance with a federal Act does not involve a breach of the FOIP Act. For example, the federal *Income Tax Act* requires employers to disclose certain payroll information for tax purposes. Since this disclosure is required by an enactment of Canada, the FOIP Act permits the disclosure (section 40(1)(f)). A federal Act that prohibits disclosure of certain information would not be inconsistent with Part 2 of the FOIP Act since the disclosure provisions in the FOIP Act permit, but do not require, the disclosure of certain information.

TIP If there is a possibility of uncertainty as to which of two Acts, the FOIP Act or a federal Act, will govern a transaction under a contract, it may be helpful to address the matter in the contract.

For further information about paramountcy, see *FOIP Bulletin No. 11: Paramountcy*, produced by Access and Privacy, Service Alberta.

Federal public-sector access and privacy legislation

The federal *Access to Information Act* and the federal *Privacy Act* apply to federal government institutions as defined in those Acts. Although the federal government has two Acts rather than one, as in Alberta, the principles in federal and provincial access and privacy legislation are similar.

The FOIP Act permits a public body to refuse to disclose information if the disclosure could reasonably be expected to harm relations between the Government of Alberta or its agencies and the Government of Canada or any of its agencies. Any disclosure of information that falls into this category must be approved by the Minister responsible for the FOIP Act in consultation with Executive Council. In addition, the FOIP Act permits a public body to disclose information supplied explicitly or implicitly in confidence by the Government of Canada or any of its agencies *only* with the consent of the body that supplies the information (section 21).

Conversely, a government institution subject to the *Access to Information Act* may refuse to disclose information if disclosure could reasonably be expected to be injurious to the conduct of federal–provincial affairs. In addition, the *Privacy Act* requires a government institution to refuse to disclose personal information obtained in confidence from the government of a province or one of its agencies, unless that government consents to the disclosure.

Neither the federal legislation nor the FOIP Act applies to First Nations.

There are, however, a few significant differences between the federal and provincial legislation.

- The *Access to Information Act* and the *Privacy Act* limit the right of access to Canadian citizens and permanent residents; the FOIP Act provides a right of access to any person.
- The "exemptions" under the *Access to Information Act* are similar to the exceptions in the FOIP Act. In some cases, however, differences in the application of a particular exception may be significant for a certain category of information. For example, the exception to disclosure for information that is subject to privilege is considerably broader under the FOIP Act than under the *Access to Information Act*. The FOIP Act permits a public body to withhold information that is subject to parliamentary privilege and work done by a lawyer or agent of the Minister of Justice and Attorney General.
- The exception for third party personal information in the *Access to Information Act* does not apply to information about a past or present officer or employee of a government institution relating to the position or functions of the individual, including the name of the individual on a record prepared by that individual or the opinions or views of the individual given in the course of employment. Alberta's FOIP Act does not *exclude* this category of

information; however, the Alberta Act may allow for non-disclosure of similar employee information under some circumstances.

- The federal *Privacy Act* has a much less stringent test regarding the manner in which personal information is to be collected than the FOIP Act.
- The federal *Privacy Act* allows for use and disclosure of personal information with the individual's consent; consent may be inferred in some cases. Under the FOIP Act, consent to the use or disclosure of personal information must be express written consent.
- The federal *Privacy Act* does not include a provision relating to the security of personal information as in the FOIP Act.

Under the *Government Organization Act*, Alberta International and Intergovernmental Relations (IIR) is responsible for approving all intergovernmental agreements entered into by a Minister, officer or agency of the Government of Alberta. Agreements with the Government of Canada, the government of another country, province or territory, or an agency or official of another government must be forwarded to IIR for approval. An inventory of agreements undertaken by ministries is published in IIR's Annual Report, formalizing the record of ministerial approval for all intergovernmental agreements signed during the period covered by the Report.

Example E **A public body enters into an agreement with a federal government institution to deliver services to a common set of clients.**

Agriculture and Agri-Food Canada and Alberta Agriculture and Rural Development enter into an agreement to operate the Canada–Alberta Farm Water Program. The purpose of the program is to provide financial and technical assistance toward the cost of long-term on-farm water supply developments. The federal department is subject to federal access and privacy legislation for information within its custody or control and the provincial department is subject to the FOIP Act for information within its custody or control. A person seeking access to information regarding the program may need to determine which body has the records sought and, in certain cases, may have to submit a request to both departments.

TIP To ensure effective access to information relating to the program, the agreement should specify the records that are within the control of each department, which records are supplied in confidence and what the process will be for requesting consent from the other department where an exception to disclosure for information harmful to intergovernmental relations may apply.

Example F **A public body enters into an information-sharing agreement with a federal government institution.**

Alberta Seniors and Community Supports has an agreement with Human Resources and Social Development Canada to match information relating to individuals receiving both Canada Pension Plan disability benefits and disability income program benefits in the province. The purpose of this information sharing is to ensure accurate reporting of income. The provincial public body is subject to

the FOIP Act for records in its custody or control; the federal government institution is subject to federal access and privacy legislation. Any records created as a result of the matching process would be in the custody and control of the body that collected the information, used it in the matching process and created the new database or record of information.

TIP When entering into an agreement to share personal information, it is advisable to cite the statutory authority for the collection, use and disclosure of personal information under the agreement, as well as the statutory authority to enter into the agreement. Since the federal *Privacy Act* does not address security, it may also be advisable to put the security measures in the contract.

Federal private-sector privacy legislation (PIPEDA)

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) governs the collection, use and disclosure of personal information by organizations in the federally regulated private sector (for example, banks, telephone companies, cable companies), regardless of where that collection, use or disclosure occurs. PIPEDA also governs the collection, use and disclosure of personal information in the course of commercial activity by organizations in provinces that have not enacted substantially similar legislation. In the case of provinces that have enacted substantially similar legislation, PIPEDA applies to the disclosure of personal information *outside* the province. Alberta's PIPA has been deemed substantially similar to PIPEDA.

Organization is defined in PIPEDA (section 2) to include an association, a partnership, a person and a trade union.

Commercial activity means any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fund-raising lists (section 2).

PIPEDA is based on a code of fair information practices developed by business, consumers, academics, and government under the auspices of the Canadian Standards Association. The code, which is included as a Schedule to PIPEDA, consists of ten principles, the most important of which is the principle of consent. PIPEDA requires organizations to obtain the consent of individuals for the collection, use and disclosure of their personal information, except in a limited number of circumstances specified in the Act.

PIPEDA does not apply to the Government of Alberta. The federal Privacy Commissioner has also stated that the Act does not apply to any public body to which the FOIP Act applies. In addition, the federal Commissioner has indicated that PIPEDA does not apply to the collection, use or disclosure of personal information by an organization outside Alberta that is under contract to provide services for the Government of Alberta. However, the courts have not yet made a determination on this point.

Some key points to bear in mind when negotiating agreements between public bodies and organizations subject to PIPEDA are as follows.

- PIPEDA applies to organizations only with respect to personal information that is collected, used or disclosed in connection with a commercial activity. If a public body discloses personal information to a non-profit organization for a purpose that does not meet the definition of commercial activity, that information has no legislated protection.
- PIPEDA does not apply to an individual's business contact information, except business email.
- PIPEDA does not apply to an organization's employees except in the federally regulated private sector.
- PIPEDA provides a right of access to an individual's own personal information. If a public body discloses information that is not personal information to an organization, there is no right of access to that information through the organization. The right of access is through the public body, which may, therefore, need to retain control of the records containing the information.

Example G **A public body enters into an outsourcing contract with a data processing organization in Manitoba.**

The public body is subject to the FOIP Act. The data processing organization is under contract to the public body and is therefore an "employee" for the purposes of the FOIP Act with respect to the services it provides for or on behalf of the public body. Records and information transferred to the organization and records and information relating to the contracted services that are created or maintained by the organization remain within the control of the public body and are subject to the FOIP Act.

TIP The contract should state that the records and information relating to the contract that are in the custody of the contractor remain within the control of the public body and are subject to the FOIP Act. In addition, the contract should clearly outline the responsibilities of the contractor with respect to personal information, especially where these obligations may differ from those that the contractor has in contracts with private-sector clients. If the contract permits the data processing organization to use subcontractors, the contract between the public body and the data processing organization should specify that personal information relating to subcontracted services remains within the control of the public body, and require the subcontractor to protect that information in accordance with the FOIP Act.

3.4 United States Legislation

The United States has a range of federal and state legislation that provides for access to information and protection of personal information, such as the federal public-sector *Freedom of Information Act* and *Privacy Act* and the access to information legislation of individual states. There is also an array of legislation that provides privacy protection for certain categories of information held by the private sector. For example, at the federal level, the *Gramm–Leach–Bliley Act* protects financial information, the *Health Insurance Portability and Accountability Act* protects certain health information, and the *Children's Online Privacy Protection Act* limits the collection of children's personal information

through websites. This is often referred to as a "sectoral" approach to privacy protection.

Safe Harbor

The sectoral approach to privacy protection created some issues for the United States when the European Union (EU) established a directive requiring member states to have a comprehensive legislative scheme to protect personal information. The directive prohibited member states from allowing personal information to be transferred to countries that did not provide an adequate level of protection for that information. The United States responded by developing, in consultation with the EU, a self-certification program called the Safe Harbor framework. Where an organization adheres to a privacy policy that meets the Safe Harbor requirements, European member states may transfer personal information to that organization. The Safe Harbor framework does not apply to personal information that is transferred between the U.S. and Canada.

The EU also decided that member states may authorize the transfer of personal information to countries which do not ensure an adequate level of protection through legislation, but which allow safeguards to be established through contractual clauses.

Further information about the Safe Harbor framework and the contracting guidelines is available at the U.S. Department of Commerce website www.export.gov/safeharbor.

3.5 Extra-territorial Application of Foreign Law

USA PATRIOT Act

The *USA PATRIOT Act*, enacted by the U.S. Congress shortly after September 11, 2001, is anti-terrorism legislation that, among things, expanded the intelligence-gathering and surveillance powers of law enforcement and national security agencies by amending the U.S. *Foreign Intelligence Surveillance Act* (FISA). Section 215 of the *PATRIOT Act* allows U.S. authorities to obtain records and other "tangible things" to protect against international terrorism. Section 218 of the Act requires that foreign intelligence gathering need only be "a significant purpose" of surveillance in the U.S., thus allowing the use of information for other, unrelated purposes. Section 505 of the Act expands the circumstances under which the FBI can compel financial institutions, telephone companies and Internet service providers to secretly disclose information about customers.

After the enactment of the *PATRIOT Act*, concerns were raised in Canada that these provisions could be used to order a corporation located in the U.S. to produce information obtained in the process of providing services under contract to a public body in Canada. In addition, it was suggested that these provisions could be used to compel information from an affiliate of a U.S. corporation located in Canada.

In 2006, the Information and Privacy Commissioner of Alberta issued a report on the risks presented by outsource practices of public bodies, and how the risks could be mitigated. The report recommended operational, contractual, and

legislative measures. Recommended operational measures included a policy for retaining personal information in Canada, preferably in Alberta, with deviations only where program requirements, costs or security could not reasonably be met within Canada.

The recommended contractual provisions included prohibiting subcontracting without written consent, requiring notice of any demand for access or unauthorized access to personal information in the contractor's custody, requiring monitoring and auditing rights, and addressing consequences for a breach.

The recommendations for legislative action to address outsourcing concerns included amending the FOIP Act to clarify that disclosure of personal information pursuant to a court order may be made only with respect to a Canadian court with jurisdiction, and increasing the penalties for a breach.

The FOIP Act was amended in 2006 to address concerns about access to personal information by foreign law enforcement authorities. This amendment makes it clear that a public body, and anyone acting on its behalf, may disclose personal information in response to a subpoena, warrant or order of a court or tribunal, or to comply with a court rule, *only* if the court or tribunal has the power in Alberta to require the public body to disclose the information. A court or tribunal of another country or of a province or territory of Canada other than Alberta does not have jurisdiction in Alberta. However, an order of such a court or tribunal may be enforceable in Alberta under legislation of Alberta that provides for the reciprocal enforcement of orders (for example, Alberta's *Interprovincial Subpoena Act*), or a court procedure that makes an order filed with a court in Alberta enforceable as an order of the Alberta court.

Intentionally disclosing personal information to a foreign court is now an offence under the FOIP Act, and is subject to a penalty of between $200,000 and $500,000 (section 92(3) and (4)).

Public bodies should address demands for information by courts in their contracts. A public body's contract with a principal contractor should also require the contractor to bind its subcontractors and employees to not disclose personal information in response to a subpoena, warrant or order of a court or tribunal without the express permission of the public body.

In addition, the contract should require the contractor to inform the public body if any subpoena, warrant or order is issued to the contractor or any person acting on behalf of the contractor, even if the subpoena, warrant or order, or the legislation governing the issuing court or tribunal, requires secrecy.

Public bodies should seek legal advice regarding contracts with organizations that are subject to U.S. law.

3.6 Jurisdictions with No Privacy Legislation

Many countries provide a lower standard of protection for personal information of Albertans than is the case in Alberta and the rest of Canada. In some jurisdictions, including certain jurisdictions in which there is a concentration of organizations providing services involving personal information, there is no statutory protection for personal information.

In these cases, contractual agreements provide the only method of protection, not only against improper use or disclosure within that jurisdiction, but also against improper disclosure to bodies outside the jurisdiction. While such contracts are enforceable in other jurisdictions, it may be difficult to impose the penalties or other remedy provided under the contract. There have been a number of different approaches in these jurisdictions to the issue of protecting personal information for the purposes of providing outsourced services. The U.S. Safe Harbor framework, discussed above, is one example of a framework designed to address the absence of a comprehensive statutory regime.

More recently, Asia–Pacific Economic Cooperation (APEC) has developed a Privacy Framework that promotes a consistent approach to data protection among APEC member countries, many of which do not have their own data protection legislation. APEC is currently working on the implementation of this Framework through the use of cross-border privacy rules (CBPRs). Organizations within APEC member countries will create their own CBPRs, which must be recognized as compliant with the nine privacy principles of the Framework, and contain acceptable enforcement provisions.

4.
Special Considerations in Contracting

4.1 Overview

Government departments and other bodies enter into a broad range of contractual arrangements relating to a wide variety of projects that fall within the Government's mandate – from the management of the province's natural resources to the inspection of commercial vehicles, from large-scale construction projects to the delivery of personal services to individuals. This range of projects brings an equally broad range of special considerations that may be expected to arise in contractual arrangements to deliver these programs and services.

This chapter will consider some issues that may be expected to arise in contracting and provide guidance on existing practices developed by public bodies to address these issues. Model contract clauses to address these issues are included in Chapter 6.

Several of the issues discussed relate primarily, though not exclusively, to the protection of personal information:

- processing or storage of personal information by a contractor located outside Alberta or outside Canada (including the interaction between Alberta privacy legislation and the legislation of other jurisdictions),
- IT outsourcing contracts (including developments in government policy),
- contracts involving sensitive personal information (such as an individual's medical information, an individual's financial information, and personal information in a law enforcement record),
- control of records created by a regulated professional under contract (for example, psychologists providing counselling services to employees or clients of a public body),
- use and retention by contractors of information about common clients (clients that have a relationship with the public body as represented by the contractor and also with the contractor acting on its own behalf), and
- corporate restructuring, mergers and buy-outs (including the possibility of conflict of interest, and considerations regarding assignment of contracts).

Other issues relate more to questions of access to information:

- costs of large-scale or complex FOIP requests, and
- confidential business information (including access to information relating to fees and charges imposed by the contractor for delivery of services).

4.2 Processing or Storage of Personal Information Outside Alberta

Alberta has a very comprehensive and robust framework of privacy legislation. The FOIP Act protects personal information within the extended public sector. Alberta's *Health Information Act* (HIA) protects health information collected by custodians such as Alberta Health and Wellness, Alberta Health Services, licensed pharmacies, pharmacists, physicians, and other health professionals. Alberta's *Personal Information Protection Act* (PIPA) protects personal information held by private-sector organizations, and by non-profit organizations engaged in commercial activity. When personal information is transferred within Alberta – among public bodies, custodians and organizations – there is a high level of assurance that the personal information will have strong statutory protections.

When personal information is transferred *outside* the province, the statutory regime and the level of protection may differ. Within the public sector, standards are reasonably comparable. For example, personal information protected under Alberta's FOIP Act would receive a similar level of protection in the hands of the B.C. government. Health information is protected in all Canadian jurisdictions, but under varying legislative regimes. Some provinces, including Manitoba, Saskatchewan and Ontario, have health information legislation. In other provinces, protection is provided by some combination of general public-sector and private-sector legislation.

Coverage of the broader private sector also varies by jurisdiction. Organizations in all Canadian jurisdictions are subject to private-sector privacy legislation for personal information that is collected, used or disclosed in the course of commercial activity. However, not all provinces offer privacy protection that is as comprehensive as Alberta's. For example, personal employee information and personal information collected for non-commercial purposes has a lower degree of protection in some provinces.

When a public body contracts with a body in another Canadian jurisdiction that is subject to other privacy legislation with respect to its own activities, the determination of powers, duties and functions requires more analysis than contracts where Alberta law applies to the parties for all activities.

There may be less legal certainty regarding the application and interpretation of the law. For example, it is well established under the FOIP Act that a public body is responsible for the protection of personal information by a contractor acting on its behalf. However, the courts have not ruled on how the federal private-sector privacy statute, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), applies when a public body contracts with a third-party service provider in another Canadian jurisdiction.

In addition, commissioners in other jurisdictions may not have the powers of enforcement that the Information and Privacy Commissioner has in Alberta. For example, the Privacy Commissioner responsible for overseeing federal privacy legislation does not have the ability to order compliance with privacy legislation; a complainant may have to pursue a well-founded complaint in the courts.

Faced with various legislative schemes, legal uncertainty and issues of enforcement, a public body may conclude that there is less risk attached to storing personal information within the province.

Nevertheless, there are situations where contracting for services within the province is not a reasonable option, and a public body may decide to contract with a service provider located in another Canadian jurisdiction. The Government of Alberta's draft *Policy for Protection of Personal Information in Information Technology Outsource Contracts* requires departments to ensure that contracts specify that records containing personal information collected, used, disclosed, or stored on their behalf will be stored within Alberta, or if that is not feasible, elsewhere in Canada. The draft policy requires departments to consult with the Office of the Corporate Chief Information Officer and with the Office of the Information and Privacy Commissioner before any decision to permit personal information to be stored outside the province. Although this policy applies only to IT outsource contracts, the draft Policy provides a helpful guide to public bodies contracting for any data processing functions or contracted services involving the storage of personal information.

If a public body decides to enter into a contract that involves the transfer of personal information outside Alberta, the contract should be very clear about the contractor's obligations with respect to the collection, use, disclosure, protection, retention, and destruction of all personal information to ensure that the public body is compliant with the FOIP Act. A separate schedule to the contract may be appropriate in some cases to address these obligations in sufficient detail. The public body may need to obtain legal advice on this matter.

The public body will need to consider all legislation that applies to the contracting parties, as well as that which applies, or may apply, to the activities to be governed by the contract. When a public body contracts with an organization that would be subject to other private-sector privacy legislation when the organization was acting on its own behalf, it needs to be clear that personal information within the control of the public body is subject to Alberta's FOIP Act.

The contract should limit, or prohibit, the use or disclosure of the personal information, as well as access to the personal information outside Alberta or the jurisdiction in which the contractor is located, for any purpose where the use or disclosure would reduce the protection that the personal information would normally have in Alberta. This is particularly important if the contractor is a subsidiary of a foreign organization. The contract may need to require that personal information be stored within Alberta.

A public body considering outsourcing outside Canada needs to consider the implications of two major gaps in privacy protection. First, the other jurisdiction may have no privacy legislation requiring the organization to protect personal information (as in the case of some Asian countries where data-processing services are carried out). In such cases, protection of personal information is limited to the protection provided under the contract; there is no additional statutory protection as in Canada. Second, it may be difficult to enforce the terms

of the contract, especially if the organization has competing legal obligations. For example, the United States Foreign Intelligence Surveillance Court has the power to issue an order to an organization that is subject to U.S. law to provide access to personal information and to prohibit the organization from disclosing the existence of the order to any person, including the contracting body or the individual the personal information is about.

A Minister may consider approving an arrangement for the processing or storage of personal information outside Canada where the risk is relatively low; this may be the case where the arrangement involves some combination of the following factors:

- the contract involves a relatively small number of individuals rather than whole client populations,
- the sensitivity of the personal information is relatively low,
- the nature of the service and applicable laws allow the contractor in the foreign jurisdiction to retain the personal information for a minimal amount of time,
- the service to be provided requires expertise that is not available in Canada.

In any case where a public body proceeds with a contract for the processing or storage of personal information outside Canada, the contract should prohibit any disclosure without notification and consent of the Minister, and include substantial consequences for breach of this condition.

It should be noted that amendments to the FOIP Act made in 2006 permit a public body to disclose personal information in response to a subpoena, warrant or court order *only* if the court has the power in Alberta to compel the information. Intentionally disclosing personal information to a foreign court is an offence. A public body would be liable if a contractor in a foreign jurisdiction disclosed personal information under the control of the public body to a foreign court, even if the contractor were legally obliged to do so.

Related sections of this Guide	Chapter
▪ Extra-territorial application of foreign law	3.5
▪ Jurisdictions with no privacy legislation	3.6
▪ Business case	5.2
▪ Privacy Impact Assessment (PIA)	5.4
▪ Drafting the contract: Protection of privacy	6.3; esp. cl. Hh–Jj
▪ Drafting the contract: Monitoring compliance	6.5; esp. cl. Qq–Rr
▪ Drafting the contract: Applicable law	6.8

4.3 IT Outsourcing Contracts

IT outsourcing contracts and their associated risks vary considerably. A detailed discussion of issues relating to IT outsourcing is contained in the *Contract Management Framework for Information Technology Projects*.

The Government of Alberta also has access to the resources of the Information Security Forum, which is an independent association of leading organizations that provide research on, and solutions for, key issues in information security. There are currently over 300 members worldwide, including nine Canadian provincial governments. Membership provides access to a library of research and tools, including detailed risk assessments, which are available under licence to Government of Alberta employees and contractors. For further information on any of these resources, email ciso@gov.ab.ca

A number of business units within the Government of Alberta have developed tools to ensure high standards in IT contracts. For example, Alberta Health and Wellness has produced a *High Level Security Assessment* (HLSA), which is to be completed by organizations contracting to perform IT services for the department. The HLSA is a comprehensive security assessment based on ISO 17799 Code of practice for information security management. It includes a review of the organization's security management and architecture, access controls, application development, business continuity, as well as physical and systems security. The assessment is approved by the Alberta Health and Wellness Information Policy and Compliance Unit, as well as the Security Officer. Further information can be obtained from the Information Policy and Compliance Unit in Alberta Health and Wellness.

Related sections of this Guide	Chapter
▪ Contracting for service delivery	2.6
▪ Processing or storage of personal information outside Alberta	4.2
▪ Corporate restructuring, mergers and buy-outs	4.7
▪ Costs of large-scale or complex FOIP requests	4.8
▪ Privacy planning tool for it projects	5.3
▪ Privacy Impact Assessment (PIA)	5.4
▪ Tendering process	5.7
▪ Drafting the contract: Protection of privacy	6.3

4.4 Contracts Involving Sensitive Personal Information

What is sensitive personal information?

The FOIP Act does not create classes of personal information. This means that public bodies are required to protect all personal information in accordance with the Act's provisions for collection, use, disclosure, retention, and protection. At the same time, the Act clearly permits the disclosure of certain personal information under conditions that are less restrictive than in other cases. For example, the Act permits public bodies to disclose

- personal information about a deceased individual without restriction twenty-five years after death (section 40(1)(b) in conjunction with section 17(2)(i)),
- an individual's business contact information, provided that the disclosure does not reveal other personal information about that individual or another individual (section 40(1)(bb.1)), and
- certain information about an individual's participation in public events provided that this is not contrary to the public interest or the wishes of the individual (section 40(1)(b) in conjunction with section 17(2)(j) and section 17(3)).

The Act also recognizes that, while virtually any personal information may be sensitive in certain contexts (for example, disclosure of a home address may expose an individual to risk for personal or professional reasons), there are certain categories of personal information that are considered sensitive for all or most individuals. Section 17(4) of the Act states that it is presumed to be an unreasonable invasion of personal privacy to disclose such categories of information, including

- an individual's medical information,
- personal information in a law enforcement record,
- an individual's financial information,
- an individual's educational history,
- an individual's employment history, and
- personal evaluations and character references.

Assessing risk

In any contracting arrangement involving personal information, the public body should consider the degree of risk with respect to the privacy and security of personal information under the proposed contract with the prospective contractor. This requires a determination of the likelihood of a breach of privacy, and the severity of the impact if the breach were to occur.

The likelihood of a breach occurring may be affected by factors such as

- the number of contracted staff who have access to the personal information,
- the level and training of the contracted staff,
- the use of subcontractors,
- the security of the contractor's IT system,
- the distribution of IT resources (mobile offices, laptops, BlackBerries, etc.),
- whether the contractor handles information from other organizations in the same location, using the same personnel, using the same IT system.

The severity of the impact of a breach may be affected by factors such as

- the number of individuals whose personal information is contained in the database,
- the number of data elements pertaining to each individual that are contained in the database,
- the sensitivity of the personal information,
- whether the contractor has direct access to the public body's IT system (for example, some public bodies require the contractor to enter data directly into their information system).

In addition to these factors, specific contracts may pose special risks. These risks may arise, for example,

- the contractor will be collecting the information in an individual's residence,
- the contractor will be collecting information about children, or
- the information will be collected directly from children.

Public bodies that propose to implement projects involving the collection, use or disclosure of sensitive personal information will normally complete a formal Privacy Impact Assessment (PIA). This is the case whether the public body intends to do the work itself or to have the work done under contract. As an alternative to a PIA, some public bodies have developed an assessment tool in the form of a questionnaire designed for specific service providers. This approach is considered particularly useful for small and medium-sized organizations. The questions can be made very specific, which makes it easier for smaller contractors to respond. Also, the questions can be designed for specific types of organization and to address specific risks associated with the particular contract.

Related sections of this Guide	Chapter
▪ Fee-for-service contracts	2.5
▪ Privacy Impact Assessment (PIA)	5.4
▪ Assessing privacy capabilities of smaller contractors	5.5
▪ Tendering process: Protection of personal information	5.7
▪ Drafting the contract: Protection of privacy	6.3; esp. cl. Bb

4.5 Contracting with a Member of a Professional Regulatory Association

Members of professional regulatory organizations are subject to professional standards and have obligations to their governing bodies. Some standards, such as the Generally Accepted Auditing Standards for chartered accountants, require members to document certain matters in their working papers during an audit. Working papers generally describe the records prepared by a professional, such as an accountant or lawyer, as tools to perform a work assignment. Courts have traditionally held that these working papers remain solely in the custody and under the control of the professional. The Information and Privacy Commissioner

has also indicated that a public body may not have control of records held by a contracted professional if the records were created for the professional's own purposes (for example, fulfilling professional obligations), or where the public body would not have the authority to collect the personal information in the records (for example, medical information collected by a counselling services to employees of a public body, under contract) (*Order F2006-028*).

When contracting with a member of a regulated profession, public bodies should make clear in the contract which records relevant to the contract will remain within the custody and the control of the regulated professional, and which records will come within the custody or control of the public body.

There may be situations in which a public body does not want to maintain control of a contractor's records, for example, when a public body contracts with a psychologist to provide counselling under an employee assistance program. In the event that the public body receives an access request for the working papers of a professional with whom the public body has contracted, a clear provision in the contract stating that such papers do not fall within the public body's custody or under its control would support a claim that the FOIP Act does not apply to the records. (An individual could request access to his or her own personal information under PIPA.)

In other situations, where a public body wants to maintain control of records such as working papers in order to maintain accountability to the public, the contract should stipulate that the professional must turn over all working papers to the public body at the end of the contract. Alternatively, the contract could state that the public body retains control over all documentation for the purposes of the FOIP Act.

When negotiating and drafting an agreement with a member of a professional regulatory organization, the public body should bear in mind the requirements of the profession's legislation and code of conduct. The public body should ensure that the agreement allows the member to comply with his or her professional requirements, and to meet the public body's obligations with respect to access to information and the protection of privacy.

4.6 Use and Retention of Information about Common Clients

In addition to providing services to a client on behalf of a public body, a contractor (another public body or a private-sector organization) may provide services to the client on its own behalf. This may occur either at the same time as performing services under contract to the public body, or immediately following expiry of the contract with the public body. This situation raises issues of control of the personal information about clients in the records held by the contractor, and the disposition of the information at the end of the contract.

For example, a public body may contract with a post-secondary educational institution to provide skills training to an individual. That institution may also provide that individual with other training at the same time as, or after, the program that was funded by the public body. Some or all of the information

collected by the institution under the contract with the public body will be required by the institution to provide services on its own behalf to the individual.

Similarly, a public body may contract with an employer to provide on-the-job training to an individual, and the employer may decide to employ the individual after the end of that contract. As a prospective employer, the contractor will need much of the information that was provided by the public body at the commencement of the individual's training, or was created in the course of the training.

The public body may wish to consider the following measures to ensure that the contractor uses personal information provided for the purposes of the contract only as permitted under the FOIP Act.

- State in the contract that personal information necessary to provide the contracted services to the public body remains under the control of the public body.
- Specify in the contract what personal information may be disclosed to the contractor acting for the public body and what personal information, if any, may be disclosed to the contractor in its capacity as an independent entity acting on its own behalf. Specify the purpose for which the public body may disclose the information, the circumstances under which the information may be disclosed and any conditions that may apply.
- Specify in the contract that the contractor may collect personal information of a client from the public body for the contractor's own purposes only if the public body is authorized to disclose the information and decides to do so. The contract should state that the public body has no obligation to disclose personal information to the contractor, even if it may be reasonable to do so.

  If the public body determines that it has the authority to disclose personal information to the contractor for the purpose specified, the public body may require the contractor to confirm that it has the legal authority to collect the information and to do so indirectly (if the contractor is a public body) or without consent (if the contractor is an organization). Details relating to the process of disclosure by the public body and collection by the contractor acting on its own behalf (including any process of obtaining an individual's consent, if applicable) may be set out as a personal information-sharing agreement in a separate schedule to the contract.
- Ensure that notification provided to an individual by the contractor acting on behalf of the public body meets the requirements of the FOIP Act, by providing
  - the purpose for which the information is being collected by the public body (including the contractor acting on behalf of the public body),
  - the specific legal authority for the collection by the public body,
  - contact information for a person who can answer the individual's questions about the collection, use and disclosure of the personal information by the public body.

The contractor should also notify the individual that the public body (including the contractor acting on behalf of the public body) is required to protect personal information in accordance with the FOIP Act.

Consider requiring the provision of additional information, including

- the specific personal information that may be disclosed to the contractor for the purposes of the contractor acting on its own behalf, and the purpose for which that information will be disclosed, and
- the specific legal authority for disclosure to the contractor acting on its own behalf and, if consent for disclosure is required, who is responsible for obtaining consent and how valid consent will be obtained.

It is the responsibility of the contractor to provide any required notification to the individual of

- the purposes of the collection of personal information by the contractor on its own behalf,
- contact information for a person who can answer the individual's questions about the collection, use and disclosure of the personal information by the contractor,
- the contractor's obligation to protect personal information disclosed by the public body to the contractor for the contractor's own purposes in accordance with the privacy statute that is applicable to the contractor acting on its own behalf.

Related sections of this Guide	Chapter
▪ Key concepts: Custody and control	1.2
▪ Information-sharing agreements	2.9
▪ Joint service delivery agreements	2.10
▪ Interaction between the FOIP Act and other legislation	3
▪ Drafting the contract: Protection of privacy	6.3

4.7 Corporate Restructuring, Mergers and Buy-outs

Organizational restructuring, corporate mergers and buy-outs have occurred with some frequency in recent years. This possibility should be considered in any outsourcing arrangements, and, in particular, with respect to multi-year contracts, multi-party contracts, IT contracts, public–private partnership (P3) agreements, and large-scale contracts.

Some issues that may arise over the life of these kinds of contract and some mitigating measures that public bodies should consider include the following.

- A corporate buy-out or merger involving two separate contractors of the public body could create a conflict of interest. An example would be the merger of a contractor that is responsible for providing services to the public

body with a contractor that is responsible for auditing or investigating other contractors for the same public body. The public body may choose to include a condition in the contract that the public body could terminate either or both of the contracts should such a merger of contractors create a potential conflict of interest.

- A contractor may be bought out by another organization that has a different privacy framework or culture, with policies and procedures that do not meet the standards of the public body. The organization taking over the business of the original contractor may also be subject to different privacy legislation from the original contractor. To address these possibilities, the public body may include a provision in the contract that a Privacy Impact Assessment, a privacy audit, an on-site visit, or a combination of these measures, may be required prior to the public body's approval of the assignment of the contract. The contract clause may include a provision that the new organization would be responsible for the costs associated with this requirement.
- A contract may stipulate that personal information must not be processed or stored outside of Canada. In this case, the contract should also stipulate conditions that will apply if a corporate merger or buy-out would lead to a breach of that condition. The contract may provide that the contract will immediately cease to have effect or that conditions for continuation of the contract must be approved by the Minister. In either case, the terms of the contract should ensure continued access by the public body to information within the public body's control and an orderly transition.

Related sections of this Guide	Chapter
▪ Public–private partnerships	2.8
▪ Interaction between the FOIP act and other legislation	3
▪ Drafting the contract: General contractual clauses with FOIP implications	6.9

4.8 Costs of Large-Scale or Complex FOIP Requests

Public bodies normally include a condition in the contract stating that, if the public body receives an access request under the FOIP Act for any records maintained by the contractor, but under the control of the public body, the contractor must provide responsive records within a given time to the public body at the contractor's expense. The contractor is obliged to comply regardless of the size or complexity of the access request.

Where a contract contains such a clause, the contractor is presumed to have included the potential costs of FOIP requests in the cost of the contract. However, it is difficult to predict the number, the regularity, or the scope of FOIP requests that may be made in the course of any given project. If the contractor projects an excessive amount for potential FOIP requests, the cost of the contract to the public body may be inflated unnecessarily. If the contractor does not allocate sufficient resources, the contractor may be unwilling or unable to retrieve and to provide the responsive records. This could affect the processing of the FOIP

request, and hence the public body's compliance with the FOIP Act. Alternatively, the contractor may attempt to recoup the cost of its part in processing the FOIP request from funds intended to provide the core services of the contract.

This issue has become more critical with respect to more recent IT contracts, many of which involve large-scale and complex IT systems and databases. For example, under the Service Coordinator Initiative and the Alberta Secure Access Service Project, it may be extremely costly, time-consuming, and technically demanding to retrieve the personal information of any particular individual. The question arises whether the usual contractual condition that requires the contractor to bear all of the risk is fair and appropriate. How should the public body address this issue? Some of options that may be considered are as follows.

- Establish a base amount that the contractor will be responsible for if asked to produce records relating to FOIP requests in a given year. Beyond that level, the contractor will be reimbursed for the costs by the public body either as extra work, or through contingency fees included in the budget under the contract. The rate of reimbursement should be predetermined, perhaps in accordance with the fee schedule under the FOIP Regulation. (This option is based on the notion that, prior to the outsourcing arrangement, the public body was obliged to handle any large or complex FOIP requests, in some instances by redeploying financial or human resources to handle these requests.)
- Consider including a specific amount in the contract for privacy-related activities. This could include the costs of any FOIP requests as well as the costs of privacy training for the contractor's staff. Any money not used in a given year could be carried over to the next contract period.

The number and nature of options that are available to address this issue is constrained by the current FOIP Regulation and the *Financial Administration Act*. The fees that a public body is allowed to charge under the FOIP Regulation will cover only a small portion of the costs associated with any large-scale or complex request. Also, under section 14 of the *Financial Administration Act*, FOIP fees are paid to the General Revenue Fund rather than to the public body.

Related Topics	Chapter
▪ IT outsourcing contracts	4.3
▪ Business case	5.2
▪ Tendering process	5.7
▪ Drafting the contract: FOIP access to information requests	6.4

4.9 Confidential Business Information

When a public body contracts with a private-sector business to provide services, there is often a need for the business to share confidential information with the public body. This may consist of commercial, financial, labour relations, scientific or technical information. In certain cases, disclosure of this information

by the public body may significantly harm the competitive position of the business, interfere with its ability to negotiate, or cause undue financial loss. It is therefore critical for the parties to the contract to have a clear understanding about what business information is supplied to the public body in confidence. This will ensure that the public body does not cause harm to a business by disclosing confidential business information in response to a request under the FOIP Act.

Where it is important to include confidential business information within a contract, a good practice is to set out the confidential information in a schedule rather than in the body of the agreement. This will facilitate severing in response to an access request. Exceptions to disclosure in response to a FOIP request are discussed in Appendix 2.

Another issue that may arise in relation to confidential business information is disclosure for the purpose of reviewing fees and charges for services to clients. Review of fees and charges stems from a decision of the Supreme Court of Canada in 1998. The Court declared in the *Eurig Estate* case that probate fees charged in Ontario, which had been established by regulation, were unconstitutional. The Court ruled that, since the revenue collected was much greater than the cost of providing this compulsory service, the fee should be considered a tax and must therefore be authorized by legislation.

Following that decision, Alberta established a Fees and Charges Review Committee, which released a report to the Government in 2000. In this report, the Committee established a guiding principle for the review process: where a compulsory charge is a genuine fee for service, the fee should reflect the cost of providing the service.

The Government accepted and continues to apply this guiding principle. If a contractor is authorized to charge a user fee for the services it provides to public users on behalf of the government (for example, licensing or inspection services), the fee may require Government approval. Departments must obtain approval of their Senior Financial Officer for new or amending regulations that introduce a change in fees or charges.

Where a number of organizations deliver the same service on a competitive basis, the information used to determine the fee may be considered competitive commercial information, which the public body has an obligation to protect. A public body that manages agreements involving fees and charges needs to ensure that it communicates the rationale, the review process and the protections provided for business information to the organizations concerned.

The measures that a public body may wish to consider include

- consulting with the department's Senior Financial Officer to determine whether the proposed method of cost recovery through user fees to be charged by the contractor will require Government approval, the process and information required to secure the approval, and the confidentiality of any cost information submitted to the committee;

- setting out this requirement in the RFP or other communication to prospective contractors and explaining that the final contract, or at least the fee schedule of the contract, may not be executed until Government approval is secured; or
- indicating the type of cost information that the contractor may be required to provide and the protection provided to that information in the event of an access request under the FOIP Act.

Related sections of this Guide	Chapter
▪ Tendering process	5.7
▪ Drafting the contract: FOIP access to information requests	6.4

5.
Pre-contracting Processes

5.1 Overview

Ensuring compliance with the FOIP Act and the RMR should begin well before the contracting process. By clearly addressing requirements relating to access to information, protection of privacy and records management early, the public body can ensure that

- the implications of a proposal to enter into a contract are understood,
- the contractor can make an informed assessment of the responsibilities involved in the contract, and
- the full cost of compliance is recognized.

This chapter provides consideration of some of the pre-contracting processes that may require attention to access, privacy and records management considerations, namely:

- development of the business case for a business initiative involving sensitive personal information,
- the Privacy Planning Tool required for all IT projects,
- the Privacy Impact Assessment (PIA),
- the assessment of the privacy capabilities of smaller contractors,
- the organization of records prior to implementing an alternative service delivery initiative, and
- the solicitation or tendering process, from the initial stage of communicating the requirements of the contract to the final disposition of submissions.

Table 1 provides a summary of risk mitigation strategies in tendering documentation and contracts.

5.2 Business Case

The Alberta Government has designed a business case template as a means for provincial public bodies to analyze major business initiatives such as a decision to adopt an alternative form of service delivery. Where the initiative involves the collection, use or disclosure of sensitive personal information, the public body should include an evaluation of the related risk factors, as well as the cost of compliance with the FOIP Act and the RMR. This evaluation does not replace the requirements of a more detailed Privacy Impact Assessment. It does, however, provide a high-level review of the privacy issues within the overall framework of the business initiative.

The business case should address the following questions.

- How does the proposed form of service delivery, including any process changes to the collection, use, disclosure, and protection of personal

information, affect the public body's obligations under the FOIP Act and RMR? What mitigating measures should be included in the arrangement, and what are the costs of these measures?

- How will the alternative form of service delivery affect the public right of access to information related to the program? What mitigating measures should be included? What, if any, are the additional costs of the measures to the public body and to the public?
- How will routine disclosure and active dissemination of information be affected by the proposed outsourcing? Can a process be established to enable the continuation of routine disclosure and active dissemination of information?

5.3 Privacy Planning Tool for IT Projects

The Privacy Planning Tool (PPT) is part of Alberta's Information and Communications Technology (ICT) Privacy Framework. The purpose of the tool is to assist project managers with the management of new information or of existing information in new ways or for new purposes. The tool is also intended to assist in the development, acquisition and implementation of software. The tool is an online questionnaire based on the principles embodied in the Privacy Impact Assessment (PIA). However, it is shorter and simpler and is intended to be completed early in the project cycle, before any PIA, as part of the project management process.

The tool is intended to be used for every ICT project. The information is submitted to Service Alberta, which provides recommendations with respect to privacy risk assessment and risk mitigation measures.

5.4 Privacy Impact Assessment (PIA)

A Privacy Impact Assessment (PIA) is undertaken during the planning and implementation of a program or system. It involves a detailed consideration of appropriate and effective measures to ensure compliance with Part 2 of the FOIP Act. In Alberta, PIAs are submitted to the Office of the Information and Privacy Commissioner for review and acceptance. The Commissioner does not *approve* PIAs, but acceptance indicates that the flow of information contemplated under the proposed program or system is in compliance with the provisions of the FOIP Act, that risks have been assessed and the public body has a plan to mitigate the risks.

A PIA is not mandatory under the FOIP Act when a public body proposes to enter into a contract relating to a program or service that involves personal information. However, it is a good practice to complete a PIA for any contract involving the collection, use or disclosure of personal information, unless only business contact information was involved and the personal information would not be stored outside Alberta or Canada.

In cases where a new contractual arrangement involves the collection, use, disclosure, protection, retention and disposal of sensitive personal information, or where the contract may require the processing or storage of personal information outside Alberta, a public body should conduct a PIA to ensure that the impact of

the contractual arrangement is fully evaluated. The PIA should be conducted prior to the tendering process so that any privacy requirements can be reflected in that process.

TIP A public body that is a custodian for the purposes of Alberta's *Health Information Act* (HIA) or that is considering entering into an agreement with a custodian should bear in mind that a custodian is required, under section 64 of the HIA, to prepare a PIA prior to implementing any administrative practices or information systems that may affect the privacy of an individual's health information. The planning process should allow time for the development and review of the PIA.

For consideration of when a PIA is needed, see section 9.3 of FOIP *Guidelines and Practices*, published by Access and Privacy, Service Alberta. For a detailed explanation of the PIA process and requirements, see the documentation available on the Commissioner's website at www.oipc.ab.ca.

Related sections of this Guide	Chapter
▪ Contracting for service delivery	2.6
▪ Public–private partnerships (P3s)	2.8
▪ Joint service delivery agreements	2.10
▪ Processing or storage of personal information outside Alberta	4.2
▪ IT outsourcing contracts	4.3
▪ Contracts involving sensitive personal information	4.4
▪ Use and retention of information about common clients	4.6
▪ Drafting the contract: Protection of privacy	6.3; esp. cl. Ff, Ii, Jj

5.5 Assessing Privacy Capabilities of Smaller Contractors

The PIA process is designed to ensure a public body can comply with its privacy obligations. Part 1 of the PIA relates to the prospective contractor. Some public bodies have developed an assessment tool, which is a simplified version of Part 1 of the PIA, to allow prospective contractors to assess their privacy and security capabilities. This approach is considered particularly useful for small and medium-sized organizations. The questions can be made very specific, which makes it easier for smaller contractors to respond. Also, the questions can be designed for specific types of organization and to address specific risks associated with the particular contract.

There are a number of areas that should be considered in determining a contractor's information privacy and security capability. The following are some of the key factors.

The contractor's operational context, including

- the number of staff, including students and volunteers,

- the use of subcontractors, including subcontractors that work off-site,
- the number of locations in which the contractor operates and the location of the facilities used by the contractor (especially locations outside Alberta),
- the contractor's IT system,
- the contractor's business continuity planning, and
- the privacy legislation applicable to the contractor.

The contractor's privacy framework, including

- the position of the contractor's privacy officer within the organization's reporting structure,
- the contractor's information privacy and security policies (including training requirements, confidentiality provisions, and penalties for breach of organizational policies),
- the contractor's program for training staff on privacy,
- the contractor's practices with respect to the collection of personal information (including notification, obtaining consent where applicable), as well as processes used to limit the use and disclosure of personal information to authorized purposes,
- the contractor's ability to provide access to an individual's personal information,
- verification procedures used by the contractor to ensure the accuracy of information,
- the contractor's ability to correct personal information in its records and to track disclosures, and
- protocols for breaches of privacy or security.

The contractor's general ability to safeguard physical and electronic records from unauthorized access and duplication, and from perils such as theft, computer hacking, fire, flood, power interruption, to provide backup and off-site storage, and to manage record retention and disposal in a secure manner. These capabilities may be assessed through a review of the following areas of the contractor's operations.

- IT security (especially important if the contractor is authorized to input data directly or to access the public body's IT system), including provisions to control access (for example, role-based access, user ID and password controls), barrier technology (for example, firewalls, virus protection), data transmission technology, and use of access logs and audit trails,
- physical security of buildings, record storage, work areas, and office equipment (for example, fax machines, photocopiers, computers), and

- administrative security, especially in the management of human resources, including practices relating to recruitment, ongoing training in privacy and security, and termination.

Public bodies may also need to address the protection of personal information in relation to the specific service provider by other means. Contract clauses that address specific risks will be an important part of that process. Chapter 6 provides a number of model contract clauses developed for this purpose.

If the proposed contract presents a high level of risk – especially if there is a need for assurance that a contractor has the capacity to comply with contractual obligations – the public body may need to conduct a full-scale PIA. If the contract is awarded, the public body may need to consider contractual clauses to address specific risks identified during the assessment process. Chapter 6 provides model contractual clauses.

Related sections of this Guide	Chapter
▪ Fee-for-service contracts	2.5
▪ Privacy Impact Assessment (PIA)	5.4
▪ Drafting the contract: Protection of privacy	6.3; esp. cl. Bb–Gg.1

5.6 Organization of Records for Alternative Service Delivery

A public body that proposes to implement an alternative form of service delivery, for example, by outsourcing or privatization, will need to conduct an inventory of program records affected by the proposed arrangement. The inventory should include the records held by staff currently responsible for program delivery. It is likely that program staff have official records in their offices, as well as working files. After the implementation of the proposed arrangement, many of these staff may no longer be involved in the program, so a plan should be put in place to organize the affected records. The plan should include

- an inventory of the locations where the affected records may be held,
- an inventory of the staff who may have affected records (official records, working files, email, etc.),
- a plan and time frame for the retrieval of records from various locations, and from staff who will not be involved with the program after outsourcing,
- a plan to rationalize the records to
    - eliminate duplicate and transitory records,
    - ensure that records are disposed of in accordance with the applicable record retention and disposition schedule, and
    - ensure that the remaining records are organized according to the public body's records management system for easy retrieval by the public body, or by the contractor if such records are transferred to the contractor for program delivery.

5.7 Tendering Process

Communicating requirements

The requirements related to access to information, protection of privacy and records management should be clearly stated in the tendering process documentation. This will ensure that prospective contractors understand their responsibilities and build the cost of compliance into their proposals. It may be helpful to provide a draft contract at this time.

Records under the control of the public body

The tendering documentation should specify the records that the contractor will be expected to collect, create, maintain, or store under the contract, including any of the public body's records that will be transferred to the contractor for the delivery of the contracted services. The tendering documentation should also identify which records will be under the control of the public body. These records will generally be related to the operational requirements of the contracted services.

Records created by contractors in the course of administering their own businesses, such as their financial records and other internal administrative matters, will not normally be under the control of the public body.

Contractor's administrative records

A public body may require a contractor to submit supporting evidence to justify an invoice, or to provide access to records for the purpose of an audit (for example, time sheets of the contractor's staff and receipts for expenses). The public body should restrict the records required from the contractor to those necessary to support payment and accountability.

The contractor should be required to sever any extraneous information before submission, including business information of the contractor and personal information of the contractor's employees.

For example:

- A time sheet may contain information relating to the contractor's work on other projects, as well as personal information of the contractor's staff, such as employees' personal identification numbers, holidays, sick days and other time off, home addresses and phone numbers.
- Employees' credit card numbers and loyalty program numbers may appear on receipts for airline tickets and hotel bills. Hotel bills may also include an employee's home address and vehicle licence plate number.
- A credit card statement submitted as proof of payment is likely to include the individual's credit limit, home address, credit card number, and information regarding purchases not related to the project.

The public body should not collect extraneous information for the following reasons:

- collection of personal information that is not necessary for the purpose of an operating program or activity may not be authorized under the FOIP Act,
- if such information is collected, the public body will have to sever the information (or conduct third party consultation) if the records are subject to a FOIP request,
- the public body may be held responsible if there is a privacy breach relating to the personal information.

The contractor should be advised at the outset of the contracting process that the severing process may involve administrative costs.

The following specification may be included in the tendering documentation:

Model Specification A

> The contractor may be required to submit supporting documents to substantiate billings in a manner specified by the Minister. Without limiting the generality of the foregoing, the contractor may be required to remove information not required to substantiate the billing, in a manner specified by the Minister and at the contractor's expense, before submitting the information to the Minister.

Records management

Any special conditions relating to the management of records that may add to the contractor's costs should be identified. Examples of such conditions include requirements to store and process data in Alberta, to segregate the public body's records, to provide special security measures, and special arrangements for the disposal of records.

Protection of personal information

In some contracts, the collection and handling of personal information constitutes part of the services to be provided. In these cases, the tendering documentation should describe the privacy protection requirements that the contractor will be expected to observe (for example, training requirements).

For example:

Model Specification B

> The contractor will meet the following standards for all personal information the contractor has access to, collects, uses, discloses, or destroys as a consequence of carrying out obligations under the contract: [specify requirements that may affect the ability of a contractor to provide services, the manner in which services will be provided, or the costs of the services].

Alternatively, it may be helpful to provide a draft contract.

If handling personal information is a major part of the services to be provided, the prospective contractor should be required to include in the response to the tendering documentation how the contractor intends to meet the privacy

obligations under the FOIP Act. This may be achieved through the requirement of a complete PIA, or Part A of the PIA, or an assessment of the contractor's information privacy and security capabilities. The following specification may be included in the tendering documentation:

Model Specification C

> The *Freedom of Information and Protection of Privacy Act* requires the protection of the privacy of individuals whose personal information may be involved in meeting contract requirements. The contractor will be required to protect personal information that is accessible to the contractor or collected under this contract. The contractor must include in its response to this tender document [choose one of the following, as applicable:
>
> - a Privacy Impact Assessment in accordance with Guidelines issued by the Office of the Information and Privacy Commissioner,
> - Part A of the Privacy Impact Assessment in accordance with Guidelines issued by the Office of the Information and Privacy Commissioner, or
> - a plan to describe how the above requirements will be met]
>
> to indicate how it intends to meet the privacy obligations.

Access to information

A prospective contractor responding to tendering documentation should be informed of the contractor's obligations in the process of responding to a FOIP request for records in the custody of the contractor.

For example:

Model Specification D

> Where the contractor must maintain records specified in this tender document that remain under the Minister's control, the records and information are governed by the *Freedom of Information and Protection of Privacy Act*.
>
> If the Minister receives a request for access to any of these records, it will be the contractor's responsibility to provide the records to the Minister, at the contractor's expense. The contractor must provide the records to [position title, name of the public body] within __ calendar days from notification by [name of official].

This specification is similar to Model Clause Rr in Chapter 6.

If the public body has arranged to assist the contractor with the cost of handling large-scale FOIP requests, the above clause would need to be revised to reflect that arrangement.

Access to tender submissions

It is important to inform prospective contractors that, because of the access provisions of the FOIP Act, public bodies cannot guarantee complete

confidentiality for any record. However, prospective contractors should be advised that, if a FOIP request is made for their submissions, they may be given an opportunity to comment on the disclosure of records before a decision is made by the public body. As well, a number of exceptions outlined in the Act may be applicable, including section 16 (third party business information), and section 17 (unreasonable invasion of personal privacy). The tendering documentation should contain a specification similar to the following:

Model Specification E

All records submitted to the Minister become the property of the Minister and are governed by the access and privacy provisions of the *Freedom of Information and Protection of Privacy Act*. The records will not be returned after the selection process is completed.

While the *Freedom of Information and Protection of Privacy Act* allows persons a right of access to records in the custody or under the control of the Minister, the Act also prohibits the Minister from disclosing information that would significantly harm business interests or would be an unreasonable invasion of the personal privacy of a third party.

If the Minister receives a request under the *Freedom of Information and Protection of Privacy Act* for access to records or information in the bidder's submission, the bidder will be given a notice allowing it to consent to disclosure, or to explain why the disclosure would significantly harm the bidder's business interests or would be an unreasonable invasion of personal privacy. The bidder will bear any costs incurred in responding to this notice.

If it is the policy of the public body to make certain information relating to the contracting process routinely available, this policy should be indicated in the tendering documentation. Such information might include the total value of the contract, the list of potential bidders who received the tender document, the list of those who submitted a proposal, and minutes of the bidders' meeting.

For example:

Model Specification F

All records submitted to the Minister become the property of the Minister and are governed by the access and privacy provisions of the *Freedom of Information and Protection of Privacy Act*. The records will not be returned after the selection process is completed.

The Minister will [**either** release the following information upon request by any interested party **or** post the following information on the website of the Ministry, as applicable] from the submissions of all bidders: [list types of information].

The *Freedom of Information and Protection of Privacy Act* allows persons a right of access to all records in the custody or under the control of the

Minister, including other information contained in a bidder's submission. The Act prohibits the Minister from disclosing information that would significantly harm business interests or would be an unreasonable invasion of personal privacy of a third party.

If the Minister receives a request under the *Freedom of Information and Protection of Privacy Act* for access to records or information in the bidder's submission, the bidder will be given a notice allowing it to consent to disclosure, or to explain why the disclosure would significantly harm the bidder's business interests or would be an unreasonable invasion of personal privacy. The bidder will bear any costs incurred in responding to this notice.

Bidders should be encouraged to identify any part of their submissions that are provided in confidence. Entire records should not be identified as confidential, but if the release of certain information would be harmful to the business interests of prospective contractors, this should be noted in the record itself or in a covering letter.

Model Specification G

Specific records or specific portions of records submitted by a bidder that are identified as confidential will be treated by the Minister as having been supplied in confidence and will not be released unless required by law.

This would clearly establish the bidders' expectations about the records, both to the public body and to the Information and Privacy Commissioner, should there be a review of the public body's refusal to disclose this information in response to a FOIP request.

Rating and evaluation records

The tendering documentation should state that contractor ratings will not normally be disclosed to third parties. They may be released to the contractor that is the subject of the rating at the discretion of the public body. For example:

Model Specification H

Assessment criteria and allocation formulae for this tendering process are public information. Individual assessments of bidders are considered confidential and may be of interest to competitors or other bidders responding to this tendering process. Some individual assessment information will be provided, upon request, to the bidder to whom it relates. Requests for this information by others will be handled in accordance with the *Freedom of Information and Protection of Privacy Act*.

Personal information of contractors' employees and agents

In many cases, tendering documentation may require bidders to provide personal information about their employees and agents; for example, resumés, evaluations and work history. Therefore, a notice to collect personal information similar to

the following should appear in the introductory section of the tendering documentation.

Model Specification I

> The purpose of collecting the personal information that must be provided in response to this tender document is to enable the Minister to ensure the accuracy and reliability of the proposal and to evaluate the bidder's response to this tender document. Authority for this collection is [name of statute and section(s)]. The bidder may contact [name of appropriate officer] at [address and phone number] for answers to any questions about the collection of personal information in this tendering process.

TIP Subject to the necessary modifications, the above specifications E–I may be included in a grant application process.

Retention of unsuccessful tender submissions

The public body should determine how long submissions from unsuccessful bidders will be kept. This information will generally be of no value or interest to the public body within a short time after the contract is awarded. The retention period of unsuccessful bids should be included in the public body's Records Retention and Disposition Schedule. The public body should assess whether and how section 35 of the FOIP Act affects the retention period. A public body that does not include this information in the tendering documentation should be prepared to provide this information to prospective contractors and others upon request.

Approval of fees and charges

If the contractor is authorized to charge a user fee under the contract, the fee may be subject to Government approval. The successful bidder may be required to provide detailed costing information to the public body. The amount of the user fee, or the final contract itself, may not be finalized until the proposed user fee is approved.

Model Specification J

> Where service delivery is delegated to a private-sector organization, the assessment of a service fee or charge may be permitted by agreement. Any proposed user fees included in a proposal that is selected by the Minister may be subject to Government review. The Minister may require the successful contractor to provide detailed costing information in addition to information included in the tender submission, in accordance with the requirements of the department's Senior Financial Officer. Final approval of the contract is subject to the approval of any proposed user fees.

Table 1
Methods of Managing Risk

Area of Risk	Tendering Documentation	Contract Clauses	Ongoing Management of Contract
Collection, use and disclosure of personal information	• Indicate FOIP requirements related to collection, use and disclosure	• Establish collection, use and disclosure criteria	• Establish procedure for authorizing new collection, use or disclosure of personal information • Provide FOIP training to staff collecting and using personal information
Custody and control	• Identify who has custody and control of records created by the contractor	• Identify who has custody and control of specific records • Establish whether contractor can transfer data to others • Specify requirements of subcontractors • Establish procedures for orderly transition	• Monitor compliance with contract
Records storage and access	• Assess financial viability • Specify any restrictions on location of records • Identify requirements for access to records by public body	• Specify limitations on location of records • Establish public body rights to access data centres • Establish irrevocable right of access	• Review regular financial reports • Monitor compliance with contract
Security	• Identify security requirements to safeguard paper and electronic records	• Specify security access procedures • Specify monitoring/audit procedures • Specify procedures relating to personnel replacement	• Monitor compliance with contract and audit security arrangements
Destruction of records	• Reference Records Management Regulation • Specify penalties for wilful destruction	• Set out retention and disposition requirements • Address destruction of information in electronic storage devices	• Monitor compliance with contract • Provide FOIP training to staff managing records
Sensitive information	• Identify additional requirements as needed	• Specify any special requirements	• Monitor compliance with contract • Provide FOIP training to staff handling sensitive information
Monitoring and compliance	• Indicate reporting requirements	• Establish reporting requirements	• Analyze reports

6.
Drafting the Contract

6.1 Overview

The FOIP Act and the RMR apply to records relating to the performance of a contract that are in the custody of the contractor and that are under the control of the contracting public body. The FOIP Act also applies to the collection, use and disclosure of personal information by a contractor acting on behalf of a public body. This is the case regardless of whether or not the contract contains specific clauses relating to the contractor's duties with respect to that legislation (see Chapter 1 for an explanation of how the FOIP Act applies).

However, it is important to establish the obligations of the contractor within the contract for several reasons.

First, a public body is legally responsible for the compliance of its contractors with the requirements of the Act and the contract is a means of ensuring compliance.

Second, the FOIP Act is an Act of general application; it sets out a number of general principles that apply to a very broad range of programs and services. The contract allows the public body to provide clarity with respect to its understanding of how the Act applies within the specific circumstances of the matter to be governed by the contract.

Third, the contract allows public bodies to specify adherence to policies and best practices that may not be required under the Act but have been adopted as standard for government operations.

Finally, the contracting process provides an opportunity to address matters that are not addressed in the FOIP Act, but which are necessary to ensure effective management of matters relating to the contractor's obligations, such as the monitoring of performance.

For example, the FOIP Act provides that the head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction (section 38). The contract allows the contracting public body to establish exactly what reasonable security arrangements the contractor must have in place and provides a mechanism for the public body to ensure compliance by the contractor.

The contract should, where applicable, contain the FOIP and records management requirements that were in the tendering documentation. The contract may also include clauses that allow the public body to monitor performance during the life of the contract to ensure compliance with the FOIP requirements and the RMR.

This chapter of the guide presents model clauses relating to:

- records management,

- protection of privacy,
- access to information,
- monitoring compliance, and
- jurisdiction.

Some of these clauses work in conjunction with other related clauses, and cannot be used in isolation. For example, Model Clause N, which requires a contractor to keep a log of records disposition, must be accompanied by a clause that addresses situations in which a contractor must not dispose of records related to the contracted service.

How these elements are addressed in a particular contract will depend on a range of factors, including, for example, the roles and responsibilities of the government body and the contractor respectively, the amount and sensitivity of personal information involved, whether the contractor is from Alberta or outside Alberta, and whether the personal information will be processed or stored outside Alberta.

The model contract clauses provided in this chapter are examples only and are limited to access to information, privacy and records management. They do not constitute complete contractual requirements. Existing standard clauses may provide adequate protection in certain cases. Legal advice should be sought on any clauses to be used in particular contracts.

Where the word "Minister" is used, it may be appropriate to replace it with the name of a corporate public body that is not headed by a Minister. The word "agreement" or other similar term can be substituted for the word "contract."

Where the term "contractor" is used, this may apply to any person that has entered into a contract with the public body, including an individual, a partnership, a corporation, a non-profit organization, a public body or another government.

This chapter presents model contract clauses for a range of situations. In a number of cases, two or more separate options are provided (for example Model Clauses G, G.1 and G.2). In some other cases, a model clause includes two or more internal options. If a clause on the subject is needed, the public body should choose the option that is most appropriate in the circumstances.

6.2 Records Management

When drafting the contract, it is critically important to consider the issue of custody and control of records, since this will determine which records fall within the scope of the FOIP Act and the RMR (see Chapter 1 for a discussion of custody and control). The contract must clearly define the records that are in the custody or under the control of the public body and how these records are to be managed over time.

The contractor should be required to manage records under the public body's control according to the policies established under the RMR. The public body's

Senior Records Officer (SRO) should be involved in establishing terms and conditions in a contract for the management of records, retention periods for records, and the conditions governing how records will be stored, disposed of or destroyed.

Where appropriate, contracts should specify

- the definition of a record as it is understood in the contract,
- the types of information and records the contractor is expected to collect, create, maintain, or store for the public body while performing the contract,
- the types of records transferred to the contractor,
- the public body's rights of control and ownership of the records,
- the conditions for maintaining these records (for example, access, control, confidentiality and security, retention, or disposition or destruction),
- the record retention periods and the conditions governing the disposition of records, and
- the basis on which the public body will access records in the custody of the contractor for the purposes of monitoring the contractor's operations (for example, on-site inspection or transfer of the records to the public body).

Definition of "record"

The contract may simply refer to the FOIP Act. Under this option, the contract would not have to be changed if the definition of "record" in the FOIP Act is amended.

Model Clause A

> In this contract, "record" means record as defined in the *Freedom of Information and Protection Privacy Act*, as may be amended from time to time.

Alternatively, if the records involved belong to specific categories, the contract may also specify those categories. For example, the contract may specify that both paper and electronic records are subject to the contract.

Model Clause B

> In this contract, "record" means a record of information in any form, including [list types of records].

Records collected, created, maintained, or stored

If the contract requires the contractor to collect, create, maintain, or store specific types of records, consideration should be given to defining them in the contract. For example:

Model Clause C

> Under this contract, the contractor will collect, create, maintain, or store the following types of records: [list types of records].

Transfer of records and conditions of management

In some contracts, custody of certain records may be transferred from the public body to the contractor, with the public body maintaining control of the records. In such cases, the contract should identify the records that are to be transferred and conditions regarding the management of these records. For example:

Model Clause D

> Under this contract, the following records will be provided by the Minister to the contractor for the delivery of the program or services under this contract: [list types of records]. The contractor must maintain these records in the same organization and under the same conditions as they have been maintained by the Minister, unless specifically directed otherwise by the Minister in writing.

OR

Model Clause D.1

> Under this contract, the contractor must maintain all records in a usable, organized form according to any conditions or standards established by the Minister and appended to this contract.

Control of records

Unless the intent is for the contractor to have both custody and control of the records, the public body should establish in the contract that any record transferred, collected, created, maintained, or stored by the contractor on behalf of the public body remains under the control of the public body and is subject to the FOIP Act.

Model Clause E

> Under this contract, all records transferred to the contractor by the Minister or collected, created, maintained, or stored by the contractor in the performance of the contractor's duties under this contract, except for the contractor's records [list types of records, such as administrative, accounting and human resources records], remain under the control of the Minister and are subject to the *Freedom of Information and Protection of Privacy Act*.

A separate clause would be required for records that are subject to the *Health Information Act*.

Records not under the control of the public body

In some cases, it may be beneficial to specify the records that are not under the control of the public body. For example:

Model Clause F

> The following types of records are deemed to be the sole property of the contractor and under the control of the contractor: [list types of records].

A public body cannot evade its responsibilities under the FOIP Act by saying that it does not have control of records. However, the clause above could be used to make it clear that business records of a contractor that are unrelated to the contract are not in the custody or under the control of the public body.

Ownership of records

The FOIP Act and the RMR apply to records in the custody or under the control of the public body but do not deal with ownership. However, most contracts for services will also address ownership of information in records produced under the contract. This is one way for the public body to exert control over the records produced under the contract and to protect the government's investment.

The following three sample clauses may be considered:

Model Clause G

> The contractor acknowledges that all [or specified] documents, surveys, plans, reports, examinations, analyses, master plates for a final report, and any and all other materials related to the services provided under this contract are the sole property of the Minister. They must be given to the Minister immediately upon request or when the contract ends, whichever occurs first.

OR

Model Clause G.1

> All technical information, inventions, methods, and processes conceived or developed or first actually reduced to practice in carrying out this contract are the sole property of the Minister and must be fully and properly disclosed in writing to the Minister by the contractor. The contractor may not, without the written consent of the Minister, divulge or use such technical information, inventions, methods, or processes other than in carrying out the services under this contract.

OR

Model Clause G.2

> Unless otherwise indicated by the Minister in a notice, the copyright to all material prepared by the contractor under this contract belongs to the Government of Alberta. Such material is to be delivered to the Minister upon completion of the project or as otherwise specified in this contract.

Segregation of records

In some cases, especially where sensitive personal information is transferred, collected, created, used, or stored, the public body may require the contractor to maintain those records separately from other business records. For example:

Model Clause H

> The contractor must keep separate from all its other records and information all personal information transferred to it by the Minister or collected, created, maintained, or stored under this contract.

Access by the public body

The public body must ensure that it is able to have access to records in the custody of the contractor that are deemed to be under the control of the public body. One method of doing this is to include a clause to ensure that the public body has a right of access to the records at any time. For example:

Model Clause I

> The contractor will provide [specify types of records] to the Minister according to the following schedule: [provide details].

OR

Model Clause I.1

> The contractor will provide to the Minister, at the contractor's expense, any and all records required to be collected, created, maintained and stored under this contract within __ calendar days of notification by [position title].

OR

Model Clause I.2

> The contractor will allow the Minister to inspect or review [specify types of records] at the request of the Minister within __ calendar days of notification by [position title].

In addition, the public body may include a clause to ensure that access will not be affected in the case of a contract dispute with the contractor:

Model Clause J

> Notwithstanding any dispute between the parties, the contractor will continue to provide the Minister with access to the records in accordance with the terms of this contract.

Retention and disposition of records

The RMR requires the deputy head of a public body to ensure that there is a record retention and disposition schedule for all records under the control of the public body. This requirement applies to records in the custody of the contractor but under control of the public body. To ensure the Minister retains control over the disposition of the records, the contract should contain a clause similar to the following:

Model Clause K

> The records under the control of the Minister in this contract are the sole property of the Minister and are to be
>
> **EITHER**
>
> retained and disposed of according to the conditions of the attached record retention and disposition schedule.

OR

delivered to the Minister at the contractor's expense at the request of the Minister upon the termination or expiry of the contract, whichever occurs first.

OR

disposed of in accordance with the record retention and disposition schedule attached to the contract.

In some cases, it may be beneficial to all the parties concerned for a public body to transfer certain information to the contractor for the contractor's use at the conclusion of the contract. Although the information may be within the custody of the contractor, transfer of information for the contractor's own purposes would be a disclosure under the FOIP Act. If the public body is legally authorized to disclose the information, and determines that a transfer of information is appropriate in the circumstances, the contract should specify the terms under which the information is disclosed.

For example, personal information may be disclosed with the consent of the individual the information is about (under section 40(1)(d)). If disclosure is authorized by virtue of consent, the contract should specify who will be responsible for obtaining the individual's consent and consequences for failure to obtain proper consent. To ensure that the Minister retains full discretion to determine whether a transfer of information is appropriate, the contractual provision should state that the Minister may withhold approval of a request for disclosure for any reason. The following clause may be considered:

Model Clause L

Despite clause __ [i.e. clause concerning disposition of records], the Minister may approve the retention by the contractor of [specify the records or information to be retained, including details of personal information and the purpose for which that personal information will be used]. The Minister may withhold approval for any reason and without providing explanation.
If the Minister approves the retention of the specified records or information, the contractor must obtain the individual's consent, in a manner specified by the Minister, for the public body to disclose the individual's personal information to the contractor in the contractor's capacity as an entity providing services on its own behalf. The contractor shall retain evidence of the consent to disclosure in a manner specified by the Minister.

[The public body must specify consequences for failure to obtain proper consent, e.g. notification to the individual whose consent should have been obtained.]

If a record retention clause is used in the contract, a complementary clause relating to transitory records should be included. The Government's policy on

transitory records is set out in *Transitory Records Retention and Disposition Schedule* produced by the Records and Information Management Branch, Service Alberta. It should be noted that, once a contractor has been advised that a FOIP request has been received, the contractor cannot destroy any records that may be related to the request, including transitory records. The following clause may be considered to address transitory records:

Model Clause M

> In this contract, a transitory record means a record containing information of temporary value that does not have some future administrative, financial, legal, research, or historical value to the government.
>
> Transitory records as defined under this contract may be disposed of when they are no longer required, unless the Minister advises otherwise. Where permitted, destruction of transitory records must be done according to the rules and regulations of the Government of Alberta, as may be amended from time to time.

In cases where a contractor is delivering services to clients on behalf of a public body, it is likely that the contractor will have primary responsibility relating to the retention and disposition of records in accordance with the public body's directions. The public body may want the contractor to track the disposition of the records to ensure that the contractor discharges the public body's duties relating to disposition, particularly where the records involve sensitive information. For example:

Model Clause N

> The contractor must maintain a log of the disposal of any records that are under the control of the Minister and that have been authorized to be disposed of under this contract. The log must contain at least the following information and must be provided to the Minister immediately upon request by the Minister:
>
> (a) the particulars of the records that were disposed of (e.g. file name, file number, date(s) of the records),
> (b) format of the record (e.g. paper, electronic),
> (c) date of disposition,
> (d) method of disposition, and
> (e) name of the person who carried out the disposition.

Notification prior to record destruction

As a safeguard against unlawful destruction of records, the public body should consider whether notification of destruction should be required (even when destruction is allowed under the contract). This notification would allow the public body to have the assurance that only records that should be destroyed are destroyed. This is especially important when contracts are of a lengthy duration.

A contract clause similar to the following could be used to establish the notice requirement:

Model Clause O

In addition to the above specifications or retention period, the contractor must receive the Minister's prior written approval for destruction of records, except for transitory records. The contractor must notify [position title, name of the public body] in writing at least ___ days prior to the scheduled destruction. The contractor must notify the Minister once the approved destruction has taken place.

6.3 Protection of Privacy

Under Part 2 of the FOIP Act, the head of each public body must protect individual privacy by complying with sections 33 to 42 of the Act. Therefore, if the contract involves the collection, use or disclosure of personal information for a public body, clauses must be included in the contract to ensure that contractors handling the personal information meet those privacy obligations.

Contracts must clearly state the requirements imposed by the FOIP Act on the public body, and assumed by the contractor, for collecting, compiling, ensuring the accuracy of, protecting, using, disclosing, providing access to, correcting, and disposing of personal information. If a contract involves only some of these activities, the contract should include only the relevant requirements.

If a contract will permit the use of subcontractors and agents, the contract must ensure that the obligation to protect personal information in a manner consistent with the requirements of the FOIP Act is also required of the subcontractor and the subcontractor's employees and agents.

The FOIP Act states that personal information may be collected only when specific authority for the collection exists. Therefore, it is essential, before entering into a contract, to make sure that the public body has the legal authority to collect and use personal information for the purpose of the program or service. This will normally be done by consulting with the program manager and the public body's FOIP Coordinator.

Where a contractor is collecting personal information on behalf of a public body and also on its own behalf (for example, when a public body and an organization are each providing services, such as training, to the same client), the collection of personal information required for these separate purposes may be governed by the FOIP Act and other privacy legislation. In some cases, it may be necessary to manage the personal information for each purpose separately (see Model Clause H – segregation of records). In other cases, it may be possible to manage elements of the personal information (for example, client contact information) in a single information system. This may have advantages for clients in terms of integrated service. However, each party must comply with the legislation governing the protection of the personal information, including consent requirements.

For example, a public body may want to permit an organization to use the personal information for its own purposes. The public body may permit such use only if the public body is authorized to disclose the personal information to the organization under section 40(1), for example, with the individual's consent. In

these situations involving common clients, it will be necessary to analyze the flow of information, and a Privacy Impact Assessment may be required. It may also be helpful to append an information-sharing agreement to the contract.

The Government of Alberta's draft *Policy for Protection of Personal Information in Information Technology Outsource Contracts* also requires a public body to undertake certain steps and include specific contractual provisions for the protection of personal information, unless the personal information is restricted exclusively to business contact information and the personal information is being stored only in Alberta. The requirements are as follows.

- The public body must conduct an adequate risk assessment, in the pre-contractual stage, that specifically addresses the requirements under the FOIP Act, the RMR, as well as any other business implications, and must complete a Privacy Impact Assessment (PIA).
- Requests for Proposal (RFPs), solicitation records, bid evaluations and any ensuing contracts must address identified risks to privacy, regardless of the jurisdiction where the personal information is kept.
- Contracts must specify that records containing personal information collected, used, disclosed, or stored on behalf of public bodies will be stored within Alberta, or, if that is not feasible, within Canada. Decisions to permit the storage of personal information outside Alberta should only be made after careful consideration of the issues and risks associated with the protection of personal information, and in consultation with the Office of the Corporate Chief Information Officer and with the Office of the Information and Privacy Commissioner.
- Contracts should specify the contractor's obligations to protect personal information, including conditions for collection, use and disclosure of personal information, location of the information security and confidentiality measures, and retention and disposition of records.

In summary, the public body should consider including clauses in the contract that cover the following matters:

- conditions under which personal information may be collected, used or disclosed on behalf of the public body;
- practices related to the protection of privacy by employees, agents, and subcontractors of the contractor;
- responsibilities for maintaining the accuracy and completeness of personal information and for correcting personal information;
- any limits or conditions related to data matching;
- any restrictions on the location of the personal information;
- the ability of the public body to audit or inspect the contractor's records, systems and facilities;

- responsibilities for reporting breaches of privacy or requests for personal information; and
- consequences for breach of the contract.

Definition of "personal information"

Contracts should include a definition of "personal information" under the FOIP Act. For example:

Model Clause P

> In this contract, "personal information" means personal information as defined in the *Freedom of Information and Protection of Privacy Act*, as may be amended from time to time.

Responsibilities of the contractor for its employees, agents and subcontractors

The contractor has the overall responsibility for ensuring that its employees, agents and subcontractors adhere to the terms of the contract, including requirements to protect personal information under the control of the public body.

Particular care should be taken with respect to subcontractors or agents that are located or have ties outside Canada, as this could result in personal information being accessed by a foreign jurisdiction. A public body should assess the risk and consider contract measures to mitigate the risk, such as prohibiting the contractor from using subcontractors or agents, giving the public body the right to approve any subcontractor or agent, or requiring the contractor to obtain the public body's approval for any proposed change to a subcontractor or agent identified in the contractor's tender, proposal or other submission.

Employees, agents and subcontractors that are responsible for the performance of the contract and whose duties involve personal information must receive information or training respecting the contractor's obligation to act in a manner consistent with the FOIP Act. The information or training must be appropriate to the nature of the personal information and sufficient to ensure the contractor has the ability to act in a manner consistent with the applicable provisions of the Act.

Should the public body wish to impose additional obligations, it may include a term in the contract requiring employees, agents and subcontractors to attend specific FOIP training.

Model Clause R

> The contractor is responsible for ensuring that its employees, agents and subcontractors are aware of and understand the requirements of the FOIP Act as it relates to this contract [training requirements may be specified] before the employees, agents or subcontractors perform duties that involve personal information under the control of the Minister.

The public body may want the contractor to submit a Privacy Impact Assessment or another form of assessment of the contractor's information privacy and

security capability, if the contract involves sensitive personal information. (Further information on these processes can be found in Chapter 5.) The public body may want the contractor to apply a similar standard in subcontracting:

Model Clause S

> Should the contractor engage the services of a subcontractor to perform activities that would involve personal information under the control of the Minister, the contractor must verify the ability of the prospective subcontractor to protect the privacy and security of the affected information, in a manner specified by the Minister, before awarding the subcontract. The contractor must supply a record of such verification to the Minister upon request by the Minister.

Collection of personal information

Prior to entering into a contract involving the collection of personal information, it is important to ensure that the public body has the authority to collect the personal information under section 33 of the FOIP Act. To ensure that the contractor does not place the public body in breach of the Act, the contract should contain a clause similar to the following:

Model Clause T

> The contractor may not collect personal information for the Minister pursuant to this contract, unless the collection is specifically authorized under the contract or expressly authorized in writing by the Minister prior to the collection.

Purpose of collection

The contract should specify the purposes for which the contractor may collect personal information under the contract and the type of information that may be collected. For example:

Model Clause U

> Unless otherwise expressly authorized in writing by the Minister, the contractor may collect personal information on behalf of the Minister only for the following purposes: [specify purposes].
> The type of personal information to be collected by the contractor is limited to: [specify type(s)].

A similar clause should be considered when the contractor is required under the contract to compile a record containing personal information.

Direct collection

Section 34 of the FOIP Act states that personal information must be collected directly from the individual the information is about (except in limited circumstances identified in the Act) and that the individual must be advised of

- the purpose of the collection;

- the legal authority for collection; and
- the contact information for someone able to respond to questions about the collection.

The contract should include a clause similar to the following:

Model Clause V

> Where personal information is collected for the Minister, the contractor must collect the information directly from the individual the information is about and must notify the individual of
>
> (a) the purpose for which the information is being collected;
> (b) the specific legal authority for the collection; and
> (c) the title, business address, and business telephone number of an officer or employee of the Minister who can answer the individual's questions about the collection.
>
> Notification must be given before or at the time of collection [time and manner may be specified].

In addition to the requirements for notice, where the contractor is required to collect information from individuals in person at their place of residence or by telephone, the following clauses should be considered:

Model Clause W

> When collecting personal information from individuals in person at their place of residence, the contractor's employees must carry a letter provided by the Minister confirming that the personal information is being collected on behalf of the Minister, and carry picture identification in a format and manner approved by the Minister. A copy of the letter provided by the Minister must be presented to the individual upon request.

OR

Model Clause W.1

> When collecting personal information from individuals by telephone, the contractor's employees must inform the individual of the name and telephone number of a contact person within the Minister's department who can confirm the purposes for which the information is being collected on behalf of the Minister.

Indirect collection

If the contractor will be collecting personal information indirectly from a third party, this authority should be stated in the contract. For example:

Model Clause Y

> The contractor is authorized to collect the following types of personal information: [specify]. The specified personal information may be collected from the following third parties: [specify]. Collection of the personal

information from a source other than the individual the information is about is authorized by [cite appropriate paragraph of section 34(1) of the FOIP Act].

Accuracy and completeness

If an individual's personal information will be used by a public body to make a decision that directly affects the individual, section 35 of the FOIP Act requires the public body to make every effort to ensure that the information is accurate and complete. If section 35 applies to the activities under the contract, a clause similar to the following should be included:

Model Clause Z

The contractor will make every reasonable effort to ensure that personal information that will be or is intended to be used to make a decision that directly affects an individual is both complete and accurate.

When necessary, specific conditions to ensure accuracy and completeness should be stated. For example, the public body may supply the contractor with regular data updates and require the contractor to update its own records accordingly. Alternatively, the contractor may be required to update the information at specified time intervals either directly from the affected individuals, or indirectly from other sources if the public body has the authority to collect the information indirectly from a third party.

Correction

Section 36 of the FOIP Act gives individuals the right to request a correction to their personal information. The following clauses may be considered to ensure that the contractor will correct the information if the public body determines that a correction is necessary.

Model Clause Aa

The contractor acknowledges that individuals or their representatives have the right to request that the Minister correct personal information that the contractor may have either received from the public body or collected or created about an individual. The contractor must make any correction or annotation required by the Minister within 5 working days of receiving notice and direction to do so by the Minister.

At the direction of the Minister, the contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to the Minister, the contractor disclosed the information subject to correction or annotation.

AND

Model Clause Aa.1

If the contractor receives a request under the FOIP Act for correction of personal information from a person other than the Minister, the contractor must immediately advise the person to make the request to the Minister unless the Minister has directed the contractor to make the type of correction requested. [Specify here any type of correction that the Minister directs the contractor to make under this contract.]

Some requests for correction of personal information will be routine requests that do not fall under the FOIP Act, for example, a notice of a change of address.

Protection of personal information

Section 38 of the FOIP Act states that the public body must protect personal information by making reasonable security arrangements. If sensitive personal information or significant amounts of personal information are handled by the contractor, or if particular standards are required, a description of the standards that the contractor must adhere to (for example, information security plans, disaster recover plans) should be attached to the contract.

A clause relating to disaster recovery should address the costs associated with recovering personal information affected by the disaster, and notification to the Minister.

Model Clause Bb

The contractor must protect personal information in its custody that is subject to this contract by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, disposal, and disaster. Specific measures include [state specific measures for physical, personnel and information technology security, including measures applicable to disaster recovery].

Personnel standards

The contract may require the contractor to have appropriate human resource standards in place. For example, the contractor may be required to provide information privacy and security training to its employees (see Model Clauses R and S). The contractor should also be required to restrict access to personal information to only those employees who require the information to perform the contractor's responsibilities under the contract. The following clause should be considered:

Model Clause Cc

The contractor must restrict access to records containing personal information under the control of the Minister to only those persons who are authorized to use the information in the performance of their duties pursuant to this contract and only if the information is necessary for the performances of those duties. Access by those persons must be limited to the types of personal information necessary for the performance of this contract.

The contractor's employees may also be required to execute an undertaking of confidentiality. The following clause may be considered:

Model Clause Dd

> Before allowing an employee to have access to any personal information, the contractor must ensure that each employee signs an undertaking of confidentiality. The undertaking must cover all personal information the employee may become aware of in carrying out this contract and must include the employee's consent to the disclosure of the undertaking to the Minister. The undertaking is to be maintained on file by the contractor for the duration of the contract and for ___ years after completion of the contract unless otherwise specified in writing by the Minister, and is to be disclosed to the Minister upon request.

Physical standards

The following model clause may be considered to address the physical security of the premises and the equipment where the information is stored:

Model Clause Ee

> The contractor must maintain the security of the information transferred or collected, maintained, or stored by the contractor under this contract. The following physical measures [specify measures, e.g. fire-proof and water-proof locked cabinets, security zones, locked rooms, controlled access to the premises] and information technology security measures [specify measures, e.g. controlled computer access, authentication of system users, barrier technology, communications security] must be used to provide security. The Minister may alter the security requirements during the term of the contract.

The Government of Alberta has a longstanding draft *Policy for Protection of Personal Information in Information Technology Outsource Contracts*, which requires records containing personal information be stored in Canada, preferably in Alberta. The contract should contain a clause similar to the following:

Model Clause Ff

> The contractor must not process, store or transfer any personal information under this contract beyond the boundaries of Alberta [or Canada] without the prior written consent of the Minister.

If the information should be processed or stored only in a particular building because it has the necessary security features, or in a particular location because of concern regarding the potential impact of extra-provincial legislation, the following clause may be considered:

Model Clause Gg

> The contractor will process and store personal information under this contract only at [specify address]. [If off-site backup storage is required, specify here]. The contractor will store back-up information under this contract at [specify address].

AND

Model Clause Gg.1

If the contractor wishes to change the location for the processing or storage of the information specified in clause ___, the contractor must provide ___ days of advance notice to the Minister of the proposed new location. The Minister may undertake an assessment of the potential impact on information privacy and security that may result from the change, or require the contractor to prepare such an assessment in a manner specified by the Minister. The contractor may be required to pay for the cost of the assessment, whether the assessment is prepared by the Minister or the contractor. The Minister may refuse to accept the change of location, or may agree with the proposed change of location subject to the inclusion of additional information privacy and security measures as the Minister deems necessary.

Use and disclosure of personal information

Sections 39 to 42 of the FOIP Act govern the use and disclosure of personal information. Contracts should contain a clause similar to the following:

Model Clause Hh

The contractor must not, either directly or indirectly, use or disclose personal information transferred to or collected, created, maintained, or stored by the contractor under this contract except for the following purposes necessary for performing the services provided by the contractor under this contract: [state purposes]. Any use or disclosure for any purpose other than those stated in this contract must have prior express written authorization from the Minister. This prohibition survives this contract.

OR

Model Clause Hh.1

The contractor must ensure that no use or disclosure may be made of the personal information transferred to or collected, created, maintained or stored by the contractor under this contract for any purpose other than what is needed to carry out this contract, unless the use or disclosure is specifically authorized under the contract or expressly approved in writing by the Minister prior to the use or disclosure. This prohibition survives this contract.

Demands for disclosure from a foreign jurisdiction require special consideration. At the same time, there is some uncertainty about the law in this area; the legal relationship between Alberta privacy legislation and privacy legislation of other jurisdictions has not been tested in a court of law. A recent amendment to the FOIP Act prohibits disclosure of personal information in response to a subpoena, warrant or order from a court that does not have jurisdiction in Alberta. Intentionally disclosing personal information in contravention of this provision is an offence, and subject to a penalty up to $500,000.

Contracts should contain provisions requiring the contractor to notify the Minister of any demand made to the contractor for disclosure of personal information. For example:

Model Clause Ii

> The contractor undertakes that, if it receives a demand for disclosure of personal information it has received or collected, created, maintained, or stored for the Minister under this contract, whether the request is from a person, a government other than Alberta, a non-government organization, a court of law, or from any other source, and the disclosure is not for a purpose authorized under the contract, the contractor
>
> (a) must require that any demand be made in writing setting out the authority of the person making the demand;
> (b) must immediately advise the Minister of the demand made to the contractor and forward a copy of the demand to the Minister; and
> (c) must not disclose the information unless otherwise directed by the Minister.

A contract should also address the contractor's obligation when responding to a review by Alberta's Information and Privacy Commissioner, or another similar officer in Canada. The contract should include a provision requiring the contractor to notify the Minister of the review, and to provide the Minister a copy of the original access request (if applicable), any response to the request and any correspondence with the Commissioner or other official. For example:

Model Clause Jj

> The contractor agrees that, if the personal information in its custody under this contract is the subject of a review by an information and privacy commissioner in the contractor's jurisdiction (e.g. a requester appeals the contractor's refusal to provide access to the personal information), the contractor must immediately notify the Minister. The contractor must provide a copy of the original request for information, any records responsive to the request in its custody, any response to the request, and any correspondence with or submissions to the information and privacy commissioner at least __ days prior to the submission so that the Minister may make a submission or provide suggested changes to the contractor.
>
> The contractor also acknowledges that the Minister reserves the right to participate as an interested party in a proceeding of the information and privacy commissioner on such a matter and will provide a copy of all notices from the information and privacy commissioner respecting the review.

Record of disclosures

The public body may wish the contractor to keep a record of all disclosures of the personal information in the contractor's custody under the contract. In addition, the public body may require the contractor to be able to produce a record of persons who have had access to the personal information (a record of access to

computer system files is often called an "audit trail"). This record may be of particular importance when sensitive personal information is involved. The following clause may be considered:

Model Clause Kk

The contractor must maintain a log, in a form satisfactory to the Minister, of the disclosure of any personal information that has been transferred to or collected, created, maintained, or stored by the contractor under this contract and has been authorized to be disclosed under this contract. At a minimum, the log must contain the following information:

(a) the particulars of the information disclosed (e.g. file name, file number, date);
(b) format of the record (e.g. paper, electronic);
(c) name and contact information of person to whom the information was disclosed;
(d) date of disclosure;
(e) authorization for disclosure;
(f) method of transmission; and
(g) name of the person who made the disclosure.

The log must be provided to the Minister immediately upon request.

AND

Model Clause Kk.1

The contractor must maintain an audit trail of access to the personal information that has been transferred to or collected, created, maintained, or stored by the contractor under this contract. The audit trail information must be provided to the Minister immediately upon request by the Minister.

Data matching

Some contracts may involve data matching as part of the contract. If so, the contract should include a clause similar to the following:

Model Clause Ll

For the purposes of this contract, data matching is the comparison of personal information obtained from different sources, including both electronic and paper-based formats, for the purpose of making decisions about the person to whom the data pertains. The contractor is permitted to carry out data matching under this contract only for the following purposes and in the following manner: [specify purposes and manner].

Disposition of records at the termination of the contract

Records management, retention and disposition are discussed in detail in section 6.2. In addition to the model clauses considered in that section, the public body should include requirements for the disposition of records (consistent with the public body's obligations respecting retention under section 35(b) of the FOIP

Act) upon the expiry or termination of the contract, and where applicable, during the life of the contract (for example, when electronic equipment is being upgraded prior to the termination of the contract). The following clause may be considered:

Model Clause Mm

> At the expiry or termination of the contract, or at such time as the Minister may direct, the contractor must do any or all of the following with respect to records required by the Minister:
>
> (a) return to the Minister all original records transferred to or collected, created, maintained, or stored by the contractor in relation to this contract;
> (b) destroy all copies (including electronic copies) of records transferred to or collected, created, maintained, or stored by the contractor in relation to this contract in the manner specified by the Minister, and provide confirmation of the destruction to the Minister in a manner specified by the Minister; and
> (c) wipe the hard drive used for the storage of information in electronic format and otherwise destroy the information in a manner specified by the Minister, and provide confirmation of the destruction to the Minister in a manner specified by the Minister.
>
> In the event that any record or part of a record transferred to or collected, created, maintained or stored by the contractor in relation to this contract is located at a future date, the contractor must immediately notify the Minister that the record or part of a record has been found and return, destroy or dispose of the record or part of a record in a manner specified by the Minister. This obligation survives this contract.

6.4 FOIP Access to Information Requests

The contract should address access by the public body to records and information that relate to the contract and that are in the custody of the contractor. The contract must ensure that the public body can comply with the access provisions of the FOIP Act. The public body should consider including

- a general clause stating that all records transferred or collected, maintained or stored by the contractor under this contract remain under the control of the public body for the purposes of the FOIP Act;
- clauses dealing with requests for access to records made under the FOIP Act;
- a statement regarding offences and penalties for altering, falsifying, concealing, or destroying records, or directing another person to do so; and
- conditions of storage of information (including media format, data and file specification), disaster recovery, and a business resumption plan.

General clause

The following general clause pertaining to the FOIP Act can be useful in setting the stage for subsequent, more detailed descriptions of the contractor's obligations. However, the public body should not rely exclusively on a general

clause as it is unlikely to be effective if a dispute arises. Therefore, the contract needs to deal with the details of what is required of the contractor regarding an access request.

Model Clause Nn

> The contractor acknowledges that the *Freedom of Information and Protection of Privacy Act* applies to all information and records transferred to or collected, created, maintained, or stored by the contractor under this contract.

Responding to FOIP requests

The records in the custody of a contractor may be the subject of a FOIP request if they are under the control of the public body. It is important that the contract clearly state the responsibilities of both the public body and the contractor in dealing with access requests. For example:

Model Clause Oo

> Records and information transferred to or collected, created, maintained, or stored by the contractor for the Minister under this contract are subject to the access and privacy provisions of the *Freedom of Information and Protection of Privacy Act*. If the Minister receives a request for any records or information that are in the contractor's custody, it will be the contractor's responsibility to provide the records [or copies of the records, as the case may be], at the contractor's expense. The contractor must provide them to the Minister [pursuant to the Minister's direction] within __ calendar days from notification by [name of the official].

Large-scale or complex FOIP requests may involve a considerable financial burden to the contractor. If the public body has made arrangements to assist with the contractor's costs, the above clause should be revised to specify the arrangements.

The contract should also address the responsibilities of the contractor in the event that the contractor receives a FOIP access request directly from the requester. For example:

Model Clause Pp

> If a contractor receives a request for access under the FOIP Act for records in the custody of the contractor as a result of this contract but under the control of the public body, the contractor must
>
> (a) immediately advise the requester to make the request to the Minister;
> (b) immediately advise the Minister of the request made to the contractor and forward any copy of the request to the Minister; and
> (c) must not disclose the information in the records unless otherwise directed by the Minister.

6.5 Monitoring Compliance

Section 38 of the FOIP Act specifically places a duty upon the head of a public body to protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, or destruction. Also, the public body must ensure that it is capable of responding to any FOIP request and to inquiries from the Information and Privacy Commissioner.

The public body should consider setting up processes to allow the public body to demonstrate that it is complying with the Act. The extent of these processes will depend on the scope of the services covered by the contract and the duration of the contract. Some processes to consider are:

- requirements for the contractor to provide regular reports on compliance, and
- on-site audits or evaluations of compliance.

The following models clauses may be considered:

Model Clause Qq

> In addition to any other rights of inspection or audit the Minister may have under this contract or under statute, the Minister, a person authorized by the Minister, or the Auditor General of Alberta, may, at any reasonable time and on reasonable notice to the contractor, inspect and evaluate the contractor's compliance with the privacy, security and information management requirements under this contract through any or all of the following:
>
> (a) on-site visit,
> (b) observation of the performance of the services in progress,
> (c) access to records and the ability to make copies of the records,
> (d) oral or written communications or with any clients, employees, agents, or subcontractors of the contractor.

OR

Model Clause Qq.1

> The contractor will prepare a procedure in a manner specified by the Minister to monitor the compliance of the contractor and the contractor's agents and subcontractors with respect to the information management, privacy and security requirements under this contract, and provide a written report on the monitoring in a manner and at a time specified by the Minister.

AND/OR

Model Clause Rr

> The contractor must review the Privacy Impact Assessment [or other similar document] at least once every __ months. The contractor must indicate in writing that there are no material or substantive changes to the Assessment, or identify material changes that may affect the privacy, security or information management of the records in the custody of the contractor under this contract. Without limiting the generality of the foregoing, such material changes may

relate to changes to IT systems, administrative procedures, the contractor's privacy organizational framework, subcontractors, and agents.

OR

Model Clause Rr.1

The contractor will notify the Minister in writing immediately of any material changes to the contractor's operation that might have an adverse effect on the privacy, security and information management of the records in the custody of the contractor under this contract.

6.6 Notification of Breach of Privacy

The contractor must be required to notify the public body immediately when it anticipates or becomes aware of an occurrence of breach of privacy. For example:

Model Clause Ss

In the event that the contractor anticipates a breach of privacy or becomes aware of a breach relating to the personal information transferred, collected, maintained, or stored by the contractor under this contract, the contractor must immediately notify the Minister in writing of the following, to the extent known:

(a) the nature of the information that was breached (type and date of the information, name(s) of the person(s) whose information is affected);
(b) when the breach occurred;
(c) how the breach occurred;
(d) who was responsible for the breach;
(e) what steps the contractor has taken to mitigate the matter; and
(f) what measures the contractor has taken to prevent reoccurrence.

Consequences of breach

In addition to the fines outlined in section 6.7 for offences under the FOIP Act, a contract may provide for a genuine pre-estimate of damages to be awarded against the contractor for breach of a term of the contract, particularly for a breach involving personal information. Such a clause should be given serious consideration where there is a possibility that the personal information involved in the contract may be subject to a request for access from a foreign jurisdiction. The existence of the possibility of substantial damages may act as a deterrent against the unauthorized disclosure of the information by the contractor, its employees, agents, or subcontractors to the foreign jurisdiction. Other consequences may include exercising rights against a letter of credit, notice by the contractor to an affected third party, or suspension or termination of the contract.

The public body may also wish to consider a general clause regarding consequences upon breach of the privacy provisions of the FOIP Act by the contractor:

Model Clause Tt

> Should there be any use or disclosure of the information by the contractor, its employees, agents, or subcontractors contrary to this contract, the Minister may
>
> (a) terminate or suspend the contract immediately;
> (b) demand immediate return of all records in the custody or control of the contractor at the expense of the contractor;
> (c) require that the contractor issue notice, at its own expense, to any third party whose information was improperly used or disclosed; or
> (d) take any other action that the Minister, in his sole discretion, considers appropriate.

6.7 Offences and Penalties

Section 92(1) of the FOIP Act contains several offences and penalties. It is an offence to, among other things, wilfully

- alter, falsify, or conceal any record, or direct another person to do so, with the intent to evade a request for access to the record,
- destroy any records subject to the FOIP Act, or direct another person to do so, with the intent to evade a request for access to the records;
- collect, use, or disclose personal information in contravention of Part 2 of the FOIP Act; or
- gain or attempt to gain access to personal information in contravention of the FOIP Act.

The penalty for these offences is a fine of up to $10,000.

Contracting documents should clearly state that destroying records to evade providing access to them is an offence under the FOIP Act. For example:

Model Clause Uu

> The contractor shall notify subcontractors and employees that section 92 of the *Freedom of Information and Protection of Privacy Act* specifies that a person who wilfully alters, falsifies or conceals any record, or who wilfully destroys any record that is governed by the Act or directs another person to do so with the intent to evade a request for access to records, is guilty of an offence and is liable to a fine of not more than $10,000.

AND

Model Clause Vv

> The contractor shall notify subcontractors and employees that section 92 of the *Freedom of Information and Protection of Privacy Act* specifies that a person who wilfully collects, uses, or discloses personal information in contravention of Part 2 of the Act or gains or attempts to gain access to such personal information in violation of the Act, is guilty of an offence and is liable to a fine of not more than $10,000.

6.8 Applicable Law

Model Clause Ww

The contract should contain a provision establishing the jurisdiction of the law that governs the contract. For example:

> This contract is governed by the laws in force in the Province of Alberta, and all matters arising under this contract shall be heard exclusively by the courts of the Province of Alberta.

6.9 General Contractual Clauses with FOIP Implications

The purpose of the model clauses in this chapter are to ensure that a public body continues to meet its obligations under the FOIP Act when contracting out a service. The clauses are limited to the collection, use and disclosure of personal information, the security of the personal information, and access to information in the custody of a public body.

The FOIP Act may also have implications for other general contractual matters, such as

- an assignment of the contract (for example, in the case of a corporate buy-out or merger);
- subcontracting;
- employee security or background checks; and
- impending litigation.

Assignment and subcontracting

A corporate buy-out or merger involving the contractor may create a potential conflict of interest, or may introduce unanticipated information privacy and security considerations. This may include issues such as different corporate privacy frameworks and culture and the impact of extra-provincial privacy legislation. A general contractual clause addressing the possibility of a buy-out or merger may include a requirement for the contractor to provide a Privacy Impact Assessment or a similar assessment to the Minister upon any request by the contractor to assign the contract.

For similar reasons, contract clauses concerning subcontracting may include a requirement for the contractor to perform a Privacy Impact Assessment and obtain approval from the Minister before engaging a subcontractor or agent. A contractor may also be required to specify in a subcontract or agency contract that all records transferred to or collected, created, maintained, or stored by the subcontractor in performing services on behalf of the contractor remain under the control of the Minister and are subject to the FOIP Act.

Employee security checks

It may be appropriate to require the contractor to screen employees who will have access to the personal information. Any security requirement should be based on an assessment of risk of unauthorized collection, use, disclosure and destruction

of personal information and any other relevant circumstances, including the sensitivity of the personal information.

It may be appropriate to require a contractor to obtain a Canadian Police Certificate for employees that will be collecting information directly from or about children, or collecting information in other similar sensitive circumstances.

Consideration needs to be given to the level of security screening that will be appropriate in the circumstances, as well as what results will be required.

Impending litigation

Litigation imposes specific obligations with regard to record retention; these obligations are similar to the obligations that arise when a public body receives a FOIP request. A contract should address the responsibilities of the contractor where a contractor becomes aware that there is a reasonable possibility of impending litigation in relation to the performance of services under the contract.

Appendix 1
Checklist for Contract Managers

Preliminary Planning

☐ What kind of contract or agreement is involved and are there any specific access or privacy issues associated with this type of contract?

For further information see

- 2.2 Purchase agreements for the acquisition of goods
- 2.3 Rental agreements and leases for business machines
- 2.4 Software licensing agreements
- 2.5 Fee-for-service contracts
- 2.6 Contracting for service delivery
- 2.7 Privatization
- 2.8 Public–private partnerships (P3s)
- 2.10 Joint service delivery agreements
- 2.11 Grant agreements
- 2.12 Agreements where the public body is the service provider

☐ What operational records will the contractor have to collect, create, maintain, or store?

For further information see

- 6.2 Records management – Records collected, created, maintained, or stored

☐ Will the contract involve records or information that are subject to the FOIP Act?

For further information see

- 1.2 Key concepts – What is subject to the Act; Exclusions

☐ If the contract involves the collection of personal information for the public body, what is the authority to collect that information?

For further information see

- 6.3 Protection of privacy

☐ If the contract involves collection of personal information for the public body from third parties, is indirect collection for the purpose of the contract authorized under the FOIP Act?

For further information see

- 2.10 Joint service delivery agreements
- 4.6 Use and retention of information about common clients
- 6.3 Protection of privacy – Indirect collection

☐ If the contract involves sharing personal information with another public body or a private-sector organization, what is the authority to disclose that information, and what is the authority of the other entity to collect and use that information?

For further information see

- 2.9 Information-sharing agreements
- 2.10 Joint service delivery agreements
- 4.6 Use and retention of information about common clients

☐ Is the contract likely to involve any recognized privacy issues?

For further information see

- 4.2 Processing or storage of personal information outside Alberta
- 4.3 IT outsourcing contracts
- 4.4 Contracts involving sensitive personal information
- 4.5 Contracting with a member of a professional regulatory organization
- 4.6 Use and retention of information about common clients

☐ Does the contract involve any recognized access issues?

For further information see

- 4.7 Corporate restructuring, mergers and buy-outs
- 4.8 Costs of large-scale or complex FOIP requests
- 4.9 Confidential business information

☐ Is the contract or agreement likely to involve a party or parties that are subject to other access to information or privacy legislation that may need to be considered?

For further information see

- 3.2 Other Alberta legislation
- 3.3 Federal legislation
- 3.4 United States legislation

☐ Is the contract likely to involve a party operating in a jurisdiction that has no privacy legislation?

For further information see

- 3.6 Jurisdictions with no privacy legislation

Pre-Contracting

☐ For a major business initiative involving the collection, use and disclosure of personal information, does the business case include a review of the privacy issues?

For further information see

- 5.2 Business case

☐ Does the project involve a significant information and communications technology component (including new software)?

For further information see

- 5.3 Privacy planning tool for IT projects

☐ If the contract is for IT outsourcing, what policies and procedures need to be addressed at the pre-contracting stage of the project?

For further information see

- 4.3 IT outsourcing contracts

- 5.3 Privacy planning tool for IT projects
- 5.4 Privacy Impact Assessment (PIA)

☐ If the contract involves sensitive personal information, how will the risks be mitigated?

For further information see

- 3.5 Extra-territorial application of foreign law
- 3.6 Jurisdictions with no privacy legislation
- 4.4 Contracts involving sensitive personal information
- 5.4 Privacy Impact Assessment (PIA)
- 5.5 Assessing privacy capabilities of smaller contractors

☐ If the contract involves data matching or data sharing by or for the public body, is a Privacy Impact Assessment needed?

For further information see

- 5.4 Privacy Impact Assessment (PIA)
- 5.5 Assessing privacy capabilities of smaller contractors
- 6.3 Protection of privacy – Data matching

☐ How could changes to the ownership structure of the contractor affect the contract, particularly if the contract is long-term?

For further information see

- 4.7 Corporate restructuring, mergers and buy-outs
- 6.9 General contractual clauses with FOIP implications – Assignments

☐ How will the potential costs of a large-scale or complex FOIP request for records held by the contractor be addressed?

For further information see

- 4.8 Costs of large-scale or complex FOIP requests

☐ If the contract is for outsourcing, how will this affect the right of access to information, as well as routine disclosure and active dissemination processes?

For further information see

- 2.6 Contracting for service delivery
- 4.3 IT outsourcing contracts
- 5.2 Business case
- Appendix 2, Disclosure of Contracting Records

☐ What records will the contractor be required to collect, create, maintain or store for the purposes of ensuring the accountability of the public body for a program or service associated with the public body?

For further information see

- 2.5 Fee-for-service contracts
- 2.6 Contracting for service delivery
- 2.7 Privatization
- 2.8 Public–private partnerships (P3s)
- 2.10 Joint service delivery agreements
- 2.12 Agreements where the public body is the service provider

- ☐ What requirements respecting records management, especially retention and disposition of records (including any plan for the alienation of records) need to be included in the tendering documentation and the contract?

  For further information see
  - 2.7 Privatization
  - 6.2 Records management – Retention and disposition of records

Tendering Process

- ☐ Does the tendering document state which specific records the contractor will be expected to collect, create, maintain, or store for the public body?

  For further information see
  - 5.7 Tendering process – Records under the control of the public body

- ☐ Does the tendering document make it clear which records will be in the custody or under the control of the public body and which will remain in the custody or under the control of the contractor?

  For further information see
  - 1.2 Key concepts – Custody and control
  - 5.7 Tendering process – Records under the control of the public body

- ☐ Does the tendering document specify which records will be required for operational and financial accountability?

  For further information see
  - 5.7 Tendering process – Contractor's administrative records

- ☐ Does the tendering document identify any special conditions relating to the storage of records that may add to the contractor's costs?

  For further information see
  - 2.6 Contracting for service delivery
  - 4.7 Corporate restructuring, mergers and buy-outs
  - 5.4 Privacy Impact Assessment (PIA)
  - 5.7 Tendering process – Records management

- ☐ If special security measures or restrictions on the location of data are required, does the tendering document specify what they are?

  For further information see
  - 4.2 Processing or storage of personal information outside Alberta
  - 4.3 IT outsourcing contracts
  - 5.7 Tendering process – Records management

- ☐ Does the tendering document describe the privacy protection requirements that the contractor will be obliged to meet? Or, if handling personal information is a major part of the contract, does the tendering document provide for the prospective contractor to submit a plan for addressing privacy protection requirements under the FOIP Act?

  For further information see
  - 4.4 Contracts involving sensitive personal information
  - 5.4 Privacy Impact Assessment (PIA)

- 5.7 Tendering process – Protection of personal information

☐ Does the tendering document include information on the responsibilities of the contractor in the event of a FOIP request for records that are subject to the FOIP Act?

For further information see

- 5.7 Tendering process – Access to information

☐ Does the tendering document inform prospective contractors that absolute confidentiality cannot be guaranteed for any submission? Does the tendering document advise prospective contractors to identify those parts of their submissions which they believe should be held in confidence?

For further information see

- 2.8 Public–private partnerships
- 5.7 Tendering process – Access to tender submissions

☐ If it is intended to make contract prices public, is this stated in the tendering document?

For further information see

- 5.7 Tendering process – Access to tender submissions

☐ Does the tendering document include information on access to contractor ratings?

For further information see

- 5.7 Tendering process – Rating and evaluation records

☐ Does the tendering document indicate that any user fee the contractor may be authorized to charge will be subject to Government approval?

For further information see

- 4.9 Confidential business information
- 5.7 Tendering process – Approval of fees and charges

☐ Does the tendering document include a notice, as required by the FOIP Act, stating the public body's authority to collect personal information contained in submissions (e.g. personal information about the contractor's employees)?

For further information see

- 5.7 Tendering process – Personal information of contractors' employees

The Contract

☐ Has there been consultation with the public body's legal advisors (as well as its FOIP coordinator and SRO, if applicable) regarding the form and structure of the contract to be used, and whether the detailed FOIP provisions should be included in the body of the contract, or in a schedule?

For further information see

- 2.1 Contracts and agreements – Overview
- 6.1 Drafting the contract – Overview

- ☐ Does the contract define the terms "record" and "personal information"? If the contract involves a variety of record types, does the contract define those as well?

  For further information see
  - 6.2 Records management – Definition of "record"
  - 6.3 Protection of privacy – Definition of "personal information"

- ☐ What personal information will the contractor have to collect, create, maintain, or store?

  For further information see
  - 6.2 Records management – Records collected, created, maintained, or stored

- ☐ Does the contract specify the types of information and records the contractor is expected to collect, create, maintain and store?

  For further information see
  - 6.1 Drafting the contract – Overview
  - 6.2 Records management – Records collected, created, maintained, or stored

- ☐ Does the contract state which records are transferred to the contractor and specify standards for their management, including general obligations under the FOIP Act and the RMR? Does the contract include specific conditions for maintaining the records?

  For further information see
  - 6.2 Records management – Transfer of records and conditions of management

- ☐ Does the contract need to include a general clause stating that records created under the contract are subject to the FOIP Act, in addition to detailed clauses relating to matters of access to information and protection of privacy that are relevant to the specific contract?

  For further information see
  - 6.2 Records management – Control of records

- ☐ Does the contract include a general clause respecting conditions that apply to assignment and subcontracting?

  For further information see
  - 6.9 General contractual clauses with FOIP implications

- ☐ Does the contract specify which records of the contractor will be in the custody or under the control of the public body and which will be in the custody or control of the contractor?

  For further information see
  - 1.2 Key concepts – Custody and control
  - 2.7 Privatization
  - 6.2 Records management – Control of records

- 6.2 Records management – Records not under the control of the public body

☐ If the contract involves sensitive personal information, are the terms and conditions adequate in relation to the increased risks? Does the contract specify that the information must be segregated from the contractor's other business records?

For further information see
- 4.4 Contracts involving sensitive personal information
- 6.2 Records management – Segregation of records

☐ If the contract involves sensitive personal information, is there a requirement for employee security checks in the contract?

For further information see
- 4.4 Contracts involving sensitive personal information
- 6.9 General contractual clauses with FOIP implications – Employee security checks

☐ Does the contract provide for the right of the public body to access the records?

For further information see
- 6.2 Records management – Access by the public body

☐ Does the contract specify requirements respecting retention and disposition of records? Does the contract include conditions governing the disposition of records, including transitory records?

For further information see
- 2.7 Privatization
- 6.2 Records management – Retention and disposition of records

☐ Does the contract include a requirement for the contractor to provide notification of destruction to the public body?

For further information see
- 6.2 Records management – Notification prior to record destruction

☐ Does the contract include a general requirement with respect to the retention of records for the purposes of litigation?

For further information see
- 6.9 General contractual clauses with FOIP implications

☐ Does the contract identify the responsibilities of the contractor with respect to requests for access under the Act?

For further information see
- 2.10 Joint service delivery agreements
- 6.4 FOIP access to information requests

- ☐ If the contract involves personal information, does it specifically state the requirements of the Act with regard to all of the following that are relevant to the contract?
  - collection of personal information,
  - notice for direct collection,
  - authority for indirect collection,
  - specific conditions for ensuring accuracy,
  - the right of an individual to request correction of his or her own personal information,
  - specific standards for the protection of personal information,
  - restrictions on the use and disclosure of personal information,
  - record retention periods, and
  - final disposition of the records

  For further information see
  - 6.3 Protection of privacy

- ☐ Does the contract make it clear that the requirements of the FOIP Act apply to everyone working under the contract? Are requirements relating to employees of the contractor, such as FOIP training, included in the contract?

  For further information see
  - 1.2 Key concepts – Application of the FOIP Act to contractors
  - 6.3 Protection of privacy – Responsibilities of the contractor for its employees, agents and subcontractors

- ☐ If the contract involves the sharing of personal information with another public body or private-sector organization, does the contract specify the purposes for which the other entity may use or further disclose the information, how the information must be protected and disposed of, and how the contract will be monitored?

  For further information see
  - 2.9 Information-sharing agreements
  - 4.5 Use and retention of information about common clients
  - 6.3 Protection of privacy – Protection of personal information

- ☐ Does the contract specify requirements for disaster recovery?

  For further information see
  - 6.3 Protection of privacy – Protection of personal information

- ☐ If data matching or data linkage is part of the contract, does the contract specify terms and conditions?

  For further information see
  - 6.3 Protection of privacy – Data matching

- ☐ Does the contract include clauses allowing the monitoring of performance to ensure compliance with the FOIP Act and the Records Management Regulation (RMR)?

  For further information see
  - 6.5 Monitoring compliance

- ☐ Does the contract specify terms of access by the public body for the purposes of monitoring the contractor's operations?

  For further information see
  - 6.5 Monitoring compliance

- ☐ If the contract involves personal information, does the contract specify what the contractor must do in the event of a breach of privacy?

  For further information see
  - 6.6 Notification of breach of privacy

- ☐ Does the contract require the contract to notify subcontractors and employees of offences and penalties under the FOIP Act?

  For further information see
  - 6.7 Offences and penalties

- ☐ Does the contract include information on offences and penalties under the Act?

  For further information see
  - 6.7 Offences and penalties

Appendix 2
Disclosure of Contracting Records

1. Overview

When a request is received for contracting records or for information about the contracting process, the public body should first consider whether it can disclose the information without a FOIP request or whether the requester should make a FOIP request. If the public body would be required to consult with third parties or to sever information in response to a FOIP request, the public body should require the requester to submit a FOIP request. This formal process ensures that the applicant and any third party have the right to request a review of the public body's decision regarding disclosure of the requested information.

An applicant has a right of access to the records in the custody or under the control of a public body, subject to the limited and specific exceptions set out in the Act. There are two types of exceptions – mandatory exceptions and discretionary exceptions.

If a *mandatory* exception applies to the information, the public body has a duty to refuse access. Mandatory exceptions that may apply to information in contracting records include the exceptions for

- disclosure harmful to the business interests of a third party (section 16),
- disclosure harmful to personal privacy (section 17), and
- privileged information of a person other than a public body (section 27(2)).

If a *discretionary* exception applies to the information, the public body may decide whether or not to apply the exception. The more common discretionary exceptions that may relate to information in contracting records include the exceptions for

- confidential evaluations (section 19),
- advice from officials (section 24),
- disclosure harmful to economic or other interests of the government or a public body (section 25), and
- privileged information of a public body (section 27(1)).

All these exceptions, except solicitor–client privilege under section 27(1) of the Act, apply to *information contained in* a record, not the entire *record*.

This Appendix explains the exceptions in the FOIP Act most commonly applied to contracting records. See the FOIP *Guidelines and Practices* manual, published by the Access and Privacy, Service Alberta, for more detailed explanations.

Harms test

A number of exceptions in the FOIP Act provide that a record may not or must not be disclosed if disclosure could reasonably be expected to cause a specified harm. The general test for harm under the FOIP Act is whether there is a reasonable expectation of harm flowing from disclosure of the specific information at issue.

The test, established in *Order 96-003*, has three parts:

- there must be a reasonable expectation of probable harm,
- the harm must constitute damage or detriment and not mere inconvenience, and
- there must be a causal connection between disclosure and the anticipated harm.

For a detailed discussion of the test, see *Practice Note 1*, *Applying "Harms" Tests*, issued by the Office of the Information and Privacy Commissioner.

Consent to disclosure

A public body *must* refuse access to third party information that is subject to the exception for confidential business information (section 16) or the exception for unreasonable invasion of personal privacy (section 17), *unless* the third party consents to disclosure. A public body that is considering giving access to a record that may contain information to which section 16 or section 17 applies must give notice to the third party. The third party may consent to disclosure or make representations to the public body as to why the information should not be disclosed. If the third party consents to disclosure, the public body may not withhold the information unless another exception applies to the information.

Exercise of discretion

Where the Act provides for the exercise of discretion in applying an exception, the public body must be able to show that the records were reviewed, that all the relevant factors were considered and, if the decision is to withhold the information, that there are sound reasons to support the decision. The public body may consult with other public bodies if appropriate.

When exercising discretion a public body should consider

- the general purposes of the Act,
- the wording of the discretionary exception and the interests which the exception attempts to balance,
- whether the applicant's request may be satisfied by severing some information and providing the applicant with as much information as is reasonably practicable,
- the historical practice of the public body with respect to the release of similar types of records,

- the nature of the record and the extent to which the record is significant or sensitive,
- whether disclosure of the information will increase public confidence in the operation of the public body,
- the age of the record,
- whether there is a definite and compelling need to release the record, and
- whether the Commissioner has ruled that similar types of records or information should or should not be disclosed.

(See *Orders 96-017* and *2000-021*.)

Severing

If information is subject to an exception, but that information can reasonably be severed from the record, the applicant has a right of access to the remainder of the record (section 6(2)). This provision for severing does not apply to records to which a legal privilege in section 27(1) or (2) is claimed (*Order 96-017*). The legal privilege must be applied to the entire record

3. Mandatory Exceptions

Disclosure harmful to business interests of a third party (section 16)

Section 16(1) of the FOIP Act creates a mandatory exception for information which, if disclosed, would reveal certain types of third party business information supplied in confidence, and could also result in one or more specified harms.

Section 16(1)(a) to (c) provides a three-part test (*Order 97-013*). The exception applies only if the information meets all three parts of the test.

1. **Disclosure of the information would reveal trade secrets or commercial, financial, labour relations, scientific or technical information of the third party (section 16(1)(a)).**

To meet this part of the test, the disclosure must *reveal* one of the specified types of information. In addition, the information must be proprietary information of the third party. Information of one the specified types may be revealed not only if information is itself disclosed, but if information that is disclosed makes direct reference to one of the specified types of information, or allows the reader to draw an accurate inference about one of the specified types of information.

Section 16(1)(a) does not apply to information that has already been disclosed.

Trade secret, as defined in section 1(s) of the Act, means information, including a formula, pattern, compilation, program, device, product, method, technique or process,

- that is used, or may be used, in business or for a commercial purpose,
- that derives independent economic value, actual or potential, from not being generally known to anyone who can obtain economic value from its disclosure or use,

- that is the subject of reasonable efforts to prevent it from becoming generally known, and
- the disclosure of which would result in significant harm or undue financial loss or gain.

Commercial information means information that relates to the buying, selling, or exchange of merchandise or services (*Order 97-013).* This information includes a contract price, pricing structure and business plan. It also includes third party associations, history, references and insurance policies (*Orders 96-003, 96-013*, *97-003, 99-008* and *2001-021*). An agreement between two business entities may also contain commercial information (*Order 2001-021)*.

Financial information relates to the third party's financial capabilities, assets and liabilities, past or present (*Orders 96-018* and *2001-008*). Financial forecasts, investment strategies, budgets, and profit and loss statements may all be considered financial information.

Labour relations information includes information about relationships within and between workers, working groups and their organizations, as well as between managers, employers and their organizations (*Order 2000-003*).

Scientific information is information exhibiting the principles or methods of science (*Order 2000-017*).

Technical information is information relating to a particular subject, craft or technique (*Order 2000-017*). Examples of technical information include system design specifications and plans for an engineering project.

2. The information was supplied explicitly or implicitly in confidence (section 16(1)(b)).

The Commissioner has indicated that, in order to meet the second part of the test, a third party must, from an objective point of view, have had a reasonable expectation of confidentiality with respect to the information that was supplied. To make this determination, it is necessary to consider whether the information was

- communicated to the public body as confidential and meant to be kept confidential,
- handled in a consistently secure manner by the third party prior to disclosure to the public body,
- not otherwise disclosed or available from sources to which the public has access, or
- prepared for a purpose which would not entail disclosure.

  (*Orders 96-012*, *96-018* and *2000-010.*)

Section 16(1)(b) does not apply to information that is generated jointly through negotiations with the public body (*Order 96-013*). The provision may apply where the information supplied by the contractor to the public body during

negotiations remains relatively unchanged in the agreement, or could be inferred from the agreement (*Order 2000-005*).

If there is a specific provision in the Request for Proposal that states the information will be kept confidential, the Commissioner has considered information supplied in accordance with the Request for Proposal to have been supplied explicitly in confidence. The Commissioner has also stated that, if proposals are required to be submitted in sealed envelopes, confidentiality is implied (*Order 97-013*).

Information supplied by a third party will also be considered to have been supplied in confidence if the public body then supplies that information in confidence to a second public body (*Order 2001-008*).

The Commissioner has accepted as evidence of intended confidentiality statements by the prospective contractor in the proposal or the covering letter that the information supplied is confidential (*Order 96-013*). However, the Commissioner has recommended that public bodies and contractors ensure that their contracts state explicitly whether the parties intend the transaction to be confidential (*Order 2000-009).*

3. Disclosure could reasonably be expected to result in one of the harms specified (section 16(1)(c)).

The third part of the test requires evidence that disclosure can be expected to

- significantly harm the competitive position of the third party,
- interfere significantly with the negotiating position of the third party,
- result in information no longer being available,
- result in undue financial loss or gain to any person or organization, or
- reveal information supplied to a person appointed to resolve a labour relations dispute.

In *Order 96-013,* it was held that a public body intending to withhold information on the basis that disclosure would harm a third party's competitive position or result in financial loss must be able to show that the harm would be "significant" or that the loss would be "undue."

In the context of contracting, the method of the contracting may also be a factor. In *Order 99-008,* it was determined that disclosure of proprietary business information was likely to be more harmful when the contract was awarded on a sole-source basis rather than through a public bidding process.

The exception for third party business information does not apply under certain conditions specified in the Act, including the following:

- if the third party has consented to disclosure of the information (section 16(3)(a); see section 2 of this Appendix on consent to disclosure);

- if an enactment of Alberta or Canada authorizes or requires disclosure (section 16(3)(b));
- if the information relates to a non-arm's length transaction between a public body and another party (section 16(3)(c)).

Disclosure harmful to personal privacy (section 17)

Section 17 of the FOIP Act protects the personal privacy of individuals whose personal information may be the subject of a FOIP request by someone else. The protection is provided through a mandatory exception if disclosure of personal information would be an unreasonable invasion of an individual's privacy.

Section 17(2) sets out the circumstances in which disclosure of personal information is *not* considered an unreasonable invasion of a third party's personal privacy. The following circumstances are particularly relevant to contracting records:

- the third party has consented to the disclosure (section 17(2)(a); see section 2 of this Appendix on consent to disclosure),
- the disclosure reveals financial and other details of a contract to supply goods and services to a public body (section 17(2)(f)),
- the disclosure reveals details of a discretionary benefit of a financial nature granted to the third party by a public body (section 17(2)(h)).

In *Order 2004-014* the Commissioner decided that section 17(2)(f) applied to information in contracting records requested by an applicant. The Commissioner required the public body to disclose financial details of the contract for services between the public body and each of several instructors, including each instructor's hourly rate, total hours, and hours per month, as well as the public body's total financial commitment.

Section 17(4) of the Act identifies cases in which it is presumed that disclosure of personal information would be an unreasonable invasion of an individual's personal privacy. Of particular relevance in the context of contracting records is section 17(4)(d), "the personal information relates to employment or educational history." Proposals submitted in a competitive bidding process may include information about the prospective contractor's employees, including detailed resumés. This personal information would not normally be disclosed to a third party unless the individual consented.

In determining whether a disclosure of personal information constitutes an unreasonable invasion of personal privacy, the public body must consider all relevant circumstances, including those identified in section 17(5) of the Act. The most significant for records relating to contracting is section 17(5)(a), "the disclosure is desirable for the purpose of subjecting the activities of the Government of Alberta or a public body to public scrutiny." In *Order 97-002,* it was held that in order for this provision to take precedence over section 17(4), there must be evidence to demonstrate that the activities of the Government of

Alberta or a public body had been called into question. A finding that section 17(5)(a) was applicable would weigh in favour of disclosure.

Other circumstances may weigh against disclosure, for example:

- the third party will be exposed unfairly to financial or other harm (section 17(5)(e)),
- the personal information has been supplied in confidence (section 17(5)(f)).

Another relevant circumstance, not specifically listed in section 17(5), is whether the personal information may fall within the meaning of section 40(1)(bb.1), which permits disclosure of personal information without the consent of the individual the information is about "if the personal information is information of a type routinely disclosed in a business or professional context, and the disclosure

- is limited to an individual's name and business contact information, including business title, address, telephone number, facsimile number and email address, and
- does not reveal other personal information about the individual or personal information about another individual."

Personal information means "recorded information about an identifiable individual" (section 1(n) of the FOIP Act). Only human beings can have personal information. Corporations are not individuals and their information is not personal information for the purposes of the FOIP Act. The Commissioner has also found that a sole proprietorship is not a natural person and therefore does not have "personal information" (*Order F2002-006*).

Privileged information of a person other than a public body (section 27(2))

Section 27(2) provides that a public body *must* refuse to disclose information subject to legal privilege that relates to a person other than the public body. Public bodies are most likely to have privileged records of a third party if there is a legislated requirement for the third party to provide the information to the public body or if records have been provided to the public body in the course of a dispute resolution process. There are a number of types of legal privilege; those most likely to apply to third parties are solicitor–client privilege and litigation privilege.

A record may be subject to *solicitor–client privilege* if

- the record is a communication between a lawyer and the lawyer's client,
- the communication entails the giving or seeking of legal advice, and
- the record is intended to be confidential (*Order 96-017*).

Legal advice includes a legal opinion about a legal issue, and a course of action, based on legal considerations, regarding a matter with legal implications (*Order 2000-013)*.

A record may be subject to *litigation privilege* if records were created or obtained by a client for the use of the client's lawyer in existing or contemplated litigation. Records may also be subject to this privilege if they were created by a third party, or obtained from a third party on behalf of the client, for the use of the client's lawyer in existing or contemplated litigation.

A public body must refuse access to privileged information of a third party (section 27(2)) unless the third party waives the privilege. Waiver is established when the party entitled to the privilege knows of the existence of the privilege and demonstrates a clear intention to forego the privilege (*Adjudication Order No. 3*). The FOIP Act does not provide for a public body to give notice to a third party whose information is subject to section 27(2). An applicant claiming that a third party has waived privilege has the burden of proof on review.

4. Discretionary Exceptions

Confidential evaluations (section 19(1))

Section 19(1) of the FOIP Act states that a public body *may* refuse to disclose an applicant's personal information that is evaluative or opinion material compiled for the purposes of determining the applicant's suitability, eligibility or qualifications for employment or for the awarding of government contracts or other benefits, where the information is provided explicitly or implicitly in confidence.

The exception may be applied to information that is supplied by the source of the evaluation or opinion, but not to information compiled by the public body. For example, a verbatim transcription or a summary of a reference check for a potential contractor that is supplied in confidence may be excepted from disclosure. However, an analysis of an interview by the public body could not be withheld under this provision.

Section 19(1) applies only when an individual, or an authorized representative, is requesting his or her own personal information.

Advice from officials (section 24)

Section 24 is intended to protect the deliberative process involving officials of the public body or Executive Council members. A public body *may* refuse to disclose information under section 24 if the disclosure could reasonably be expected to reveal a specified class of information. The more commonly used provisions for contracting records are those relating to the following classes of information:

- advice, proposals, recommendations, analyses or policy options developed by or for a public body or a member of the Executive Council (section 24(1)(a));
- consultations or deliberations involving officers or employees of a public body, a member of Executive Council, or the staff of a member of the Executive Council (section 24(1)(b));
- positions, plans, procedures, criteria or instructions developed for the purpose of contractual or other negotiations by or on behalf of the Government of

Alberta or a public body, or considerations that relate to these negotiations (section 24(1)(c)).

The exception applies to information generated during the decision-making process, not the decision itself (*Order 96-012*).

The Commissioner has interpreted section 24(1)(a) strictly, and determined that the list of words after "advice" constitute examples of advice. There is an established three-part test for determining whether advice falls within the scope of the exception (*Order 96-006*). The advice must be

- sought or expected, or be part of the responsibility of a person giving it by virtue of that person's position;
- directed toward taking an action, including making a decision; and
- made to someone who can take or implement the action.

The Commissioner has determined that a statement of fact, without any direction toward action to be taken, does not qualify as advice under section 24(1)(a) (*Order 97-007*). However, factual information may be withheld if it is sufficiently interwoven with other advice, proposals, recommendations, analyses or policy options, and it cannot reasonably be considered separate or distinct (*Order 99-001*). In *Order F2002-002,* it was held that section 24(1)(a) applies to the weight assigned to the criteria for the evaluation of a Request for Proposal and the actual points awarded to each proposal by the public body.

Section 24(1)(b) allows a public body to refuse to disclose information relating to "consultation" or "deliberation" that occurs during a public body's decision-making process. In *Order 96-006,* the Commissioner held that "consultation" occurs when the views of one or more officers or employees are sought as to the appropriateness of particular proposals or suggested actions. "Deliberation" occurs when there is a discussion or consideration by officials of the public body of the reasons for or against an action. The Commissioner also held that the criteria for "advice" apply to section 24(1)(b).

Section 24(1)(c) may apply if disclosure of the information can reasonably be expected to reveal positions, plans, procedures, criteria or instructions which have been developed for the purpose of the public body's negotiations, or considerations that relate to those negotiations. "Consideration" in the context of the contracting situation means the matters taken into account in making decisions about the public body's negotiating positions (*Order 99-013*). The criteria for "advice" also apply to section 24(1)(c).

In applying the exceptions under section 24(1), a public body must ensure that disclosure could reasonably be expected to *reveal* the information. That is, the information must not have been previously disclosed.

If section 24(1) is found to apply, it is necessary then to consider section 24(2), which states that the provision does not apply to certain information, for example, information that is fifteen or more years old.

For further information on these and other exceptions in section 24, see the FOIP *Guidelines and Practices* manual, published by the Access and Privacy, Service Alberta.

Disclosure harmful to economic or other interests of the Government or a public body (section 25)

Section 25(1) of the FOIP Act states that a public body *may* refuse to disclose information if the disclosure could reasonably be expected to harm the economic interest of a public body or the Government of Alberta or the ability of the Government to manage the economy. The exception may apply to the following classes of information:

- trade secrets of a public body or the Government of Alberta;
- financial, commercial, scientific, technical or other information in which a public body or the Government of Alberta has a proprietary interest or a right of use and that has, or is reasonably likely to have, monetary value;
- information the disclosure of which could reasonably be expected to
    - result in financial loss to,
    - prejudice the competitive position of, or
    - interfere with contractual or other negotiations of,

  the Government of Alberta or a public body;
- scientific or technical information obtained through research by an employee of a public body, the disclosure of which could reasonably be expected to deprive the employee or public body of priority of publication.

See the discussion of section 16(1) of the Act in section 3 of this Appendix for definitions of *trade secret*, *financial information*, *commercial information*, *scientific information* and *technical information*.

Section 25(1) permits the head of a public body to exercise discretion to withhold information if harm would result from disclosure. The types of information noted in the section are illustrative only. Section 25(1)(b) allows the exception of "other information" that could reasonably be expected to cause harm to economic interests.

Whatever type of information is involved, a public body that is relying on this exception the public body must reasonably expect that disclosure of the information could harm the economic interest of a public body of the Government of Alberta or the ability of the Government to manage the economy (*Orders 96-013* and *96-016*). See section 2 of this Appendix for a discussion of the harms test.

Privileged information of a public body (section 27(1))

Section 27(1**)** of the Act provides that a public body *may* refuse to disclose information that is subject to any type of legal privilege. In addition, section 27(1) allows a public body to withhold

- information prepared by a public body's lawyer in relation to a matter involving the provision of legal services, and
- information in correspondence between a public body's lawyer and any other person in relation to a matter involving the provision of legal services.

The following are some common examples of records in a contract file that *may* be subject to legal privilege:

- a letter, fax, email or other correspondence to or from the public body's lawyer, including a lawyer at Alberta Justice and Attorney General,
- a lawyer's working papers,
- a communication between employees of a public body quoting written or verbal legal advice given by a lawyer,
- a note documenting legal advice given by a lawyer,
- an invoice or a statement of account from a lawyer that details the services provided by the lawyer,
- information that relates to an existing or contemplated lawsuit against a contractor,
- a record that relates to a public body's investigation of a contractor.

A public body that is considering disclosing privileged information to an applicant should obtain legal advice.

Table 2
Disclosure of Contracting Information

Document	Disclosure Policy		Possible Exceptions	Comments
	Routinely Available	FOIP Request Required		
Requisition	no	Yes	s.24 Advice from officials s.25 Economic interests of government or public body	Definition of requisition sometimes differs among public bodies
Tender documents, including Requests for Quote (RFQ) and Requests for Proposals (RFP)	yes	No	None	May be public documents, or available on request for fee
Bidders invited to tender	yes	No	None	Generally available to public on request
Bidders' meeting minutes, written responses to bidder questions	yes	No	None	Usually disclosed directly to attendees or posted to website
List of bidders who bid	yes	No		Available on request
Bids, proposals, tenders	no	Yes	s.16 Third party business interests s.17 Disclosure harmful to personal privacy	Bottom-line $ amounts should be released
Unit prices	usually not	yes, when no routine release	s.25 Economic interests of government or public body s.16 Third party business interests	Withheld
Evaluation committee's notes, memos, etc.	no	Yes	s.16 Third party business interests s.17 Disclosure harmful to personal privacy s.19 Confidential evaluations s.24 Advice from officials	Usually require severing if disclosed under the FOIP Act
Evaluation of each bid, proposal, tender	no	Yes	s.16 Third party business interests s.17 Disclosure harmful to personal privacy s.19 Confidential evaluations s.24 Advice from officials	Own evaluation may be available to each bidder at discretion of public body
Summary of all evaluations	no	Yes	s.16 Third party business interests s.17 Disclosure harmful to personal privacy s.19 Confidential evaluations s.24 Advice from officials s.25 Economic interests of government or public body	May require severing if disclosed under the FOIP Act
Negotiation information	no	Yes	s.16 Third party business interests s.17 Disclosure harmful to personal privacy s.19 Confidential evaluations s.24 Advice from officials s.25 Economic interests of government or public body	Usually requires severing if disclosed under the FOIP Act

Document	Disclosure Policy		Possible Exceptions	Comments
	Routinely Available	FOIP Request Required		
Recommendation to award	no	yes	s.24 Advice from officials	Usually requires severing if disclosed under the FOIP Act
Signed contract or purchase order	no	Yes	s.16 Third party business interests s.17 Disclosure harmful to personal privacy s.25 Economic interests of government or public body	Generally disclosed with some severing
Bidder's correspondence and responses	no	Yes	s.16 Third party business interests s.17 Disclosure harmful to personal privacy	Usually requires severing if disclosed under the FOIP Act

* NOTE: This chart is a guide showing the example of a typical case. As for all FOIP requests, a review of the particular records requested must be made.

Appendix 3
Records Management Regulation

(Consolidated up to 186/2008)

ALBERTA REGULATION 224/2001

Government Organization Act

RECORDS MANAGEMENT REGULATION

Table of Contents

Interpretation

1(1) In this Regulation,

(a) "Committee" means the Alberta Records Management Committee established under section 2(1);

(b) "department" has the meaning given to it in section 14 of Schedule 11 to the *Government Organization Act*;

(c) "deputy head", in respect of a department, means

(i) the chief officer of the department, or

(ii) if there is more than one chief officer of the department, the chief officer of that part of the department for which he or she is responsible;

(d) "Minister" means the Minister of Service Alberta;

(e) "record" has the meaning given to it in the *Freedom of Information and Protection of Privacy Act*;

(f) "Schedule" means Schedule 1 to the *Freedom of Information and Protection of Privacy Regulation* under the *Freedom of Information and Protection of Privacy Act*.

(2) For the purposes of this Regulation, an agency, board, commission, corporation, office or other body listed in the Schedule is considered to be a department.

AR 224/2001 s1;251/2001;35/2007; 186/2008

Alberta Records Management Committee

2(1) There is established the Alberta Records Management Committee consisting of the persons appointed as members under subsection (3).

(2) On the request of the Minister, nominations must be made in accordance with the following and submitted to the Minister:

(a) 5 people must be nominated by the Department of Service Alberta;

(b) one person must be nominated by the Provincial Archives of Alberta;

(c) one person must be nominated by the Department of Justice;

(d) one person must be nominated by the Department of Finance and Enterprise;

(e) repealed AR 68/2008 s17;

(f) repealed AR 9/2006 s2.

(3) The Minister may appoint as members of the Committee

(a) the persons nominated in accordance with subsection (2), and

(b) any other persons the Minister considers appropriate.

(4) A person nominated under subsection (2)(c) may in writing designate an employee of the Government who is under the administration of the Minister of Justice and Attorney General to attend and act on behalf of the person at one or more meetings of the Committee.

AR 224/2001 s2;9/2006;35/2007; 68/2008

Chair, vice-chair and secretary

3 The Minister must designate a chair, vice-chair and secretary for the Committee from the persons nominated under section 2(2)(a).

AR 224/2001 s3;9/2006

Records management program

4(1) The Minister is responsible for establishing a records management program.

(2) For the purpose of providing the details for the operation of the records management program, the Minister may establish, maintain and promote policies, standards and procedures for the creation, handling, control, organization, retention, maintenance, security, preservation, disposition, alienation and destruction of records in the custody or under the control of departments and for their transfer to the Provincial Archives of Alberta.

Evaluation of program

5 The Committee may evaluate the implementation of the records management program in each department.

Approval of records retention and disposition schedules

6(1) A records retention and disposition schedule and any subsequent amendment to it must be approved by the Committee before it is implemented in the department.

(1.1) The Committee or the secretary of the Committee on the Committee's behalf may set an expiry date for and approve amendments to a records retention and disposition schedule and, where it is no longer required, cancel a records retention and disposition schedule.

(1.2) Notwithstanding subsection (1.1), the secretary of the Committee may not approve an amendment of the type described in section 10(2)(b) or (e) to an approved records retention and disposition schedule of a department.

(2) The Committee may approve records retention and disposition schedules submitted by the secretary of the Committee that are to apply to all departments.

AR 224/2001 s6;9/2006

Advice to the Minister

7 The Committee may provide advice to the Minister relating to the policies, standards and procedures referred to in section 4(2).

Archival appraisal

8 The member of the Committee referred to in section 2(2)(b)

(a) must provide an archival appraisal of each records retention and disposition schedule submitted by a department, and

(b) may provide advice on archival concerns.

Departmental responsibility

9 The deputy head of a department must ensure that records in the custody or under the control of the department are managed in accordance with the policies, standards and procedures established under section 4(2).

Records retention and disposition schedule

10(1) The deputy head of a department must ensure that the department prepares records retention and disposition schedules for all records under the control of the department.

(2) The records retention and disposition schedule must

(a) describe the records under the control of the department,

(b) specify how long the department must keep the records,

(c) specify where the records must be kept,

(d) specify the format in which records must be stored, and

(e) describe what the final disposition of the records will be.

(3) Repealed AR 9/2006 s5.

(4) Records may be disposed of only in accordance with the approved records retention and disposition schedule.

AR 224/2001 s10;9/2006

Destruction of records

11 The deputy head of a department must ensure that records are destroyed only in accordance with policies established under section 4(2).

Repeal

12 The *Records Management Regulation* (AR 57/95) is repealed.

Expiry

13 For the purpose of ensuring that this Regulation is reviewed for ongoing relevancy and necessity, with the option that it may be repassed in its present or an amended form following a review, this Regulation expires on March 31, 2016.

AR 224/2001 s13;9/2006

Appendix 4
Glossary of Terms

Alternative service delivery (ASD) has been described as a process of public sector restructuring that redistributes governance functions by determining appropriate roles for individuals and groups and the most cost-effective way to improve services for clients. ASD encompasses a wide range of activities, arrangements and funding options involving the broader public sector, the private sector and not-for-profit organizations.

Assignment entails the transfer of rights or responsibilities from one person to another (for example, from a contractor to another person). A change in ownership or ownership structure of the contractor may also be considered an assignment.

Business contact information means an individual's name and business contact information, including business title, address, telephone number, facsimile number, and email address (section 40(1)(bb.1) of the FOIP Act).

Commercial activity is defined in the *Personal Information Protection Act* (PIPA, section 56(1)(a)) and in the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA, section 2(1)) to mean any transaction, act or conduct, or any regular course of conduct, that is of a commercial character, and includes the selling, bartering or leasing of membership lists or of donor or other fund-raising lists. The definition of *commercial activity* in PIPA also expressly includes the operation of a private school, an early childhood services program and a private college.

Commissioner. Unless otherwise indicated, references to "the Commissioner" in this Guide mean Alberta's Information and Privacy Commissioner, who is responsible for independent review of decisions and the resolution of complaints made under the FOIP Act, the *Health Information Act* (HIA) and the *Personal Information Protection Act* (PIPA). There are other commissioners in Canada who are responsible for access to the information and privacy legislation of other jurisdictions, including the federal Information Commissioner and the federal Privacy Commissioner.

Common clients. This term, as used in this Guide, means individuals receiving services from more than one public body, considered from the perspective of the public bodies providing those services. For example, a public body that administers a program to provide financial support to persons with low incomes and a public body that administers a program to provide support to persons with disabilities may have common clients.

Common or integrated program or service (section 40(1)(i) of the FOIP Act). A *common* program or service means a single program or service that is delivered by two or more public bodies subject to the FOIP Act. An *integrated* program or service means a program or service with several distinct components, each of

which may be delivered by separate public bodies, but when put together comprise the complete program or service.

Consent. To consent means to agree to something; to give approval or permission for some act or purpose. Consent may either be *express* where it is clearly and unmistakably stated, or *implied*, where consent is inferred from one's conduct, rather than a direct statement. Privacy legislation in Alberta prescribes the manner of consent.

- Under the FOIP Act, disclosure of personal information under sections 39(1)(b) or 40(1)(d) requires consent that specifies to whom the personal information may be disclosed, and how the personal information may be used (section 7, FOIP Regulation).
- Under HIA, disclosure of individually identifying health information to persons other than the individual who is the subject of the information requires *written* or *electronic* consent that includes specific information as outlined in section 34(2)(a) to (f).
- Under PIPA, consent to the collection, use or disclosure of personal information about the individual may be *written* or *oral*, and may be *express*, *implied* or *opt-out*.

Contracting is the process by which a public body enters into a contract enforceable in law where a legal obligation is defined between the public body and another party or parties.

Control. A record is under the *control* of a public body when the public body has the authority to manage the record, including restricting, regulating and administering its use, disclosure or disposition.

Custodian is defined in Alberta's *Health Information Act* to include a regional health authority, the Minister and department of Alberta Health and Wellness, licensed pharmacies, pharmacists, physicians, and other health professionals designated as custodians in the Health Information Regulation.

Custody. A public body has *custody* of a record when the record is in the physical possession of the public body. A record is in the custody of a public body when, for example, it is on the premises of the public body, in active files or in a central filing facility, or in off-site storage. A record is also in the custody of the public body when a record is in use by an employee in an office, at a work site or in a home or vehicle.

Disposition of records is the process of applying record retention and disposition schedules to records. Records disposition includes the transfer of records from government departments to the Alberta Records Centre for interim off-site storage or for destruction upon the expiry of their retention periods; the transfer of records to the Provincial Archives of Alberta for permanent preservation; the alienation of records from the custody and control of government; and the transfer of records for immediate destruction.

Employee, in relation to a public body, includes a person who performs a service for the public body as an appointee, volunteer or student or under a contract or agency relationship with the public body (section 1(e) of the FOIP Act). The Commissioner has defined the term "for" in other provisions of the FOIP Act to mean "on behalf of."

Fee-for-service contract. A fee-for-service contract is used when the Government retains an individual or company to provide a specific service. The *Public Service Act* distinguishes between a contract of employment and a fee-for-service contract in terms of whether an employment relationship exists, which affects matters such as liability. For the purposes of the FOIP Act, the term "employee" includes both an employee who has entered into a contract of employment and a person that has entered into a fee-for-service contract. *See also* **employee**, **personal service contractor**.

Health information means diagnostic, treatment and care information, and registration information that is collected, used or disclosed by custodians. The FOIP Act does not apply to health information that is in the custody or under the control of a custodian. Alberta's *Personal Information Protection Act* (PIPA) does not apply to health information to which the *Health Information Act* applies. PIPA applies to health-related information to which the *Health Information Act* does not apply, such as health-related information in employee records.

HIA is the acronym used to refer to Alberta's *Health Information Act*, which governs the protection of health information held by custodians.

Information-sharing agreement means a written agreement setting out the terms and conditions for the collection of information by one party and disclosure of information by the other party. A party that enters into an information-sharing agreement may collect and disclose information only as permitted by applicable legislation. The elements of an information-sharing agreement normally include a statement of the objectives to be achieved under the information-sharing agreement and provisions specifying the specific personal information involved (i.e. the data elements), the purpose for which the information may be used by the recipient, persons to whom the recipient may disclose the information, the method for transmission, requirements for the protection, retention and disposal of the information, and measures to audit or monitor compliance with the agreement.

Joint service delivery is a coordinated method of delivering services that fall within the mandate of different public bodies, different levels of government and, in some cases, the non-profit sector. *See also* **common or integrated program or service**.

Memorandum of Understanding (MOU) is an agreement between interested parties establishing their respective rights and responsibilities regarding a project and serving as a basis for a future formal contract. In the government context, a Memorandum of Understanding is often used as the final contract between agencies of the Crown and would address all relevant matters.

Organization, as defined in the *Personal Information Protection Act*, includes

- a corporation,
- an unincorporated association,
- a trade union as defined in the *Labour Relations Code*,
- a partnership as defined in the *Partnership Act*, and
- an individual acting in a commercial capacity,

but does not include an individual acting in a personal or domestic capacity (section 1(i)).

Outsourcing is the process by which a public body enters into an agreement with another party (usually the private sector, but sometimes a non-profit organization or another public sector body) to deliver services or carry out operations on behalf of the public body. In these instances, the public body retains the responsibility for the service or the operation and may pay the other party to carry out the government's responsibilities.

Paramountcy. Where two enactments are inconsistent or conflict, the principle of paramountcy helps determine which law will prevail.

Personal information means recorded information about an identifiable individual, including

- the individual's name, home or business address or home or business telephone number,
- the individual's race, national or ethnic origin, colour or religious or political beliefs or associations,
- the individual's age, sex, marital status or family status,
- an identifying number, symbol or other particular assigned to the individual,
- the individual's fingerprints, other biometric information, blood type or inheritable characteristics,
- information about the individual's health and health care history, including information about a physical or mental disability,
- information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given,
- anyone else's opinions about the individual, and
- the individual's personal views or opinions, except if they are about someone else (section 1(n) of the FOIP Act).

Personal service contractor is defined in the *Financial Administration Act* as

- an individual whose services are engaged by the Crown, a Provincial agency or a fund administrator in consideration of the payment of a fee, whether or not the contract for those services is made with that individual or another person, or

- a person who contracts to provide the services of such an individual.

Although the *Financial Administration Act* differentiates between an employee and a personal service contractor, a personal service contractor is considered an employee for the purposes of the FOIP Act.

PIPA is the acronym used to refer to Alberta's *Personal Information Protection Act*, the Act that governs the protection of personal information in the provincially regulated private sector.

PIPEDA is the acronym used to refer to the *Personal Information Protection and Electronic Documents Act* (Canada), the Act that governs the protection of personal information in the federally regulated private sector and in provinces that do not have substantially similar private-sector privacy legislation.

Privacy Impact Assessment (or PIA). A PIA is the detailed consideration, during the planning and implementation of a program or system, of appropriate and effective measures to ensure compliance with Part 2 of the FOIP Act.

Privacy schedule refers to a separate schedule to a contract that sets out requirements relating to the protection of personal information. A privacy schedule is required, as a matter of Government policy, for IT contracts.

Privatization is the process by which a public body ceases to be responsible for a service or carry out an operation and transfers the service or operation to the private or non-profit sector.

Public body is defined in section 1(p) of the FOIP Act to include

- a department, branch or office of the Government of Alberta,
- an agency, board, commission, corporation, office or other body designated as a public body in Schedule 1 of the FOIP Regulation, and
- the offices of the Officers of the Legislature.

For the purposes of this Guide, the term *public body* is limited to the bodies listed above; the Guide does not apply to local public bodies.

Public–private partnership (P3) refers to a contractual agreement between a public body and one or more private or non-profit parties for the provision of goods or services with resources, risks and rewards allocated among the parties (this is not a partnership in law). P3s normally have the following characteristics:

- a long-term contractual arrangement
- a sharing of risks and rewards
- a joint investment
- clearly assigned responsibilities
- a model of delegated authority and control

(Annual Report of the Auditor-General of Alberta, 2003-2004).

Reasonableness. In the context of PIPA, reasonableness is an objective standard based on what a reasonable person would consider appropriate in the circumstances (section 2 of PIPA).

Record means a record of information in any form, and includes notes, images, audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records (section 1(q) of the FOIP Act).

RMR is the acronym used to refer to Alberta's Records Management Regulation established under the *Government Organization Act*.

Sensitive personal information. The FOIP Act does not recognize sensitive personal information a separate class of information. However, the Act has special provisions for certain categories of personal information, including an individual's medical information, personal information in a law enforcement record, an individual's financial information, an individual's educational and employment history, and personal evaluations and character references.

Subcontractor means a person who has contracted with a primary contractor or with another subcontractor to perform a contract.

Transitory record means a record (as defined above) containing information of temporary value that does not have some future administrative, financial, legal, research, or historical value to the government. This would include such records as duplicates, draft documents, working materials, publications, blank forms, and temporary notes that do not have long-term value. *See also* **record**.