7.
PROTECTION OF PRIVACY

Overview

This chapter covers the obligations of public bodies regarding

- the collection, use and disclosure of personal information;
- the accuracy of personal information;
- the retention of personal information;
- the protection of personal information; and
- the right of an individual to request a correction of his or her personal information.

Privacy principles

The *FOIP Act* ensures the protection of informational privacy (the right to exercise control over your own personal information) by establishing rules for the collection, use, disclosure and retention of personal information. The Act also contains rules regarding the accuracy of personal information, and gives individuals the right to request a correction to their personal information in the custody or control of a public body.

Most of the provisions respecting the protection of personal information are found in **Part 2** of the Act; however personal privacy is also considered in **section 17**.

Part 1

Part 1 of the *FOIP Act* provides individuals with a right of access to information, including information about themselves, from public bodies, subject to limited and specific exceptions. One of those exceptions, **section 17**, sets out factors to determine when disclosure of personal information would be an unreasonable invasion of a third party's privacy. These factors comes into play whenever someone other than the individual the information is about, or the individual's authorized representative, makes a request for access to a record containing personal information about a third party.

Personal information, as defined in **section 1(n)**, means recorded information about an *identifiable* individual. It is information that can identify an individual (for example, name, home address, home phone number, e-mail address, ID numbers), and information about an individual (for example, physical description, educational qualifications, blood type). An individual may be identified by their name, where they live, what they do, or as a result of a compilation of information that relates to only to a small number of people (see, for example, *IPC Investigation Report F2004-IR-001*). The definition of personal information does not include information about a sole proprietorship, partnership, unincorporated association or corporation (see *IPC Order F2002-006*).

Part 2

Information about an identifiable individual that is collected must be collected, used, disclosed, secured, and retained only in accordance with the provisions in **Part 2**,

unless the information is outside the scope of the Act (see sections 1.5 and 1.6 of Chapter 1 regarding excluded records and the effect of paramountcy, respectively).

Part 2 requirements are based on internationally accepted fair information practices or principles adopted by the Organization for Economic Cooperation and Development (OECD) in 1982. This set of principles collectively works to establish what is commonly referred to as *privacy protection*. An individual's privacy is protected when the individual is able to decide who to give their information to, is aware of how the information will be used and disclosed, and gives consent to use and disclose the information if appropriate.

Privacy is protected in the *FOIP Act* by

- giving individuals a right of access to their own personal information and the opportunity to request corrections to it;
- collecting personal information only as authorized by law;
- requiring public bodies to collect personal information directly from the individual the information is about, unless the individual, another Act or a regulation under another Act, the Information and Privacy Commissioner, or **section 34(1)(b)** to **(o)** of the *FOIP Act* authorizes collection from someone else;
- requiring public bodies to provide individuals with notice of the authority for the collection, the purposes for which the information is collected and contact information for a person who can explain the collection process in more detail, if required;
- requiring public bodies to ensure that information that will be used to make a decision about an individual is accurate and complete;
- requiring public bodies to retain information used to make decisions affecting an individual for at least one year (unless the public body and the individual agree otherwise) to allow adequate time for the individual to exercise their right of access or correction, if they choose to;
- requiring public bodies to take reasonable security precautions against such risks as unauthorized access, collection, use, disclosure or destruction;
- limiting a public body's use and disclosure of personal information to the purpose for which it was collected, a consistent purpose, another purpose with consent or a purpose set out in the Act;
- further limiting a public body's use and disclosure of personal information to the amount and type necessary to enable the public body to carry out its purpose in a reasonable manner;
- enabling individuals to make complaints to the Commissioner, and empowering the Commissioner to investigate complaints regarding possible collection, use or disclosures in contravention of **Part 2**;
- enabling employees of a public body to disclose to the Commissioner, in good faith, circumstances in which they believe that personal information is being collected, used or disclosed in contravention of **Part 2** (see section 2.9 of Chapter 2);

- requiring each public body to publish a directory of its personal information banks (repositories of personal information that can be searched by name or identifier); and
- providing for fines for individuals of up to $10,000 if they wilfully collect, use or disclose personal information in contravention of **Part 2**, or gain, or attempt to gain, access to personal information in contravention of the Act (among other offences).

The *FOIP Act* does, however, also recognize that public bodies must collect and maintain a variety of personal information for purposes related to direct service delivery to members of the public or for broader public purposes. In some instances, authority to collect, use or disclose personal information is expressly granted in the *FOIP Act*. In others cases, the authority to collect, use of disclose personal information is granted by other enactments of Alberta or Canada.

FOIP Coordinators are advised to take a comprehensive and collaborative view of privacy protection within their public bodies and involve individuals with responsibility for program management, information technology, records and information management, security, human resources and, at times, their legal counsel. FOIP Coordinators should also be aware of other privacy legislation that governs bodies with which they interact. For example, a public body may not be able to collect personal information from a private-sector organization in Alberta if that organization is not authorized to disclose the information under the *Personal Information Protection Act* (PIPA).

Under the *FOIP Act*, public bodies are accountable for adhering to the privacy protection rules established in **Part 2**, and are accountable for ensuring that other organizations acting on behalf of the public body also adhere to these rules. It is in the public body's best interest to ensure that their obligations and requirements under the Act are clearly understood by any contractor or agent and the obligations are clearly communicated in the contractual agreement.

For further information on the application of the Act to the contracting process, see *Managing Contracts under the FOIP Act: A Guide for Government of Alberta Contract Managers and FOIP Coordinators*, published by Access and Privacy, Service Alberta.

7.1 Collection of Personal Information

Authority for collection of personal information

Public bodies cannot collect personal information unless the collection is authorized under **section 33** of the Act. **Section 33** of the Act authorizes the collection of personal information if

- the collection of personal information is expressly authorized by or under an enactment of Alberta or Canada;
- the personal information is collected for the purposes of law enforcement; or
- the personal information relates directly to and is necessary for an operating program or activity of the public body.

Collection occurs when a public body gathers, acquires, receives or obtains personal information. It includes the gathering of information through forms, interviews, questionnaires, surveys, polling, and video surveillance. There is no restriction on how the information is collected. The means of collection may be writing, audio or videotaping, electronic data entry or other means.

Section 33 of the Act states that collection can take place *by* or *for* a public body. A public body is bound by the requirements of the Act whether it conducts its own collection activities or an outside agent carries out the collection on the public body's behalf. This authorization may be either under contract or through an agreement or arrangement with another public body or private organization.

Examples of organizations and individuals that might collect personal information on behalf of a public body include non-profit support groups such as the John Howard Society, school counsellors and various contracted organizations.

When an outside organization or contractor is collecting personal information on behalf of a public body, the public body should have in place a written agreement or contract. This must state how the organization or contractor will meet the requirements of the *FOIP Act* regarding the collection, use, disclosure, security, retention and disposition of the personal information being collected.

Authorized by an enactment

Section 33(a) **Section 33(a)** provides that collection may be expressly authorized by an enactment of Alberta or Canada.

An *enactment* includes an Act or regulation, or any part of an Act or regulation. A municipal bylaw passed under the authority of the *Municipal Government Act* may also be considered an enactment for the purposes of **section 33(a)**. In *IPC Investigation Report F2002-IR-009*, the Investigator found that a municipal bylaw expressly authorized the City to collect criminal record information from applicants for taxi licences.

In some Acts, there are provisions for the collection of certain specific types of personal information. In these cases, the statute both authorizes collection and identifies the personal information that can be collected (e.g. section 65 of the *Post-secondary Learning Act*). More commonly, an Act will authorize a program or activity, and a regulation under that Act will provide detailed authority for collection and sometimes the format in which the information is to be collected. An example of this form of authorization for collection is the *School Act* and the Student Record Regulation. Another model for collection authority is where an Act states that collection of personal information must be in the form prescribed by a regulation under that Act.

If an enactment authorizes a program or activity, but there is no specific authorization for the collection of information for the purposes of the program or activity, a public body cannot rely on the enactment as authority for collection of the information. It is

not sufficient for an enactment to imply an ability to collect personal information (see *IPC Order F2006-004*).

If a particular collection of personal information is not authorized under **section 33(a)**, it might be authorized under **section 33(b)** or **(c)**.

For the purposes of law enforcement

Section 33(b)

Section 33(b) permits the collection of personal information for the purposes of law enforcement. *Law enforcement* is defined in **section 1(h)** of the Act and is discussed in section 4.6 of Chapter 4. It includes policing, administrative investigations, and proceedings that could lead to a penalty or sanction. Any collection of personal information for purposes of law enforcement must meet this definition.

Section 33(b) recognizes that law enforcement agencies must engage in wide-ranging information collection that would not always be allowed under the more restrictive terms of **section 33(c)**. It would be difficult for a law enforcement agency to show, at the moment of collection, how each piece of personal information collected for investigative or enforcement purposes relates directly to or is necessary for the activity under way. Certain investigative methods, such as taking witness statements, might be seriously compromised by limiting the collection of personal information.

In *IPC Investigation Report F2003-IR-005*, the Information and Privacy Commissioner reviewed a Privacy Impact Assessment submitted by a police service regarding video surveillance it intended to use in an area of the city during two periods of highest crime risk. The Commissioner agreed that the police service could collect and use personal information on video for this law enforcement activity, which included the detection and prevention of crime.

If a public body is authorized to collect personal information under this provision, it is also authorized to collect the information indirectly under **section 34(1)(g)**.

For more information on collection for the purposes of law enforcement and about the definition of law enforcement, see FOIP Bulletin No.7: *Law Enforcement*, published by Access and Privacy, Service Alberta.

Relates directly to and is necessary for an operating program or activity

Section 33(c)

Section 33(c) permits a public body to collect personal information when that information relates directly to, and is necessary for, an operating program or activity of the public body.

Relates directly to means that the personal information must have a direct bearing on the program or activity.

Necessary for means that the public body must have a demonstrable need for the information.

An *operating program* is a series of functions designed to carry out all or part of a public body's operations. An *activity* is an individual action designed to assist in carrying out an operating program.

Most often, legislation will give authority for a particular program or activity, without authorizing the collection of specific personal information. Public bodies must then determine the exact elements of personal information which they need to administer a particular program and design collection instruments to obtain this information *and no more* (i.e. the public body must have a "need to know"). Collection is authorized by **section 33(c)** of the Act.

The *FOIP Act* does not permit collection of personal information "just in case" it may have value in the future, the program may be expanded in the future or someone in the public body may ask for the information at some point in the future.

The word *and* in **section 33(c)** (relates directly to and is necessary) is restrictive. The collection must meet both parts of the two-part test in order for the public body to use **section 33(c)** as authority to collect personal information.

For example, if a program provides a particular benefit or service, information will be needed to ensure that an individual is eligible or qualified for that benefit or service. Personal information not related to decision criteria for the particular benefit or service is not required and should not be collected, even though it may be potentially useful to another program in the same public body.

In *IPC Order 98-002*, the Commissioner determined that the case manager making a decision about an individual's claim for compensation had the right to decide what medical information was relevant and necessary to collect but was bound by the *Workers' Compensation Act* in establishing that necessity and relevance. Obtaining an applicant's entire patient file was found to be an improper collection.

In *IPC Investigation Report 99-IR-007*, the Commissioner found that a municipality did not have the authority to collect its Sport Centre's members' home or business telephone numbers or dates of birth since this information was not required for an operating program or activity of the municipality.

In *IPC Investigation Report F2002-IR-010*, the Investigator found that using one questionnaire to collect personal information for two programs risked collecting more personal information than was necessary for the public body's operating program or activity. In this case, the survey was completed by both current and prospective employees, although only one of the programs applied to prospective employees. The survey collected more personal information from the prospective employees than the public body required.

A public body must establish a reasonable basis for deciding that the collection of personal information is necessary and relevant. The City of Calgary Fire Department provided sufficient evidence to show that the sensitive personal information collected during its recruitment process was relevant to job requirements, based on findings from research and potential conflict situations that a firefighter might encounter. (see *IPC Investigation Report F2002-IR-012*).

The manner in which information is collected should be minimally intrusive. Collecting information about employees through surreptitious keystroke-logging technology did not meet the "necessary" requirement since there was other less

intrusive means of collecting information about employee productivity (see *IPC Order F2005-003*).

A determination about what personal information is related directly to and necessary to collect would likely be overturned only if it was patently unreasonable (see *IPC Investigation Report F2002-IR-012*).

Review of collection practices

A public body should regularly review their collection practices to ensure that any collection of personal information is authorized by **section 33**. Such a review should

- verify that there is authority for the collection of personal information;
- discontinue the collection of personal information that does not meet the criteria set out in **section 33** and amend forms and other collection instruments, contracts and agreements, and policies and procedures that require the collection of this personal information (for more information on reviewing collection instruments, see section 9.4 of Chapter 9);
- confirm that a process is in place to ensure that all new or modified collections of personal information meet the criteria set out in **section 33** and ensure that the minimum personal information necessary to meet program needs is collected;
- ensure that information that is needed only for subsets of clients is collected only from the clients that fit the subset criteria (see *IPC Investigation Report 98-IR-003*);
- verify that procedures are in place to ensure that any irrelevant personal information that is sent to a public body is placed in a separate file so that it is not improperly used, and that it is destroyed, redirected or returned to the originator at an appropriate time after completion of the process during which the information was inadvertently collected (see *IPC Order 98-002*); and
- ensure that personal information in the custody or under the control of the public body is scheduled for retention (if the information is still needed) or for deletion or destruction and that retrieval mechanisms are deactivated (if the information is no longer needed).

This review could be carried out by the program areas having custody or control over personal information, with the advice of the FOIP Coordinator.

Administrative controls should be established in privacy policies. New collection activities and instruments should be reviewed by the FOIP Coordinator's office. The review may be carried out in conjunction with reviews of information management practices and systems, which are discussed in Chapter 9.

Unsolicited Information

If a public body does not have specific authority to collect unsolicited personal information and the information is not necessary for an operating program or activity of that public body, it is not an authorized collection (see *IPC Order 98-002*). The public body should adopt a policy of either returning the unsolicited information or destroying it in accordance with a transitory records schedule.

For example, when the Calgary Police Commission requested the names and positions of board members from the Calgary Police Association, the Association also sent the members' home addresses and telephone numbers. Since the Commission did not need this additional information, the investigating officer recommended that it be returned to the Association, and that the Commission adopt a policy that all unsolicited information be returned (*IPC Investigation Report 2000-IR-002*).

In some cases, a public body might keep unsolicited personal information for a specified period of time before destroying it (e.g. unsolicited résumés). The public body should keep the unsolicited information separate from other files so that it will not be improperly used or disclosed.

7.2 Manner of Collection

Direct collection

Section 34(1) states that, subject to some limited exceptions, a public body must collect personal information directly from the individual the information is about. This establishes direct collection as the primary method for obtaining personal information. This is an important principle for fair information practices. It helps to ensure that an individual is aware of the type of personal information being used to make a decision concerning him or her. It also allows the individual to challenge the need for the information or refuse to provide the information or participate in the program or activity. Collecting information directly from the individual it is about will generally fulfil a public body's requirement to make every reasonable effort to ensure that the personal information is accurate and complete (for further information on accuracy and completeness, see section 7.3 of this chapter).

A public body must not seek or passively receive the information from another source even though it may have the capability of doing so, unless collection from that indirect source or for that purpose is authorized in the exceptions listed under **section 34(1)**.

Exceptions to direct collection

The Act provides for circumstances where personal information about an identifiable individual may be sought from sources other than the individual the information is about. If one of the provisions in **section 34(1)** applies, personal information may be obtained in verbal, written, electronic or other form (e.g. a file transfer).

Another method of collection is authorized

Section 34(1)(a) This provision allows a public body to collect personal information about an individual from another public body, or other individual or organization under one of the specified conditions.

By the individual. When an individual authorizes the collection of his or her personal information from another source, as in the case of a student requesting a reference from a professor, this authorization should be in writing. This may take the form of a signed authorization on an application form or a letter giving authorization. If an individual provides authorization orally over the telephone, the public body

should document the conversation and, whenever possible, send a letter to the individual concerned setting out what he or she has authorized.

When asked to authorize indirect collection of personal information under **section 34(1)(a)(i)**, the person should be informed of

- the nature of the personal information to be collected (i.e. how much of what type of information is being collected);
- the purpose of the indirect collection (i.e. what the information will be used for);
- the reasons for making the collection indirectly;
- the identity of the recipient and the expiry date of the authorization, and
- the consequences of refusing to authorize the indirect collection.

If an individual authorizes a public body to collect personal information from another public body or from a custodian under the *Health Information Act*, the written authorization for the collection is often included in the same form as the authority for the other body or custodian to disclose the necessary information to the first public body. As a result, the authorization format should take into consideration the disclosure (and possibly the consent) requirements of the *FOIP Act* and the *Health Information Act* if the disclosing public body is a custodian under that Act.

By another Act or a regulation under another Act. Sometimes another Act or regulation under another Act specifically authorizes indirect collection of personal information. For example, the *Workers' Compensation Act* authorizes collection of medical information from a physician about an individual who was involved in a work-related accident.

Another example is the Student Record Regulation, which authorizes public schools to collect teachers' notes about students and other personal information in records from a student's previous private school (see *IPC Order 2001-034* and *IPC Investigation Report F2002-IR-007*).

By the Information and Privacy Commissioner. The Commissioner has the power to authorize indirect collection under **section 53(1)(h)**. This provision addresses situations where indirect collection should be considered but **section 34** does not permit it. The Commissioner has the responsibility of deciding how and under what circumstances he will exercise the power.

Information may be disclosed under Division 2 of Part 2 of the Act

Section 34(1)(b) This provision permits a public body to collect personal information from a second public body, rather than from the individual the personal information is about, where the second body is authorized to disclose the information under **sections 40** to **42** of the Act.

Part 2 of the Act is structured in such a way that if a public body is authorized to disclose certain personal information to another public body, the receiving public body is, in turn, authorized to collect the information and to use it for the purpose for which it was disclosed.

Where public bodies rely upon section 34(1)(b) to collect personal information indirectly, the public body that has the information must be satisfied that the disclosure is authorized. The public body receiving the information must ensure that it is authorized to collect it under section 33.

This provision permits disclosure of personal information by one public body to another in limited and controlled circumstances.

Information is collected in a health or safety emergency

Section 34(1)(c) This provision allows emergency services personnel, as well as other employees of a public body, to collect information needed to deal with an emergency situation.

This can happen when

- the individual is not able to provide the information directly; or
- direct collection could reasonably be expected to endanger the mental or physical health or safety of the individual or another person.

Examples of such emergency situations include cases were an injured person is not able to respond to questions about medication or an accident or fire situation when a delay in collecting information about a person's actions could result in death or severe complications.

Under this provision, a public body can collect indirectly only the information required to deal with the emergency.

Information is about a designated emergency contact

Section 34(1)(d) This provision allows for the collection of contact information such as a name, relationship, address and telephone number(s). The individual may be a family member or a friend. This is the personal information of the contact and this information would be collected from an individual who is required to provide an emergency contact.

Such information is often provided when, for example, students enter a college residence, children are registered in a day camp program or for a school field trip, or a public body hires a new employee.

Information is collected to determine suitability for an honour or award

Section 34(1)(e) This provision allows a public body to seek references and other relevant personal information about someone being considered for an honour or award. This includes honorary degrees, scholarships, prizes, and bursaries.

The nature of some awards is such that the potential recipients do not have to apply for the award and may not be aware that they are being considered. Scholarships and bursaries are often awarded on the basis of academic achievement and recommendations by faculty members. Honorary degrees are usually awarded in recognition of a person's contribution to a community or sector of society. Prizes may be awarded on the basis of athletic or scholastic achievements.

Any information collected should be directly related to the criteria for granting the honour or award. As a best practice, public bodies should develop criteria for an award in advance of the collection of personal information about award nominees and make those criteria generally available. Once the individual has been informed about the honour or award, his or her personal information should only be disclosed with consent, unless another exception for disclosure applies.

Information is collected from published or other public sources for fund-raising

Section 34(1)(f) This provision allows for limited collection of publicly available personal information without the authorization or knowledge of an individual. The information collected can be used only for fund-raising purposes. Public bodies should keep such information segregated in their records and allow access by only those employees engaged in fund-raising and fund development activities.

Published sources are publishers, including a company that produces and distributes books and newspapers, but also by a publisher that distributes information only in electronic form, most commonly on a website. Examples include newspaper reports, clipping files, corporate reports of public companies, and articles in periodicals. Most of this information would be readily available in a public or specialized library.

Other public sources includes information that is made available to the public at large in any medium. The information may not be routinely made available; it may be of a kind that can be made available on demand, for example, through a search of a database or making a request for a public record, as in the case of certain classes of court records. The information may be made available free or for a fee. Examples include information in reports of charitable organizations, announcements of honours or awards granted by or through a public body in Alberta, copies of speeches or speaking notes when the speeches are given at a public event, and information available on the Internet. Care should be taken when relying on personal information that is collected from the Internet; the credibility of the source of the information should be considered. The public body should also bear in mind that this personal information would be accessible to the individual if he or she made an access request.

Not included under this provision is information of a more private character, such as information based on personal acquaintance, friendship or observation that may be provided by members of a governing board or employees; information that could only be gathered through surveillance or from private sources; next-of-kin information; and names of parents of students. For more information on this provision, see FOIP Bulletin No. 5: *Fund-Raising*, published by Access and Privacy, Service Alberta.

Information is collected for the purpose of law enforcement

Section 34(1)(g) This provision allows the indirect collection for law enforcement activities as defined in **section 1(h)** of the Act, including policing and investigations.

It should be noted that the authority to collect personal information under **section 34(1)(g)** is limited. Under the definition of law enforcement in **section 1(h)**, as interpreted by the Commissioner, the law enforcement body must ensure that there is a specific authority to investigate and that the investigation could lead to a penalty or

sanction being imposed under a statute or regulation. See section 4.6 of Chapter 4 for information on the definition of law enforcement.

Much personal information about a person who is under investigation is collected from other sources. Reasons for this include the fact that investigators may not wish to alert the individual concerned that an investigation is taking place, the individual would not provide accurate information, or the individual might alter or destroy evidence. Disclosure of personal information by private-sector organizations in Alberta is governed by the *Personal Information Protection Act* (PIPA), or in some cases, the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). Law enforcement bodies may wish to refer to the *Requesting Personal Information from the Private Sector: A Guide for Law Enforcement Agencies*, published by Access and Privacy, Service Alberta.

Law enforcement bodies should not collect excessive amounts of personal information. One of the situations where this is likely to occur is in the use of surveillance. The Commissioner considered the use of video surveillance for law enforcement purposes in *IPC Investigation Report F2003-IR-005*.

Information is collected for the purpose of collecting a fine or debt

Section 34(1)(h) When public bodies face the problem of not being able to locate those owing money, or when they believe they would not obtain accurate information needed to collect the debt from the individual debtor, they are permitted to collect personal information from other sources.

This provision allows a representative of either the provincial government, as a whole, or any individual public body to contact any person or organization or to use publicly available information (e.g. on the Internet) that may be able to help in the collection of money owed to the public body or the government. This may include finding the home or work location or telephone number of the individual who owes money.

A *debt* is something that is owed, usually money, where the individual has an obligation to pay and the creditor has the right to receive and enforce payment.

A *fine* is a monetary punishment imposed on a person who has committed an offence, including an offence under a bylaw.

Information concerns the history, release or supervision of an individual under the control of a correctional authority

Section 34(1)(i) This provision permits correctional and parole authorities to seek out information from a variety of sources about individuals under their control or supervision. The individual may be in a correctional institution or may be under supervision in the community.

If a community service organization is itself a public body, or is under contract to a public body to provide services to individuals under the control or supervision of a correctional or parole authority, it may rely on **section 34(1)(i)** for indirect collection of personal information about the individual's history, release or supervision relevant to the service being provided.

History here means information about the person's background, including employment record, medical condition and behaviour.

Release includes both permanent and temporary release from a correctional institution.

Supervision includes any community disposition requiring supervision of an offender, including probation, bail supervision, parole, temporary absence, and ordered community service work, as well as supervision of an individual held in a correctional institution.

Information is collected for use in the provision of legal services to the Government of Alberta or a public body

Section 34(1)(j) This provision permits that lawyers representing the provincial government or a public body may have to collect personal information to perform their jobs. The information may be required for day-to-day provision of legal services, or in preparation for a proceeding before a court or tribunal.

It is often not possible to collect the personal information directly because inaccurate information may be given. It may also be desirable that legal enquiries be made in confidence, or it may be that the individual concerned may not be able to provide the required information. In these circumstances the public body's legal representatives, or others providing legal services, can collect information indirectly, or ask an employee to do so on their behalf.

Information is necessary to determine eligibility to participate in a program or receive a benefit, product or service

Section 34(1)(k)(i) Many programs operated by public bodies have eligibility criteria that must be met in order for an individual to participate in them or receive a benefit or service. This may require the public body to approach several different sources of information besides the individual to determine whether the criteria or qualifications are met. Examples include verification of income for the Alberta Seniors Benefit, low-income housing or other income-tested programs; verification of assets for programs requiring asset testing; and verification of educational prerequisites for a post-secondary program.

This collection of information can take place only in the course of processing an application from the individual, or from his or her representative. It is a good business practice to inform the individual about whom information is being collected that information from a variety of sources will be collected to document a particular application. Public bodies should not take the further step of asking an individual to authorize indirect collection unless they are prepared to modify their procedures for determining eligibility if an individual refuses to authorize the indirect collection. Authorization from the individual is not necessary if the requirements of **section 34(1)(g)** are fulfilled.

Information is necessary to verify eligibility to participate in a program or receive a benefit, product or service

Section 34(1)(k)(ii) This provision is intended to allow for cases where an individual has already qualified for a program, benefit, product, or service and the public body needs to check that the individual is still eligible. In this case, personal information may be

collected from a variety of sources other than the individual the information is about, and the individual does not need to be informed that verification is taking place.

For example, a public body may perform random checks on the income and assets of individuals on social assistance or in low-income housing to verify that an individual remains eligible for the program. Such a check may involve an interview with the individual but may also involve collection of personal information about an individual from other sources. Another example would be verification of a student's continued enrolment in a program so that the student may continue to receive student financial assistance or a grant.

As with the previous provision, it is a good business practice to inform the individual about whom the information may be collected that verification of continuing eligibility may occur without notice. This is especially the case if the individual could incur any penalty for receiving a benefit for which he or she has become ineligible.

Information is collected by the Public Trustee or the Public Guardian

Section 34(1)(l)

The *Public Trustee* is the trustee for dependent adults who are unable to administer their own financial affairs because of a mental disability. The Trustee also administers the estates of persons who die intestate if the deceased persons have no adult beneficiaries residing in the province. In addition, the Trustee acts as guardian by protecting the assets and financial interests of missing persons and children under 18 years of age.

The *Public Guardian* is charged with the responsibility of ensuring that appropriate surrogate decision-making mechanisms, supports and safeguards are available to assist adults who are unable to make personal decisions independently.

Section 34(1)(l) permits the Public Trustee and the Public Guardian to collect personal information about a prospective ward indirectly from relatives, friends and others. This may include information about the individual's mental or physical health, financial information, employment or educational history, and opinions about the individual.

Under the *Public Trustee Act*, section 44, the Public Trustee may compel a person, including a public body, that has possession of personal, financial or health-related information about a client or potential client, to provide that information or record to the Public Trustee for the Public Trustee to carry out a task, duty or function relating directly to the client or prospective client.

Information is collected for the purpose of enforcing a maintenance order

Section 34(1)(m)

This provision permits Alberta Justice and Attorney General to collect personal information for the purpose of enforcing maintenance orders.

Amendments to section 12 and section 13 of the *Maintenance Enforcement Act* require government departments, provincial agencies (e.g. post-secondary institutions) as well as business organizations (including municipalities) to provide an expanded number of types of personal information (e.g. financial information, an identification number issued by a province) to the Director of Maintenance Enforcement for the purpose of enforcing a maintenance order. Only the requested

information that is listed in that Act should be disclosed by a public body and collected by the Director.

Information is collected to manage or administer personnel of the public body

Section 34(1)(n) This provision permits the Government of Alberta as the employer for all provincial government departments. It allows government departments to collect personal information about an employee or prospective employee from other provincial government departments for the purpose of managing or administering personnel of the Government of Alberta.

Management of personnel refers to aspects of the management of human resources of a public body that relate to the duties and responsibilities of employees (see *IPC Investigation Report 2001-IR-006*). This includes staffing requirements, job classification or compensation, recruitment and selection, salary, benefits, hours and conditions of work, leave management, performance review, training and development, occupational health and safety, and separation and layoff. For the Government of Alberta, the term includes the government-wide network managed through the Corporate Human Resources. It does not, however, include the management of consultant, professional or independent contractor contracts.

Administration of personnel comprises all aspects of a public body's internal management, other than personnel management, necessary to support the delivery of programs and services. Administration includes business planning, financial, materiel, contracts, property, information, and risk management (see *IPC Investigation Report 2001-IR-006*).

Section 34(1)(n) also allows public bodies to collect information about employees or prospective employees from third parties. Any collection under this provision must have, as its purpose, the management or administration of the personnel of the public body collecting the information.

Employees should be informed in a general way as to how personnel information about them is collected and from what sources they can expect this information to be derived. They should also be aware of the purposes for which various types of information are used and of their rights under the Act.

Examples of such collection include the collection of references for prospective employees, determination of qualifications and performance for secondment and training opportunities, and the provision of pay and benefit services by one public body for other public bodies.

Section 34(1)(n) refers to official personnel activities and does not permit the collection of personnel-related information by individual officials for purposes other than official duties relating to the management and administration of personnel within a public body.

The indirect collection authorized in **section 34(1)(n**) does not apply to other internal activities of public bodies, such as Corporate Challenge events and United Way

campaigns. Personal information of employees not related to managing or administering personnel should be collected directly from the individuals and the notification provisions in **section 34(2)** need to be complied with.

Information is collected to assist in researching or validating the claims, disputes or grievances of aboriginal people

Section 34(1)(o) This provision permits a public body to collect personal information indirectly in order to research the background of the claims, disputes or grievances and expedite the settlement of wider rights of aboriginal people.

Validating means confirming rights that have been contended by the parties to a claim, dispute or grievance.

The term *claims, disputes and grievances* is interpreted broadly to include all manner of controversies, debates and differences of opinion regarding issues in contention and is not restricted to differences over land claims.

Aboriginal people means individuals whose racial origins are indigenous to Canada, including Indian, Métis and Inuit people.

Notification

Section 34(2) **Section 34(2)** sets out rules that a public body must follow when it is required to collect personal information directly from an individual. The notification requirement allows an individual to know the purpose of the collection of personal information and how the information will be used.

A public body must inform the individual of

- the purpose for which the information is collected;
- the specific legal authority for the collection; and
- the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

The *purpose* of a collection means the reason(s) the information is needed and the use(s) that the public body will make of the personal information.

The *legal authority* for collection may be a specific provision in an enactment of Alberta or Canada that expressly authorizes collection of the personal information, or **section 33(c)** of the *FOIP Act*, which authorizes collection of personal information that is directly related to and necessary for an operating program of a public body.

If a public body relies on **section 33(c)** of the *FOIP Act*, it is important to also provide the authority for the program for which the personal information is being collected. The program itself may be authorized by an Alberta or federal Act or a regulation under an Act, or a bylaw or legal resolution of a public body establishing a program that falls within its mandate under an Act.

Identifying someone to answer the individual's questions about the collection is intended to provide the individual with a knowledgeable source of information. The

person cited should be familiar with the program, and be able to explain why the personal information is being collected and how it will be used by, and disclosed to, other bodies.

Examples of cases where collection of personal information requires notification under this provision include collection of personal information for enrolment in a program, to receive a service or to apply for a benefit, collection of personal information on a client survey and collection of individually identifying information on a course evaluation form.

Where a public body would be permitted to collect personal information indirectly but chooses to collect directly from the individual the information is about, notification is still mandatory, even if it would not be required had the public body collected the information indirectly (see *IPC Order F2006-019*).

Notification may be given in many ways. It may be

- printed on a collection form;
- contained on a separate sheet or in a brochure accompanying a form;
- presented in a pop-up window linked to an online form;
- published in a calendar of a post-secondary institution or an information brochure about a program that is provided to all applicants;
- displayed on a notice hung on the wall or placed on a service counter; or
- given orally, for example, during a phone call.

Regardless of the manner in which notification is provided, all three parts of the notice must be provided to the individual (see *IPC Investigation Report 2000-IR-004*).

The notice should be given at the time that the personal information is being collected. In *IPC Investigation Report 2000-IR-007*, the Commissioner found that a school should have provided students or parents with a notification statement when school photographs were being taken rather than during the registration process since the collection of student photographs was not part of registration.

Notice should be given to individuals at the beginning of an interview when an individual is being asked to provide his or her own personal information. If the interview is being recorded, it is good practice to record the notice at the beginning of the tape.

When a notification is given orally, either in person or over the telephone, it is a good practice to refer the individual to a written copy of the notice or to provide a printed copy either at the counter or later by mail, and to retain a record that the notice was given.

When individuals are applying for and participating in extensive and complementary programs, it may be convenient and effective to place a notice explaining all collections of personal information relating to the programs in a publication about the programs, or explain orally.

Public bodies should undertake a regular review of their collection instruments to determine which ones require the inclusion of collection notices. Collection notices should be included on all print and electronic forms used to collect personal information directly. This should be done in conjunction with the review discussed in section 7.1 of this chapter and any privacy compliance audit or forms review process, as discussed in Chapter 9.

When collection of personal information is carried out by one public body for or on behalf of another public body, this must be done under a written agreement. The agreement should state the reasons for collecting information through an agent, the specific authority for the collection, and the purposes for which the personal information will be used or disclosed. Any use or disclosure of the personal information must be authorized under the *FOIP Act*.

Exception to notification

Section 34(3)

Section 34(3) provides that the requirements for collecting personal information directly and giving notice may be set aside if, in the opinion of the head of the public body, compliance with these provisions could reasonably be expected to result in the collection of inaccurate information.

Inaccurate information is incorrect, incomplete or misleading information, or information which does not reflect the truth.

This provision recognizes that in certain limited circumstances, such as the conduct of some surveys seeking opinions and in some psychological testing, there may be difficulty in getting accurate information if individuals are informed in advance of the reasons for the collection. In some cases, notifying individuals of the purpose of a survey would lead to responses that would distort the results.

This provision should be used only in limited circumstances within programs, and public bodies should maintain documentation of when the provision has been used and the reasons for using it.

7.3 Accuracy and Retention

Section 35 of the Act provides that, if a public body uses an individual's personal information to make a decision that directly affects the individual, the public body must

- make every reasonable effort to ensure that the information is accurate and complete; and
- retain the personal information for at least one year after using it so that the individual has an opportunity to obtain access to it.

Retention may be for a shorter time period under certain conditions discussed below in relation to **section 35(b)** of the Act.

A decision that directly affects the individual is one that has an impact on an individual's life or affects his or her rights. The meaning of the term is interpreted broadly and includes decision-making processes that are internal to a public body and those which involve a more direct relationship with the public.

Examples of decisions that directly affect an individual include a determination as to whether or not someone is entitled to income assistance or a student loan, a decision on hiring an individual or on admission to a course or program, and a determination regarding eligibility for subsidized housing or library services.

Section 35 does not apply if no decision, adverse or otherwise, will be or has been made about an individual. Examples include raw survey data where personal information is collected but the results are rendered anonymous, telephone messages, and unsolicited résumés that are never considered in relation to a position.

Accuracy and completeness

Section 35(a)

Section 35(a) requires the public body to make every reasonable effort to ensure that personal information is accurate and complete.

A public body makes *every reasonable effort* when it is thorough and comprehensive in identifying practicable means to assure that personal information used to make a particular decision affecting the individual is accurate and complete.

Accurate means careful, precise, lacking errors.

Complete means including every item or element; without omissions or deficiencies; not lacking in any element or particular. Information is *complete* when all the information necessary to make the decision, and only the information that will be used for that purpose, is collected.

Generally, if a public body collects personal information directly, it is likely to meet the requirement of making every reasonable effort to ensure that information is accurate and complete. This is especially so if the individual has signed a statement indicating that the information is accurate and complete. However, the burden of making every reasonable effort is higher when the consequences of a decision are greater.

Public bodies should have adequate procedures in place to properly verify the accuracy and completeness of any personal information crucial to an application, transaction or action at the time the information is provided (see *IPC Orders 98-002* and *2001-004*).

It is a good business practice for programs that use large personal information systems for delivery of programs or services to have systematic processes for updating personal information that is used on a regular or continuous basis.

Other methods of maintaining accuracy include periodically auditing files with accuracy and completeness as one of the criteria tested; ensuring limited access to information for the purpose of making corrections; and establishing cross-referencing and validation checks within the software of automated systems that identify

anomalies in data. Privacy requirements should be integrated into normal information and systems operations for the program as a whole.

Maintaining ongoing accuracy will be more challenging for programs that involve a lengthy review or approval process or an ongoing relationship with an individual. The accuracy requirements of the Act should be considered in the management of programs of this kind.

The Information and Privacy Commissioner has said that ensuring accuracy includes making certain that handwritten information used to make decisions, such as clinical notes, is legible (see *IPC Order 98-002*).

In *IPC Order F2003-008*, the Commissioner determined that the requirement to ensure accuracy and completeness does not apply to a reference provided by a former employee after that employee has left the employment of the public body.

Retention

Section 35(b) This provision requires public bodies to retain personal information for at least one year after using it to make a decision that affects an individual, so that the individual has a reasonable opportunity to obtain access to it.

This retention requirement is intended to permit individuals to review and, if necessary, to request correction of information about them that has been used by public bodies, and to do so before disposition of that information takes place. It is not necessary to retain personal information when no decision will be or has been made about the individual.

Retain means to maintain custody or control of the personal information.

Section 35(b) does not prevent public bodies from storing personal information in another location, such as the Alberta Records Centre, if the public body can retrieve the personal information in response to a request for access to it.

Section 35(b) does not include personal information in transitory records if the information is transferred to a different format. This may be the case with records such as counselling notes or notes of an interview panel member that are consolidated into a final document, if it is the policy of the public body to treat these notes as transitory records. (See section 8.5 of Chapter 8 for further discussion of transitory records.)

Section 35(b) overrides all records retention and disposition schedules by establishing a retention period of at least one year after use for personal information used in administrative decision-making.

An exception to this requirement is allowed when a public body and the individual the information is about both agree in writing to a shorter retention period. In the case of government departments and agencies subject to the Records Management Regulation, a decision not to retain the personal information requires additional

approval from the Alberta Records Management Committee. This provision might be used, for example, to permit destruction of a person's application for counselling or addiction treatment when the applicant withdraws the application and does not seek the treatment. A provision in a collective agreement permitting the destruction of certain appeal hearing records within six weeks of the hearing decision satisfied the requirements for a written agreement under this section (*IPC Order F2004-027*).

If a public body receives a request for access to personal information during the one-year retention period, the public body must keep that personal information with the request file for a further year after the last action is taken in regard to the request.

If the Commissioner conducts a review of the response to an access request that contains personal information, the information must be retained for a year from the date that the public body complies with an order by the Commissioner to disclose the personal information.

Public bodies may keep personal information longer than one year, depending on their operational needs and on legal requirements. However, keeping personal information longer than necessary increases the risk of a security breach and of "function creep" (i.e. using the information for purposes that were not originally contemplated). Also, if the information was collected for a certain purpose and the purpose has been met, the finality principle of fair information practices suggests that the public body should then destroy it. Personal information can also be rendered non-identifying or anonymous and then retained longer for statistical purposes.

To help ensure that out-of-date and incomplete personal information is not incorrectly used in a decision affecting an individual, personal information should be scheduled for retention and disposition in accordance with the appropriate authorities for the management of recorded information.

For public bodies subject to the *Government Organization Act*, retention and disposition of personal information must be in accordance with policies and procedures established under the *Government Organization Act* and the Records Management Regulation. Local public bodies must comply with legal instruments governing the retention and disposition of their records (section 3(e)(ii)).

7.4 Correction of Personal Information

Right to request correction of personal information

Under **section 36(1)**, an individual who believes that his or her personal information, in the custody or under the control of a public body, contains an error or omission may request the public body to correct the individual's personal information.

An *error* is mistaken or wrong information or information that does not reflect the true state of affairs. An *omission* is information that is incomplete or missing or that has been overlooked.

Information is personal information if it meets the definition of *personal information* in **section 1(n)** of the Act, regardless of whether the public body created or gathered the information directly or obtained it from someone else (see *IPC Order 98-001*). A public body has *custody* of a record when the record is in the possession of the public body. 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. See section 1.4 of Chapter 1 for a detailed discussion of custody and control.

In order to request a correction of personal information, an individual does not have to first make a request for access to his or her personal information. For example, a public body may refer to information contained in a record and the individual may challenge the accuracy of that record without having seen it.

A request for correction may be generated as a result of an adverse administrative decision (e.g. a denial of a claim or benefit). The *FOIP Act* does not require the public body that made the decision to revisit that decision as a result of the request.

The Act gives individuals the right to *request* a correction of personal information, not a right to have a correction made. The public body may either correct the information, by changing it or adding new information, or may refuse to correct the information, subject to other provisions discussed below.

When considering requests for correction of personal information, it is important to distinguish between the two types of information addressed by **section 36**:

- *factual information* about the applicant, such as age, date of birth, income information or qualifications (**section 36(1)**); and
- *opinions* about the applicant, such as subjective assessments or evaluations of an individual's condition, abilities or performance (**section 36(2)**).

The individual must provide proof in support of the request for correction of factual information. The proof should be of the same nature and at least the same quality as the personal information required when the original collection took place. Examples of documents that might be required to prove facts include a birth or baptismal certificate to prove age, or a notice of assessment from the Canada Revenue Agency to prove income.

Factual information does not need to be corrected if the facts are in dispute and it is not possible to make a factual determination about the issue through the inquiry process (see *IPC Orders 97-020* and *F2005-008*).

A public body must not correct an opinion (**section 36(2)**) including a professional or expert opinion (see *IPC Orders 98-010* and *2000-007*). The significance of an opinion may be that it reflects another person's view at the time it was offered, and it may be important to have a record of that view at a later date. The Act allows an

individual to have his or her views about that opinion added to the record for other readers to consider.

Although a public body cannot correct an opinion, it may, in some circumstances, seek or accept another opinion about the applicant and reconsider any decision based on the original opinion. However, the question of what information is used by a public body to make a decision about an individual is outside the scope of the Act and outside the jurisdiction of the Information and Privacy Commissioner (see *IPC Order 2001-004*).

How a request is made

In many cases, an individual will ask for personal information to be corrected and supply proof of correction without doing this in a formal way. Public bodies can, and most often will, make corrections without a request under the Act if this is practical and expedites public business.

Where, in the opinion of the individual, an error or omission exists, a request for correction can be made to the public body in the form of a letter or on a **Request to Correct Personal Information Form**, a sample of which is included in Appendix 5.

Requests for correction are subject to the same rules as requests for access under the Act. This includes time limits. It also includes a duty on the part of the public body to seek clarification of a correction request, if necessary (see *IPC Order 98-010*). The Commissioner has the power to review the actions of a public body with respect to requests for correction of personal information.

When a correction is made

When a public body decides to correct an error, all records containing the personal information must be corrected. This includes records in all information systems – paper, electronic and microform. Similarly, when a public body decides to add omitted information, all systems must be updated. The record should be annotated with the date of the correction. A linking mechanism, as described below, may have to be employed when personal information is stored on a medium such as microform, which may be more difficult to update.

To *annotate* personal information means to add the requested correction to the original record, close to the information under challenge by the applicant. An annotation should be signed and dated. When designing electronic forms and databases, provision should be made for allowing annotation. (For a discussion of annotation, see *IPC Order 97-020*.)

To *link* a record means to attach, join or connect the record to the requested correction. This may consist of a letter or statement from the applicant, or a copy of the **Request to Correct Personal Information Form**.

When a correction is refused

Section 36(3) **Section 36(3)** provides that, when a correction is refused or cannot be made, the public body must annotate or link the personal information with that part of the requested correction which is relevant and material to the record in question.

Relevant and material means that there is a direct connection between the correction requested and the use that has been or may be made of the personal information and that the correction is substantive. The correction should be both pertinent to the subject matter and significant in its content.

A public body may refuse or be unable to make a correction that an applicant requests. This may be because the information is not personal information, the applicant has not submitted adequate proof in support of the requested correction, or the information consists of an opinion rather than fact (see *IPC Orders 98-010* and *2000-007*).

In the case of factual information, when the public body is not satisfied with the proof presented, the public body does not change the information but rather annotates it or links the presented information to the original information.

In the case of an opinion, a public body may describe the information in dispute and place this description, along with a statement that the applicant does not agree with the opinion or interpretation, on the record. If practicable, the applicant's request for correction may be attached (see *IPC Order 97-020*).

A public body is required to note only that part of the requested correction which is relevant to the record being annotated or to which the link is being made. Public bodies must not place the applicant's entire request on the record if it contains material that is not germane to the use made of the record (see *IPC Order F2006-017*).

Annotating a request for correction

A model **Annotation to Personal Information Form** is provided in Appendix 5. A public body may use this form to set out an annotation relating to a correction that was requested but not made. This form clearly indicates to users that the information has been linked to a correction request and not corrected. It is filed with, or linked to, the information for which a correction was sought.

A copy of this **Annotation to Personal Information Form** or equivalent documentation must be sent to the individual requesting a correction at the time the individual is informed that the correction is not being made (see **Model Letter T** in Appendix 3). Any further information supplied by the individual after receiving this notice must be filed with the **Annotation to Personal Information Form**. (See *IPC Order 97-020*.)

In *IPC Investigation Report 2000-IR-006*, the Commissioner recommended that a municipality put a system in place that would ensure that a corrected copy of a record of personal information is sent to the individual within 30 days of a correction being made to the individual's personal information.

If the **Annotation to Personal Information Form** or the **Request to Correct Personal Information Form** cannot be physically attached to the record, a flag may be placed in the file or system containing the personal information in dispute. This will refer a user to a separate file, containing the actual disputed personal information, and indicating that a request for correction or addition of information was made but not granted.

When a public body makes an annotation or linkage regarding a request for correction that has been refused or regarding a request for correction that has been agreed upon, it must ensure that the new information is stored with the original information and will be retrieved whenever the information in question is used for an administrative purpose directly affecting the individual involved. Annotations must be made available to all users of the file or the information, including the individual, should he or she request access to his or her personal information.

In *IPC Order 2001-009*, the Commissioner found that the public body had not correctly annotated a request for correction of a videotape. Although the public body had placed the **Annotation to Personal Information Form** (see Appendix 5) on the individual's claim file, it was also required to note on the videotape label that a correction request was on the individual's file.

In *IPC Order F2003-019*, the Commissioner determined that a proper linkage was not formed when the public body simply placed the request for correction in the individual's file that contained a large number of records. The public body was required to link the request for correction to the records in question in such a manner that it would be readily apparent that a request for correction had been made for those specific records.

Notification of other public bodies and third parties

Section 36(4)

Section 36(4) obliges public bodies to inform other public bodies, groups of persons, persons, or organizations that have received an individual's personal information of the request for correction or annotation of that information. Notification is required if the personal information has been shared in the year prior to the request for correction.

The notification process ensures that other parties have accurate and complete information for their own decision-making processes. In order to fulfil the notification requirements of **section 36**, a public body should keep a record of non-

routine disclosures of personal information so that if there is a request for correction the public body can inform the persons the information was disclosed to.

Section 36(5) **Section 36(5)** provides that such notification is not necessary if

- the correction, annotation or linkage is not material; and
- the individual who requested the correction is advised and agrees in writing that notification is not necessary.

This provision recognizes that individuals may request correction of errors in a record that are not significant for the use of the record. Public bodies may dispense with third party or public body notification if the correction requested is not required for their decision-making, provided the individual agrees with this option.

Consent in writing from the individual is required to dispense with notification.

Section 36(6) **Section 36(6)** provides that other public bodies, once notified, must make any correction, annotation or linkage to the relevant personal information disclosed to them and which is in their custody or under their control. This helps ensure that all personal information disclosed by one public body to another is accurate and complete.

Time limits

Section 36(7) **Section 36(7)** provides that a public body must, within 30 days of receiving the request, give written notice to the individual that either the correction has been made or an annotation or linkage has been made. It is good practice to ensure that other public bodies or third parties are also notified within the 30-day time period.

A public body may extend the time limit to deal with a request for correction for up to 30 days or, with the permission of the Commissioner, for a longer period.

Section 14 of the Act governs these extensions; the most likely provisions to apply in correction situations are

- the applicant does not give enough detail to enable the public body to identify a requested record (**section 14(1)(a)**); or
- a large number of records is requested or must be searched and responding within the time limit would unreasonably interfere with the operations of the public body (**section 14(1)(b)**).

Model letters S, **T** and **U** in Appendix 3 deal with the correction process. Guidance on making corrections and annotations, as well as copies of the **Request to Correct Personal Information Form** and the **Annotation to Personal Information Form** are included in Appendix 5.

Transfer of requests for correction

Section 37 **Section 37** provides authority for a public body to transfer a request for correction of personal information to another public body. This can occur when

- the other public body originally collected the personal information; or
- the other public body created the record containing the personal information.

This provision ensures that the public body that originally collected or compiled the information deals with a request for the correction of that personal information. It can also ensure that all public bodies to which the information was disclosed are properly notified of the correction. **Section 37** mirrors the provisions for transfer of access to information requests.

If a request is transferred under this section, the public body transferring the request must notify the individual of the transfer as soon as possible. The public body receiving the transferred request has 30 days from the date of the transfer to respond to the request, and can extend this time limit as outlined above.

7.5 Protection of Personal Information

Section 38 of the Act requires a public body to protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.

Making reasonable security arrangements means approving and implementing a security policy for use within a public body.

In *IPC Investigation Report F2003-IR-003*, the Investigator found that a school jurisdiction had failed to make reasonable security arrangements to protect personal information against unauthorized access. Most staff members had full access to the electronic Student Information Record System and the system had no way to track who was accessing student information, when, or for what purpose. The limited access controls that did exist had not been employed, and no policies, procedures or training were in place regarding access and privacy.

Government departments and offices must adhere to certain security policies produced by the Office of the Corporate Chief Information Officer, such as the *Government Security Policy for Disk Wiping Surplus Computers* and the *Policy for Maintaining the Security of Government Data Stored on Electronic Data Storage Devices*.

Other public bodies may store or dispose of personal information only as authorized by bylaw, resolution, or other legal instrument, or under the direction of the public body's governing body (**section 3(e)**).

Public bodies should document the transfer of records containing personal information to the Provincial Archives or other archives. Public bodies should also document the destruction of records containing personal information, except for transitory records.

Public bodies are responsible for ensuring that personal information is protected during the time it is in storage, waiting to be picked up, and in the process of being transferred to archives or destroyed.

Public bodies must ensure that contractors follow proper privacy protection procedures. When contracting for services involving personal information, public bodies should incorporate privacy protection provisions in the contract. For more information on contracting under the *FOIP Act*, see *Managing Contracts under the FOIP Act: A Guide for Government of Alberta Contract Managers and FOIP Coordinators*, published by Access and Privacy, Service Alberta.

For further information on

- conducting privacy compliance reviews and threat and risk assessments;
- reviewing forms and other collection instruments; and
- developing a security policy;

see Chapter 9.

7.6 Use of Personal Information

Section 39 of the Act lists the only circumstances under which a public body may use personal information. A public body may use personal information only

- for the purpose for which the information was collected or compiled or for a use consistent with that purpose (**section 39(1)(a)**);
- if the individual the information is about has identified the information and consented, in the prescribed manner, to the use (**section 39(1)(b)**);
- for a purpose for which that information may be disclosed to that public body under **sections 40**, **42** or **43** (**section 39(1)(c)**); or
- if the information is in alumni records, for the purpose of a post-secondary educational body's own fund-raising activities (**section 39(2)**).

Use of personal information means employing it to accomplish the public body's purposes, for example, to administer a program or activity, to provide a service or to determine eligibility for a benefit. Public bodies may use personal information only under the following circumstances.

For the original or a consistent purpose

Section 39(1)(a)

The *purpose* means the purpose for which the information was collected under **section 33**. A public body can use the information for that purpose. Typical purposes include the administration of a particular program, the delivery of a service and other directly related activities.

The purpose must conform to **section 33** of the Act, which limits the purposes for which information may be collected. The authority for collection of personal information (**section 33**) is discussed in section 7.1 of this chapter.

The purpose of collection is described in the collection statement provided to the individual when the information is collected directly. When the information is not collected directly, or when it is compiled from several sources, the purpose should be stated in the written policy or procedure dealing with the program.

Compiled refers to a process by which certain information is created and becomes tied to or associated with an identifiable individual. For example, a public body creates or assigns a student ID number for each student. This information becomes the personal information of the student but the information was compiled by the public body, not collected from the student (see *IPC Order 2001-038*).

A public body may make use of personal information it has gathered, created or manipulated for the specific purposes for which it is permitted to collect or compile it.

A *consistent purpose* is one that has a direct and reasonable connection to the original purpose and that is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses the information (**section 41**).

Section 39(1)(a) also says that a public body may use personal information for a use that is consistent with the original purpose.

Consistent use is defined in **section 41** of the Act as a use that has a reasonable and direct connection to the original purpose of collection and that is necessary for performing the statutory duties of the public body.

In *IPC Order 2001-038*, the Information and Privacy Commissioner found that a school board's use and disclosure of a child's gender information for advertising, marketing and revenue generation purposes were not consistent with the original purpose for collection – namely, to register the child in school. However, use and disclosure of other personal information for the purpose of setting up and administering a student e-mail system was a consistent purpose.

Section 7.8 of this chapter deals more thoroughly with the concept of consistent uses.

For personal information held in personal information banks, public bodies must keep a record of all the purposes for which the personal information was collected or compiled and the purposes for which it is used or disclosed (**section 87.1(2)(d)**).

With the consent of the individual

Section 39(1)(b) A public body may use personal information if the individual the information is about has identified the information and has consented, in the prescribed manner, to its use.

Consenting *in the prescribed manner* means that the public body has followed the procedures for obtaining consent set out in **section 7** of the FOIP Regulation. This states that consent

- must be in writing; and
- must specify to whom the personal information may be disclosed and how the personal information may be used beyond the original purpose for which the personal information was collected or compiled.

To meet the minimum requirements under the Act, a form or other instrument requesting consent must

- **specify to whom the personal information may be disclosed; and**
- **specify how the personal information may be used.**

If consent is given in writing, the form must be signed by the person giving consent.

Consent may be given electronically or orally if the head of the public body has established a process for accepting electronic or oral consent that meets the requirements of section 7(5) or (6) of the Regulation, respectively.

Where appropriate, a form or other instrument requesting consent should

- indicate the original purpose of the collection, as well as the additional purpose for which the information is to be used and for which consent is being provided;
- indicate that consent is voluntary;
- indicate that consent may be revoked, but identify, where possible, any limitations and any consequences or implications that may result from revocation;
- to the extent possible, identify any consequences that may result from refusal to consent; and
- indicate the period of time during which the consent remains valid.

A public body may wish to seek consent for a new use of personal information. If the public body proposes to use personal information for a new purpose, the public body must get consent from the individual. If the public body is collecting additional information for a new use, the public body must have authority for the new collection and consent for the new use. The collection notice required under **section 34(2)** should be revised to indicate that the use of personal information collected from individuals after that time will be in accordance with the revised purpose.

It is important to note that, while a new use of personal information may be allowed under the Act with the consent of the individual, the public body may still be bound to adhere to its enabling enactments to authorize the new use. A public body cannot use personal information for programs that are outside the legislated area of responsibility of the public body. Also, if the public body is required to obtain additional personal information for the new use, then the collection of that personal information must be authorized by **section 33**.

Consent to a different use by the individual concerned serves as an indication that the person knows the consequences of the use of his or her personal information and has been provided with enough facts to make an informed decision about whether or not to consent to the use. When the person concerned has not indicated whether or not consent is given to a different use of personal information, public bodies cannot assume the individual has consented.

The absence of consent for a new use of information previously collected must be interpreted as the absence of authorization to use the information for the new purpose, unless otherwise permitted under the Act.

Public bodies cannot penalize individuals for refusing to give consent for use for an additional purpose by denying them any benefit or service provided in connection with the original collection. Individuals may, however, find they are denied a new benefit or service that might have been made available if the individual had consented to use of his or her personal information for that different purpose.

Section 2.5 of Chapter 2 deals with those classes of persons who may act for minors, incompetent persons, and other individuals in giving or withholding consent.

For a purpose for which the information may be disclosed to a public body under section 40, 42 or 43

Section 39(1)(c) This provision permits a public body to use personal information that has been disclosed to it by another public body under **section 40**, **42** or **43** of the Act.

For example, the Students Finance Board may disclose a student's financial information to a housing management body in order to verify the amount of rent being paid by the student (**section 40(1)(l)**). The housing management body can use the financial information disclosed by the Students Finance Board in order to verify the rental amount. The housing management body cannot use the personal information for any other purpose unless that use for the other purpose is authorized under another provision of **section 39**.

Section 39(1)(c) also allows a public body to use personal information disclosed to it for research purposes by another public body under **section 42** or by the Provincial Archives or the archives of another public body under **section 43**.

Information in alumni records of a post-secondary educational body for fund-raising

Section 39(2) and (3) This provision states that a post-secondary institution may use personal information in its alumni records for the purpose of its own fund-raising. Post-secondary educational bodies should have procedures in place to inform new alumni of this use at the time of graduation. They should not rely on this provision, which was added to the Act in May 1999, to use the personal information of individuals who become alumni after 1999 for their fund-raising activities.

The use of this personal information is qualified by **section 39(3)**. This requires the public body to discontinue using an individual's personal information for fund-raising purposes when requested to do so by that individual.

Post-secondary educational bodies should take reasonable steps to inform their alumni of this provision, for example, placing a notice in a prominent place in the institution's alumni newsletter to give individuals a chance to request cessation of the activity, or providing alumni with an opportunity to request cessation of the activity when mailing lists are updated, or mailing a notice to all alumni. For more

information on this topic, see FOIP Bulletin No. 5: *Fund-Raising*, published by Access and Privacy, Service Alberta.

Limit on use of personal information

Section 39(4)

Section 39(4) sets some limits on the extent to which a public body can use the personal information in its custody or control.

A public body can use information only to the extent necessary to carry out its purpose in a reasonable manner. This limitation applies both to the amount and type of personal information being used.

This provision is intended to ensure that public bodies to which personal information is disclosed use the minimum amount of information necessary to achieve their purposes.

For example, employees in a particular program area who have access to personal information in an electronic database should be provided with access to only those data elements they require to do their job, not to the whole database. Employees could be given access to certain views or screens in a database, rather than access to the entire database.

It may be possible to anonymize data (e.g. by stripping identifiers) so that employees without access to the personal information can manipulate and analyze the data. Only a few authorized staff would have access to the individually identifying information that is initially collected, and a unique identification number could be assigned to the information or to the data subjects. The non-identifying data can then be used for various analytical or reporting purposes within the organization.

In a reasonable manner means in such a way that a public body is not required to implement overly restrictive procedures on the use of personal information when the information is not of a sensitive nature or when the use by others in the organization would not be an unreasonable invasion of personal privacy.

Section 39(4) mirrors the limitation provision with respect to the disclosure of personal information in **section 40(4)**.

7.7 Disclosure of Personal Information

Section 40 of the Act lists the only circumstances under which public bodies may disclose personal information. **Section 40** provides for a response to an access request under **Part 1**, and for disclosure in the course of various administrative processes and in response to informal access requests.

Disclosure of personal information may occur *only* in the specific circumstances outlined in **section 40**. If **section 40** does not provide authority for a disclosure, the public body cannot disclose the information.

In *IPC Investigation Report 2001-IR-002*, the Investigator found that personal information about an investigation that was discussed at an *in camera* council meeting should not have been disclosed to a journalist since the disclosure was not authorized by any of the disclosure provisions of the Act.

Section 40 does not authorize disclosure of personal information on the basis that a third party may obtain access to that information through other means (see *IPC Investigation Report F2002-IR-005*).

Section 40 *enables* disclosure; it *does not require* disclosure. This is indicated by the word *may* in the introduction to the section. Public bodies should look at the circumstances surrounding each request and the privacy protection objectives of the Act when deciding whether to disclose personal information.

Section 40(4) states that a public body may disclose personal information only to the extent necessary to enable it to carry out the purposes described in **section 40(1)**, **(2)** and **(3)**. These purposes are described in the following pages. Disclosure has to be carried out in a reasonable manner.

Public bodies should be careful to disclose only limited amounts of personal information.

For example, when a school division issued a letter to staff, students and parents regarding the death of a student, it should have simply notified them about the death and advised parents and staff of resources available to help the students. The school division should not have provided details about the death (see *IPC Investigation Report F2003-IR-002*). In *IPC Investigation Report F2004-IR-002*, a school district was found to have disclosed too much information when reports sent to parents about their children's alleged misbehaviour contained information about other students involved in separate incidents. (See also *IPC Order F2004-010.*)

Public bodies have a responsibility in most cases to clarify and understand the reasons for the request for disclosure. Disclosures should be made in a way that helps the requester and is cost-effective for the public body. This may mean that not all disclosures are in writing, or that, when a working relationship with another body has been established, all the proofs required are not asked for each time a request is made.

Disclose means to release, transmit, reveal, expose, show, provide copies of, tell the contents of, or intentionally or unintentionally give personal information by any means to someone.

Although the Act applies to *recorded* information, **section 40** is not limited to the disclosure of *records*. Disclosure includes oral transmission of recorded information by telephone or in person; provision of personal information on paper, by facsimile copy or in another format; and electronic transmission through electronic mail, data transfer or the internet.

Section 40 provides for disclosure

- to the person whose information it is, either in response to a routine request for information or in response to a request under **Part 1**;
- to an individual's personal representative who is entitled to exercise the rights of that individual under **section 84** of the Act;
- to any other person in response to an access request; as a disclosure in the public interest (**section 32**); when the disclosure would not be an unreasonable invasion

of privacy (**section 40(1)(b)**), or when **section 40** of the Act specifically allows the disclosure; or

- to other public bodies, to legislative, legal and judicial officers, to other levels of government, or to non-government organizations (in some cases the disclosure supports the activities of the public body disclosing the information; in other cases the disclosure supports the activities of the party receiving the information).

Section 40 does not prevent the routine disclosure of an individual's personal information to that individual if the public body has adopted a policy of disclosing a particular category of personal information. In these circumstances, the public body will provide the personal information without a FOIP request.

Public bodies must keep a record of the purposes for which personal information held in any personal information banks may be disclosed (**section 87.1(2)(d)**) (see section 7.11 of this chapter).

Public bodies must also keep a record of any disclosures of personal information made under **section 40** for a purpose not included in the Directory of Personal Information Banks (**section 87.1(3)**). This may consist of a note on a file or a flag in an electronic system that refers to a paper record or another data file.

A record of a disclosure is needed to enable a public body to comply with its obligation under section 36(4) to inform anyone to whom it has disclosed personal information, of any correction to that information.

As a best practice, a record of a non-routine disclosure may include

- the name of the individual whose personal information is requested;
- the nature of the requested information and the purposes for which it will be used;
- the authority for the disclosure;
- the title, business address and business telephone number of the contact person in the requesting public body or agency; and
- the name and signature of the officer or employee of the public body who authorizes the use or disclosure.

Public bodies must have appropriate administrative controls in place to ensure that personal information is disclosed only to authorized persons.

When developing a new program, public bodies should consider whether personal information will need to be disclosed, and ensure the disclosure is authorized under the Act. Public bodies should also regularly review their disclosure policies and practices to ensure that they continue to meet the requirements of the Act. Where it is found that disclosures are not authorized, practices should be altered to meet legal requirements or discontinued. A review may be carried out in conjunction with a review of information practices and systems as discussed in Chapter 9.

Public bodies may disclose personal information only for the following purposes. Each permitted disclosure is outlined and discussed.

Disclosure in accordance with Part 1 of the Act

Section 40(1)(a) This provision permits disclosure to respond to access requests and to comply with the public interest disclosure provisions of the Act. Under this provision, a disclosure may take place when

- an applicant has requested access to his or her own personal information, subject to the exceptions in **sections 16** to **29** and to the paramountcy provision in **section 5**;
- an applicant has requested access to records containing personal information about another individual and disclosure of the personal information does not constitute an unreasonable invasion of the privacy of the other individual under **section 17**, subject to other exceptions and to third party notification requirements; or
- **section 32** applies.

Disclosure that would not be an unreasonable invasion of a third party's privacy under section 17

Section 40(1)(b) This provision permits disclosure in the clearest of cases after a complete analysis has been carried out under **section 17** and a determination made that the personal information would not be excepted under **section 17** in response to an access request. If there is any doubt as to whether the disclosure would be considered an unreasonable invasion of personal privacy, the public body should have the person who asked for the information submit an access request under **Part 1** of the Act.

When another provision of **section 40** permits disclosure, the disclosure should be made under the other specific provision. Examples are: disclosure with the consent of the individual, disclosure required or authorized by an Act of Alberta or Canada, and disclosure for research purposes.

Section 40(1)(b) gives public bodies flexibility in responding to requests for personal information that clearly would be provided if a FOIP request were made. It allows for a more helpful and timely response to such requests.

In some circumstances, public bodies will be able to establish policies and practices for routine disclosure in response to requests for particular classes of personal information (e.g. school transcripts). Policies and practices may also be established as a result of active dissemination of personal information without a request (e.g. publishing an employee directory). In establishing such policies, public bodies should determine whether any of the other exceptions outlined in **Part 1** of the Act might apply to the information (see section 2.4 of Chapter 2 for a discussion of providing routine access to records or information).

Examples of classes of personal information for which a policy might be appropriate include

- information about employee classification, salary range, employment responsibilities and discretionary benefits (**section 17(2)(e)**);

- financial and other details of a contract to supply goods or services (**section 17(2)(f)**);
- information regarding permits or licences relating to commercial or professional activities or real property (**section 17(2)(g)**);
- details of discretionary benefits of a financial nature (**section 17(2)(h)**); and
- personal information about an individual who has been dead for 25 years or more (**section 17(2)(i)**).

Public bodies may charge a fee for such information. For more information on **section 17(2)**, see section 4.3 of Chapter 4.

Section 17(2)(j) deals with a range of disclosures that can be made if disclosure is not contrary to the public interest. Individuals have the right to request that the information outlined in this provision not be disclosed. For this reason, requests for personal information that fall within the scope of **section 17(2)(j)** need to be considered on a case-by-case basis. A public body may take into consideration who is making the request, and why, in deciding whether to disclose the information.

If an individual has requested that the information not be disclosed, it cannot be disclosed under **section 40** unless another provision in that section permits the disclosure and the public body decides to disclose the information in accordance with that provision.

If disclosing the information could interfere with law enforcement or could reasonably be expected to affect someone's health or safety, the information should not be disclosed.

For more information on situations when disclosure might be made, see section 4.3 of Chapter 4 and FOIP Bulletin No. 4: *Disclosure of Personal Information "Not Contrary to the Public Interest"*, published by Access and Privacy, Service Alberta.

Disclosure for original or consistent purpose

Section 40(1)(c) The *purpose* means the purpose for which personal information was collected under **section 33**. A public body can disclose personal information for that purpose. Typical purposes include the administration of a particular program, the delivery of a service and other directly related activities. Authority for collection is discussed in section 7.2 of this chapter.

Personal information is *compiled* when certain information is created and becomes tied to or is associated with an identifiable individual. For example, a public body creates or assigns a student ID number for each student. This information becomes the personal information of the student but the information was compiled by the public body, not collected from the student (see *IPC Order 2001-038*).

A *consistent purpose* is one that has a direct and reasonable connection to the original purpose and that is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that discloses the information (**section 41**). A disclosure is therefore permissible if it is a logical extension of the original use.

Examples of disclosure for a consistent purpose include

- providing a list of participants in a program to another part of a public body for evaluation of the program; and
- disclosing the name and mailing address of the property owner for other purposes related to the operation of the municipality such as providing services and utilities.

A more detailed explanation of *consistent purpose* is provided in section 7.8 of this chapter.

Disclosure with consent

Section 40(1)(d) This provision permits disclosure of an individual's personal information when the individual has identified the information and consented, in the manner prescribed in **section 7** of the FOIP Regulation, to the disclosure. This states that consent

- must be in writing; and
- must specify to whom the personal information may be disclosed and how the personal information may be used beyond the original purpose for which the personal information was collected or compiled.

To meet the minimum requirements under the Act, a form or other instrument requesting consent must

- **specify to whom the personal information may be disclosed; and**
- **specify how the personal information may be used.**

If consent is given in writing, the form must be signed by the person giving consent.

Consent may be given electronically or orally if the head of the public body has established a process for accepting electronic or oral consent that meets the requirements of section 7(5) or (6) of the Regulation, respectively.

As a best practice and where appropriate, a form or other instrument requesting consent should

- indicate the original purpose of the collection, as well as the additional purpose for which the information is to be used and for which consent is being provided;
- indicate that consent is voluntary;
- indicate that consent may be revoked, but identify, where possible, any limitations and any consequences or implications that may result from revocation;
- to the extent possible, identify any consequences that may result from refusal to consent; and
- indicate the period of time during which the consent remains valid.

Examples of consent to disclosure include: consent to have references provided in support of job applications; consent to provide information to the Canada Revenue Agency in order to obtain income verification from that source; and consent to the use of photographs for promotional purposes.

IPC Investigation Report 2000-IR-003 provides a discussion of the consent requirements under **section 40(1)(d)** and **section 7** of the FOIP Regulation. In that case, the Investigator found that an individual's consent to release information to a private landlord was not valid because the consent had been revoked prior to the time of disclosure.

When an individual copies ("cc"s) other parties on a letter or e-mail, this is not consent for the responder to disclose personal information to the parties who were copied (*IPC Orders F2002-018* and *F2005-014*).

When the person concerned has not indicated any consent to disclose personal information, and no other provision exists to permit disclosure, public bodies cannot disclose the information.

A public body must not penalize an individual for refusing to consent to a disclosure of personal information for a purpose other than the purpose for which the personal information was collected. A public body must not deny the individual the benefit or service for which the personal information was originally collected.

A public body should not seek consent for a disclosure that is already authorized elsewhere in **section 40**, unless it intends not to disclose the personal information without the individual's consent.

Consent to a disclosure may be given by a representative acting on behalf of an individual in accordance with the conditions set out in **section 84(1)**. These conditions are discussed in detail in section 2.5 of Chapter 2.

Consent for a disclosure should be sought as early as possible after the need has been identified. Ideally, it should be sought at the time the information is collected. In such cases, the request for consent to disclose is added to the collection instrument. For more information on this topic, see FOIP Bulletin No. 17: *Consent and Authentication*, published by Access and Privacy, Service Alberta

Disclosure to comply with an enactment of Alberta or Canada or with a treaty, arrangement or agreement under an enactment of Alberta or Canada

Section 40(1)(e) This provision permits disclosure of personal information to comply with an Act of Alberta or Canada, a regulation made under such an Act, or with a treaty, arrangement or agreement made under either an Act or a regulation. It does not apply to the legislation of other provinces, territories or foreign states.

Disclosure to *comply with an enactment of Alberta or Canada* means disclosure of personal information as *required* by either provincial or federal legislation. There

must be a direct relationship between complying with the enactment and the disclosure of the personal information.

Disclosure to *comply with a treaty, arrangement, or agreement* made under an enactment of Alberta or Canada means disclosure of personal information as *required* by the treaty, arrangement or agreement. The enactment must provide authority for the provision in the treaty, arrangement or agreement, and that provision must specifically authorize disclosure of the personal information.

A *treaty* is a formally concluded and ratified agreement between or among independent states. Only the federal government of Canada has the power to conclude treaties with foreign countries. An example of a treaty permitting the exchange of personal information is the *Mutual Legal Assistance Treaty*, which provides for the exchange of information on a variety of law enforcement matters.

An *arrangement* is a coming to terms on how certain matters will be conducted, particularly if there is no formal agreement documenting this. Often administrative arrangements are managed without an agreement but there must still be authority under an enactment for entering into the arrangement, for the purposes of **section 40(1)(e)**. Arrangements should, whenever possible, be in writing. A verbal arrangement should be allowed only in very exceptional circumstances, such as sensitive law enforcement, security or intelligence matters, and only at the insistence of one or more of the parties. Where an arrangement is unwritten, disclosures should be approved at a senior level within the public body.

An *agreement* documents the obligations and responsibilities of the parties and what actions are to be taken. For the purposes of **section 40(1)(e)**, authority for the agreement or for entering into the agreement must be contained in an enactment of Alberta or Canada. *Agreements* include contracts, memoranda of understanding, collective agreements, etc. All agreements should be in writing.

Agreements concerning the disclosure of personal information by public bodies to other organizations, including federal, provincial, municipal, and foreign governments, as well as international bodies, should contain

- a description of the personal information to be collected or disclosed;
- the authority for collecting, using and/or disclosing personal information;
- the purposes for which the information is to be collected, used or disclosed, including a restriction on subsequent uses;
- a statement of all the administrative, technical and physical safeguards required to protect the confidentiality of the information, especially with respect to its use and disclosure;
- a statement specifying whether information received by a public body will be subject to the provisions of the *FOIP Act* or, for other jurisdictions where comparable legislation exists, whether that legislation will apply;
- a statement that the disclosure of the personal information will cease if the recipient is discovered to be improperly disclosing the information collected from the public body; and

- the names, titles and signatures of the officials in both the supplying and receiving public bodies who are responsible for the terms of the agreement, the date of the agreement and the period for which it is in effect.

Examples of such agreements include agreements for

- the exchange of personal information about individuals who have applied for social assistance from the Province with Human Resources and Social Development Canada to determine whether they are also receiving employment insurance;
- the exchange of personal information about applicants for the Alberta Seniors Benefit with Alberta Health and Wellness so that applicants can obtain seniors' health benefits; and
- the disclosure of personal information by schools to health authorities for the purpose of immunization and other preventive health services.

Public bodies should maintain a list of all agreements, arrangements and treaties, as applicable, under which they disclose personal information. Public bodies should include information disclosed under agreements, arrangements and treaties in the relevant personal information bank descriptions contained in the directory of personal information banks which the Act requires to be published by the public body (**section 87.1(2)(d)**).

For further information, see section 9.7 of Chapter 9 and *Guide to Developing Personal Information Sharing Agreements*, published by Access and Privacy, Service Alberta.

FOIP Bulletin No.15: *Disclosure of Personal Information to Unions: Before a First Agreement*, published by Access and Privacy, Service Alberta, discusses whether the personal information of employees may be disclosed to a union before a collective agreement is in place. It also discusses the more general issue of applying the *FOIP Act* to the disclosure of employee personal information to unions under a collective agreement.

Disclosure that is authorized or required by an enactment of Alberta or Canada

Section 40(1)(f) This provision is related to **section 40(1)(e)**. However, whereas in **section 40(1)(e)** disclosure must be *for the purpose of complying* with an enactment, and is therefore likely to be required by law, in **section 40(1)(f)** disclosure is permitted if it is either required or *authorized* by an enactment of Alberta or Canada. If disclosure of personal information is authorized – but not required – by an enactment, the head of the public body has more discretion as to whether or not to disclose the information.

Examples of Acts that *require* disclosure of personal information include the *Legislative Assembly Act*, the *Public Lands Act*, the *Public Trustee Act* and the *Maintenance Enforcement Act*.

Some Acts require a particular public body to disclose personal information for the purpose of the (disclosing) public body's program. For example, section 50 of the *Public Lands Act* requires the Minister responsible for that Act to disclose certain personal information to the public as part of the enforcement process.

If a public body is relying upon **section 40(1)(f)** as authority to disclose personal information, it must ensure that the disclosure is strictly in compliance with the enactment that authorizes the disclosure. For example, in *IPC Investigation Report 99-IR-008*, the Information and Privacy Commissioner's investigator found that the disclosure contravened the *Workers' Compensation Act* because it was a disclosure of information that was not relevant to the administration of the *Workers' Compensation Act* or its regulations.

Some Acts require *other* bodies to disclose personal information to a particular public body for the purposes of the (collecting) public body's program. For example, under the *Public Trustee Act*, section 44, the Public Trustee may compel a public body that has possession of personal, financial or health-related information about a client or potential client to provide that information or record to the Public Trustee to carry out a task, duty or function relating directly to the client or potential client.

Sections 12 and 13 of the *Maintenance Enforcement Act* require a list of personal information (e.g. financial information, an identification number issued by a province) to be disclosed to the Director of Maintenance Enforcement by government departments, provincial agencies (e.g. post-secondary institutions) as well as business organizations (including municipalities). Only the requested information that is listed in that Act should be disclosed by a public body and collected by the Director.

Examples of Acts that *authorize* disclosure of personal information include the *Charitable Fund-raising Act*, the *Workers' Compensation Act* and the *Dependent Adults Act*.

Before disclosing personal information under **section 40(1)(f)** in response to a request, a public body should ask the body requesting the information to provide their legal authority for collecting the information. A public body requesting personal information from another body should provide the disclosing body with their legal authority for collecting the information.

Disclosure to comply with a subpoena, warrant or order

Section 40(1)(g) This provision permits personal information to be disclosed in order to comply with legal processes that require the production of information. These processes include the use of a subpoena, warrant or order issued or made by a court, person or body having jurisdiction in Alberta to compel the production of information, or with a rule of court binding in Alberta that relates to the production of information.

A *subpoena*, also called a "summons to witness," is a command issued by a party in litigation requiring the attendance of someone as a witness at a court proceeding or hearing. It will specify a certain place and time when testimony on a certain matter will be required, and may also order a person to meet the requirements of a court to disclose information.

Time is usually of the essence in dealing with a subpoena, as it is often served with very little notice. Public bodies cannot ignore subpoenas since they would risk being cited for contempt of court and, at a minimum, fined.

A *warrant* is a judicial authorization to collect information – in this context, personal information.

An *order* is an authoritative command, direction or instruction to produce something – again in this context, personal information.

The court or tribunal must have jurisdiction in Alberta to require a public body to disclose information. Courts with jurisdiction in Alberta include the Supreme Court of Canada, the Court of Appeal of Alberta, the Court of Queen's Bench of Alberta, the Provincial Court of Alberta, as well as the Federal Courts.

Where a tribunal has the power to compel the production of information under legislation of Alberta or Canada, that tribunal has jurisdiction in Alberta. An example of a federal tribunal with jurisdiction in Alberta is the Canadian Radio-Television and Telecommunications Commission.

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, or a court procedure that makes an order filed with a court in Alberta enforceable as an order of the Alberta court (e.g. Alberta's *Interprovincial Subpoena Act*).

The *FOIP Act* also establishes offences and penalties for disclosure in response to a subpoena, warrant or order if the disclosure is not permitted under **section 40(1)(g)**, and no other provision of the *FOIP Act* permits disclosure. For further information on offences under the *FOIP Act*, see section 2.11 of Chapter 2.

Although **section 40(1)(g)** enables, but does not require disclosure, public bodies normally comply with orders, warrants or subpoenas because they have the force of law. However, a public body should not automatically assume that an order, warrant or subpoena is valid in Alberta.

Public bodies should consult their legal advisor when they receive a court order, warrant or subpoena in order to determine whether it refers to information that is actually in the custody or under the control of the public body, whether the instrument has been served properly, whether the court has jurisdiction in Alberta and whether there is some compelling reason to oppose the order, warrant or subpoena. They will also need to ensure that the amount and type of information disclosed is actually required by the instrument.

Disclosure to an officer or employee of the public body, or to a member of Executive Council

Section 40(1)(h) This provision permits disclosure of personal information to officers or employees of the public body that has custody or control of the personal information, and to Cabinet members. It does not allow disclosure to employees or officers of other public bodies.

An *employee* is defined in **section 1(e)** of the Act to include a person retained under contract to perform services for the public body, a volunteer and an appointee to a board or committee.

Members of a school council are not employees of a school board for the purposes of the *FOIP Act* (*IPC Order 2001-010*) but school volunteers are employees (*IPC Investigation Reports 98-IR-015 and 2001-IR-005*).

The term *officer* is included to ensure that all persons working for a public body in any capacity are encompassed by the provision. This includes an elected official, such as a school board trustee, when the official is acting on behalf of the public body to carry out the mandate and functions of the public body, as opposed to functioning as a representative of his or her constituents (see *IPC Order 99-032*).

A *member of the Executive Council* includes the President of Executive Council, a Minister, and an Associate Minister (described in the *Legislative Assembly Act* as a "Minister without Portfolio").

Section 40(1)(h) does not allow an official or employee or member of the Executive Council to have automatic access to all personal information within a public body.

The test for disclosure is whether the information is necessary for the performance of duties. Disclosure is permissible only if access to the particular personal information is needed to do a job or deal with a particular situation.

The persons to whom the information is disclosed should be able to prove a need to see, or handle the personal information in order to do their jobs. The following are some examples of cases where disclosure might be necessary for the performance of an employee's duties.

- Human Resources may require access to the résumes of applicants in order to carry out the recruitment function.
- Where there is a formal process within a public body to do so, an employee may need to report a suspected fraud (e.g. an alleged contravention of the Government of Alberta's Code of Conduct and Ethics).
- Service counter staff may need to be informed if a client has a history of acting violently when interacting with departmental staff and if there is a need for extra security when the individual approaches the office.
- A counsellor may require access to student records to provide assistance, at the request of a teacher, to a student who is not doing well in school.
- The head of a local public body may require information to prepare a report for the governing body.
- A Minister may need background information about an issue and the people he or she is meeting with in order to understand the problem and their needs.

An example of a permitted disclosure under **section 40(1)(h)** was the disclosure of the nature of a complaint against an employee under **section 40(1)(h)** to another staff

member, since the information was necessary for that staff member to fulfil his duties of assigning employees to working groups (*IPC Investigation Report 99-IR-005*).

In another example of permitted disclosure, a school board disclosed a letter responding to a complaint to its Superintendent. The Superintendent was an officer or employee of the school jurisdiction and one of his duties was to review complaints made about the jurisdiction. Without knowledge of the personal information in the matter, the Superintendent could not properly perform his duty (*IPC Order F2002-018*).

Disclosure for a common or integrated program or service

Section 40(1)(i) This provision is similar to **section 40(1)(h)**, but permits disclosure to officers or employees of *another* public body when two or more public bodies are working together to provide or deliver a common or integrated program or service. The disclosure must be necessary for the delivery of the program or service *and* for the performance of the duties of the receiving employee, official, or member of Executive Council. **Section 40(1)(h)** does not allow disclosure to an organization that is not a public body (e.g. for a program offered in partnership with a private contractor).

A *common or integrated* program or service means a single program or service that is provided or delivered by two or more public bodies; or a program or service that has several distinct components, each of which may be provided or delivered by a separate public body, but which together constitute the program or service.

Each public body partner must be integral to the program or service. For example, a nursing practicum program requires the participation of both the post-secondary institution, and the health care body; the program would not function without the services of each body. In contrast, an arrangement where several public bodies contract with the same information technology service provider is *not* a common or integrated program or service.

Section 40(1)(i) allows for the sharing of personal information between the public bodies in order to deliver the service to the clients. A common client does not, of itself, meet this definition. Factors that will determine whether or not a program or service meets the definition include

- evidence of joint planning;
- a formal agreement or legislative authority for working together;
- common goals expressed by the partners; and
- evidence of collaboration or cooperation in delivery.

When public bodies are implementing such programs or services, they should

- disclose information in non-identifiable form whenever possible;
- ensure that individuals participating in the program are notified of all the partners and of the sharing of personal information;
- disclose personal information only to those who need to know about a particular individual;

- disclose personal information only to the extent necessary for program or service delivery; and
- ensure that personal information is not used for any other purpose.

Examples of such programs and services include

- children's service initiatives delivered through Child and Family Service Authorities;
- conjoint nursing programs that require the disclosure of personal information between program departments of different post-secondary institutions;
- work placement and practicum programs;
- school-housed public libraries; and
- centralized human resource programs.

For further information, see FOIP Bulletin No. 8: *Common or Integrated Programs or Services*, published by Access and Privacy, Service Alberta.

Disclosure to enforce a legal right of the Government of Alberta or a public body

Section 40(1)(j) This provision permits the disclosure of personal information to enforce a legal right that the Government of Alberta or a public body has against any person.

The Information and Privacy Commissioner considered criteria for applying this provision in *IPC Order F2005-002*. In that Order the Appeals Commission for Workers' Compensation owed a common law duty of fairness to the parties appearing before it. The Workers' Compensation Board was enforcing its legal right to a fair hearing when it disclosed personal information about a member of the Commission in a complaint alleging bias on the part of the member.

In most cases, the disclosure of personal information under this provision will be to the legal representatives of the public body or, in the case of public bodies such as government departments, to Alberta Justice and the Minister of Justice and Attorney General as the provincial government's legal representative. The legal rights may relate to civil or criminal law.

Disclosure to collect a fine or debt or to make a payment

Section 40(1)(k) This provision permits disclosure of personal information to

- collect a fine or debt owing to the Government of Alberta or a public body or an assignee of either of them; or
- make a payment owed by the Government of Alberta or a public body.

A *fine* is a monetary punishment imposed on a person who has committed an offence, including an offence under a bylaw.

A *debt* is something that is owed, usually money, where the individual has an obligation to pay and the creditor has the right to receive and enforce payment.

An *assignee* is the person who has been given, or assigned, the right to receive and enforce the fine or debt.

Documentation for the disclosure under this provision should be in writing and specify

- the nature of the information to be disclosed;
- the name of the public body, person or organization receiving the information;
- any other necessary identifying information, such as a case or file number;
- the purpose of the request, including a citation of the legal authority for collecting the fine or debt; and
- the name, title and business address of the official making the decision to disclose.

The provision permits disclosure to Crown Debt Collections of Alberta Finance and Enterprise or to a private collection agency to which the debt has been assigned. It does not permit disclosure to assist a collection agency, or any other person or organization that is not a public body, to collect a debt owed to another public body, or to person or organization that is not a public body.

This provision enables public bodies to disclose personal information for the collection of a fine or debt owed to the Government of Alberta or a public body, or to make a payment owed by the Government of Alberta or a public body. Many public bodies have authority to collect fines and debts in their legislation, and some legislation also authorizes a public body to disclose personal information to another public body for the collecting body's purposes. This provision is intended to assist public bodies in cases where their legislative mandate does not specifically extend to the disclosure of personal information for the purposes of collecting fines and debts. **Section 40(1)(k)** gives them an authority to pursue these activities.

Section 40(1)(k) does not permit information to be disclosed by a public body for the purpose of determining whether a fine, debt or a benefit is owed. This decision must be made before the information is disclosed.

The information disclosed should be the minimum needed to collect the debt. Usually this will be the name, last known address and telephone number, and any contact information provided by the individual. It is generally not necessary to disclose the reason for the fine or debt (e.g. a penalty imposed as a result of an offence under an Act).

Disclosure of personal information under section 40(1)(k) should always be in writing.

The provision also authorizes public bodies to disclose personal information for the purpose of making a payment owing by the Government of Alberta or by a public body to an individual (**section 40(1)(k)(ii)**). For example, the name of the individual, the amount of the payment to be made and the transaction number would need to be disclosed to Alberta Finance and Enterprise or to its agent, Payment Systems Corporation, in order to generate the cheque for the payment.

Disclosure to determine or verify suitability or eligibility for a program or benefit

Section 40(1)(l) This provision permits the disclosure of personal information to determine an individual's suitability or eligibility for a program or benefit, or to verify continuing eligibility for the program or benefit.

Section 40(1)(l) allows personal information to be disclosed when there is a need to determine whether or not an individual meets the eligibility or suitability criteria for a particular program or benefit. A public body may disclose personal information to another public body, or to an organization or institution, to allow the disclosing public body to determine or verify suitability or eligibility.

Normally, disclosure will only be made after an individual has applied to participate in a program or for a benefit. Public bodies collecting this information should comply with the guidelines set out in sections 7.1, 7.2 and 7.3 of this chapter.

Eligibility means whether a person qualifies for a program or benefit.

Suitability means the characteristics of an individual that enable him or her to be chosen for a program or benefit.

Examples of disclosures that might be permitted under this provision include

- verification of employment information when someone applies for employment insurance or employment counselling;
- disclosure of information from a seniors' lodge to a health authority to determine suitability for nursing home care;
- confirmation of membership in a library when an individual uses his or her library card in another library; and
- disclosure of information about attendance or marks to enable a second year of grant support to a student.

Disclosure for audit purposes

Section 40(1)(m) This provision permits the disclosure of personal information for audit purposes to the Auditor General (Alberta) and to other persons and bodies specified in the FOIP Regulation.

The *Auditor General* is an Officer of the Legislature appointed by the Lieutenant Governor in Council. The role of the Auditor General is to examine the accounts and records of the government relating to the consolidated revenue fund and all public money, including trust and special funds under the management of the government relating to public property. The Auditor General must report annually to the Legislature on his or her work, including findings as to whether or not departments and other public bodies have carried out their financial responsibilities. This provision does not apply to the Auditor General of Canada.

For audit purposes means for the purposes of carrying out a financial or other formal and systematic examination or review of a program, portion of a program or activity that includes personal information about individuals, provided such examination or review is sanctioned by statute, regulation or public policy relating to the public body (**section 8** of the FOIP Regulation). In the case of a local public body, the audit may be sanctioned by bylaw or resolution. Audit purposes do not include operational or administrative purposes such as verification of a claimant's eligibility for a program, benefit or service, where a decision would be made about a specific individual.

The persons to whom personal information may be disclosed for audit purposes are also specified in **section 8** of the FOIP Regulation. Disclosure may be made to persons who are employees of a public body, including a person retained under contract to perform services for the public body for audit purposes (as defined above).

When a contractor is hired to conduct an audit requiring disclosure of personal information under this provision, the contractor should be advised of, and agree to abide by, the provisions of the *FOIP Act*, as well as policy relating to the protection of privacy under the *FOIP Act*. For further information on contracting under the *FOIP Act*, see *Managing Contracts under the FOIP Act: A Guide for Government of Alberta Contract Managers and FOIP Coordinators*, published by Access and Privacy, Service Alberta.

Examples of disclosures that may be permitted under this provision include:

- disclosure to the Office of the Chief Internal Auditor of the Government of Alberta, and internal auditors of a municipality;
- disclosure to an accounting or audit firm engaged to conduct a financial audit of a public body;
- disclosure to a person auditing methods a housing management body uses to determine eligibility for low income housing; and
- disclosure for personnel audits, such as classification reviews or quality assurance audits of the work being performed.

Disclosure to a Member of the Legislative Assembly

Section 40(1)(n) This provision permits disclosure of an individual's personal information to a Member of the Legislative Assembly if the individual has requested assistance from the Member in resolving a problem.

A *Member of the Legislative Assembly (MLA)* is a person elected as a representative of a constituency within the province of Alberta to represent the interests of the voters in that constituency in the Legislative Assembly.

This provision permits disclosure only to Members of the Legislative Assembly of Alberta, and only to assist the person concerned to resolve a problem.

The provision *does not* permit the disclosure of personal information to federal Members of Parliament or municipal representatives. These representatives may, however, obtain personal information about an individual with his or her consent.

The purpose of disclosure under **section 40(1)(n)** must be to *assist in resolving a problem*. This includes helping an individual to provide information to a public body, inquiring about decisions or about a service or benefit, or correcting a mistake or misunderstanding. Where resolution of the problem is relatively straightforward, the public body can discuss the issue with the MLA and, with his or her agreement, simply call the individual concerned and provide the information directly.

The written consent of the individual concerned is not normally necessary for disclosure to MLAs under this provision. If possible, the enquiry and disclosure should be recorded in writing. Where enquiries and disclosures take place orally, the transactions should be noted on the person's file.

In cases where the information is particularly sensitive (e.g. medical, financial or law enforcement information), the public body may wish to obtain the written consent of the individual concerned before disclosing the information.

Public bodies should have a policy in place for disclosure of personal information and should inform MLAs of their policy if a request is received for information.

It is likely that the MLA will pass the personal information he or she receives from a public body to the individual concerned. Under this provision, public bodies can only disclose evidence of the request for assistance and personal information about the individual requesting assistance. Public bodies should also be cautious not to disclose personal information about third parties, such as the individual's family members under this provision.

Disclosure to a representative of a bargaining agent

Section 40(1)(o) This provision permits disclosure of personal information to a representative of a bargaining agent who has been authorized in writing by the employee the information is about to make an enquiry.

Bargaining agent refers to a union or other organization that negotiates on behalf of workers with their employers for improvements in pay, hours, benefits, and other working conditions, and that works to protect the rights of employees.

The individual must sign and date a statement of authorization or representation clearly stating to whom the information may be disclosed and for what purpose. Disclosure is limited to personal information that is necessary for the purpose of making an enquiry. The representative may receive only that personal information that the employee has specifically authorized for release.

The representative, unless duly authorized as the employee's representative, may not exercise the employee's right of access to the rest of his or her personal information. Nor can he or she exercise the right to request correction of the employee's personal information.

Public bodies should ensure that their employees understand the purposes of the Act with respect to protection of personal information and the way the Act is applied in circumstances where a bargaining agent requests information about an employee.

See also the discussion of **section 40(1)(e)** above for disclosure for the purpose of complying with a collective agreement made under an enactment of Alberta or Canada.

Disclosure for archival purposes

Section 40(1)(p) This provision permits disclosure of personal information to the Provincial Archives of Alberta or the archives of a public body for permanent preservation.

The *archives of a public body* means

- a public body's own archives, in which case the records will remain in the custody or under the control of that public body (e.g. the archives of most post-secondary institutions);
- the archives of another public body, to which records are transferred as authorized under **section 3(e)**, in which case custody and control of the records will normally be transferred to the archives; or
- an archival facility that operates under a contract or agency relationship with the public body (e.g. the Glenbow-Alberta Institute), in which case custody may be transferred but control must be retained by the public body.

This provision does not permit disclosure to private archives such as those run by a private museum or historical society.

Section 40(1)(p) permits the disclosure of personal information to the personnel of the archives to obtain an archival appraisal to determine what personal information may have long-term archival and historical value.

This provision also permits the transfer and deposit of the records in the Provincial Archives or the archives of a public body, for ongoing research purposes.

Disclosure by the archives is governed by **section 43** of the Act (see section 7.10 of this chapter).

Disclosure to assist law enforcement

Section 40(1)(q) This provision permits the disclosure of personal information to a public body or a law enforcement agency in Canada to assist in an investigation

- undertaken with a view to a law enforcement proceeding; or
- from which a law enforcement proceeding is likely to result.

Law enforcement is defined in **section 1(h)** of the Act and further explained in section 4.6 of Chapter 4.

A *law enforcement agency in Canada* includes a variety of agencies that are responsible for enforcing statutes. Examples of law enforcement agencies that are public bodies are Alberta Solicitor General (*IPC Order 96-007*), provincial and municipal police services, the Alberta Fire Commissioner's Office and provincial and municipal conservation services. The RCMP and First Nations' police services, Canada Revenue Agency and the Federal Superintendent of Financial Institutions are law enforcement agencies in Canada that are not public bodies.

Proceeding means an action or submission to any court, judge or other body having authority, by law or by consent, to make decisions.

A *law enforcement proceeding* is a proceeding that leads or could lead to a penalty or sanction under a statute or regulation. Law enforcement proceedings include not only formal court proceedings but also proceedings of administrative tribunals, such as the Alberta Labour Relations Board. The penalty or sanction can be imposed by the public body conducting the proceeding (e.g. the Environmental Appeals Board) or by another body (e.g. a court).

When disclosing personal information under **section 40(1)(q)**, the public body should satisfy itself that

- the requesting party is a public body within the meaning of **section 1(p)** or is a law enforcement agency;
- there is a law enforcement investigation and that the investigation has been undertaken in contemplation of a law enforcement proceeding as defined in **section 1(h)** (i.e. a proceeding that can result in a penalty or sanction under a statute or regulation); and
- the requesting public body or law enforcement agency can provide the legal authority for the law enforcement activity.

Under **section 40(1)(q)(ii)**, the disclosure of personal information must be to assist an investigation from which a *law enforcement proceeding is likely to result*. When disclosure is contemplated before an actual law enforcement proceeding is under way, it must be probable that a law enforcement proceeding will go forward.

Public bodies that are also custodians under the *Health Information Act* must follow the rules in that Act regarding the disclosure of individually identifying health information to a law enforcement agency.

A request by a law enforcement agency for personal information should be in writing and should be retained by the public body in support of any subsequent disclosure of personal information to that agency.

A model **Law Enforcement Disclosure Form** is provided in Appendix 5. Law enforcement agencies are encouraged to use this or a similar form when requesting disclosure of personal information.

Public bodies should ensure that requests for personal information from law enforcement agencies are justified and contain

- the name of the individual whose information is requested;
- the exact nature of the information desired;
- the authority for the investigation;
- the purpose for which the requesting agency will use the information; and
- the name, title and address of the person authorized to make the request.

The record of disclosure should normally be kept in a separate file that documents all requests for disclosure from law enforcement agencies, since this record may itself qualify for an exception under **section 20** of the Act.

For further information on the meaning of law enforcement, see FOIP Bulletin No. 7: *Law Enforcement*, published by Access and Privacy, Service Alberta.

Disclosure among law enforcement agencies

Section 40(1)(r) This provision permits a public body that is a law enforcement agency to disclose personal information

- to another law enforcement agency in Canada; or
- to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority.

This provision permits law enforcement agencies in Alberta to exchange personal information with their federal, provincial and municipal counterparts in Canada. Examples include the RCMP, provincial securities commissions and other police services.

As well, the provision permits disclosure to law enforcement agencies in foreign countries. This includes police forces and other law enforcement organizations in other countries, international law enforcement organizations and municipal and state police forces in foreign countries. Examples would be the Metropolitan Police in England, the Federal Bureau of Investigation and the United States Citizenship and Immigration Services, and Interpol.

Disclosures under **section 40(1)(r)(ii)** must be made in accordance with an arrangement, written agreement, treaty or legislative authority. The same conditions for an arrangement, agreement or treaty apply as for **section 40(1)(e)** described above.

Legislative authority means a statute, regulation or other legislative instrument.

Disclosure in case of injury, illness or death

Section 40(1)(s) This provision permits disclosure of personal information so that a spouse or adult interdependent partner, relative or friend of an injured, ill, or deceased individual may be contacted. For the meaning of these terms, see the discussion of **section 40(1)(cc)** below.

Section 40(1)(s) also allows disclosure of personal information such as whether the individual has been taken to a hospital or requires assistance to get home.

Disclosure in accordance with section 42 or 43

Section 40(1)(t) This provision permits the disclosure of personal information for research and statistical purposes. The conditions applicable to research disclosures are discussed in sections 7.9 and 7.10 of this chapter.

Disclosure to an expert for the purposes of section 18(2)

Section 40(1)(u) This provision allows a public body to fulfil its obligations under **section 18(2)** of the Act. It allows the expert to determine whether or not release of the applicant's own information to the applicant could reasonably be expected to result in immediate and grave harm to the applicant's health or safety.

Section 6 of the FOIP Regulation establishes conditions for the disclosure of personal information to a chartered psychologist or other appropriate expert as follows:

- the public body may disclose information relating to the mental or physical health of an individual to an expert for an opinion on whether disclosure of this information could reasonably be expected to result in immediate and grave harm to the individual's safety or mental or physical health;
- an expert to whom information is disclosed must not use the information except for the purposes of determining the harm described above;
- the public body must require an expert to whom the information will be disclosed to enter into an agreement relating to the confidentiality of the information; and
- if a copy of the record containing information relating to the mental or physical health of an individual is given to an expert for examination, the expert must, after giving the opinion, return the copy of the record to the public body or dispose of it in accordance with the agreement between the public body and the expert.

Disclosure for use in a court or quasi-judicial proceeding

Section 40(1)(v) This provision permits disclosure of personal information for use in a proceeding before a court or quasi-judicial body to which the Government of Alberta or a public body is a party.

A *quasi-judicial body* refers to a body whose members have a duty to hold a hearing; their decision affects the rights of the applicant; they use an adversarial process or proceeding to decide the issue before them; and they have an obligation to apply substantive rules (see *IPC Order 99-025*). A quasi-judicial body exercises judicial functions that are similar to that of a court or a judge. Examples of quasi-judicial bodies are the Alberta Labour Relations Board and the Alberta Transportation Safety Board. For more information about quasi-judicial bodies see section 1.5 in Chapter 1.

Section 40(1)(v) permits the disclosure of personal information to the legal representatives of the Government of Alberta or a public body for use in these proceedings. It also permits disclosure to the members of the quasi-judicial body or court.

Disclosure is normally to, or through, the legal representative of the public body or, in the case of public bodies that are government departments, Alberta Justice and Attorney General, which represents the provincial government in legal matters. Information may be disclosed to the legal representative of the other parties to a proceeding in accordance with the court disclosure and discovery rules that apply.

In cases where the Government of Alberta or the public body is not a party to the proceeding, **section 40(1)(f)** (disclosure in accordance with an enactment of Alberta

or Canada) may authorize or require disclosure. Examples of enactments that may authorize or require disclosure of personal information for use in a court or quasi-judicial proceeding include the Alberta Rules of Court (as interpreted by the courts), statutes governing the proceedings of administrative tribunals and statutes governing the disciplinary proceedings of professional regulatory organizations. See the discussion of **section 40(1)(f)** above.

Disclosure to a place of lawful detention

Section 40(1)(w) This provision permits the Minister of Justice and Attorney General or an agent or lawyer of the Minister to disclose personal information to a place of lawful detention in order to provide for the appropriate supervision of any individual detained in custody.

Disclosure for the management or administration of personnel

Section 40(1)(x) This provision allows a government department to disclose personal information about an employee or prospective employee, such as reference information, to another government department for the purpose of managing or administering personnel. The provision recognizes the provincial government as one employer for all provincial government departments.

Section 40(1)(x) also allows other types of public bodies to disclose the same kind of information *within* their own public body for the purpose of managing or administering their own personnel.

No disclosure of personal information is permitted to other public bodies or to the private sector without the written consent of the individual, unless the disclosure is authorized under another provision in section 40.

For example, if an employee of one school board asks for a reference about a prospective employee from the prospective employee's supervisor in another school board or in a post-secondary educational institution, disclosure of the reference information would require the prospective employee's consent.

Management of personnel refers to aspects of the management of human resources of a public body that relate to the duties and responsibilities of employees (*IPC Investigation Report 2001-IR-006*). This includes staffing requirements, job classification or compensation, recruitment and selection, salary, benefits, hours and conditions of work, leave management, performance review, training and development, occupational health and safety, and separation and layoff. For the Government of Alberta, the term includes the government-wide network managed through Corporate Human Resources. It does not, however, include the management of contracts for consultants, professionals or independent contractors.

Section 40(1)(x) does not permit disclosure of employment-related personal information to a prospective outsource operator during negotiations for privatization without the employees' consent. In *IPC Investigation Report 2001-IR-006*, the Investigator found that such a disclosure was not made for the purpose of managing the public body's personnel and was therefore not authorized by **section 40(1)(x)**.

Administration of personnel comprises all aspects of a public body's internal management, other than management of personnel, necessary to support the delivery of programs and services. Administration includes business planning, financial, materiel, contracts, property, information and risk management (*IPC Investigation Report 2001-IR-006*).

Employees should be informed, in a general way, of how they should expect their personal information to be collected, used and disclosed within the personnel management system. Disclosure of personal information for the purposes of the management or administration of consultant, or professional or other personal service contracts should be addressed in the terms of the contracts.

Disclosures under section 40(1)(x) are permitted only within the official framework that governs the management and administration of personnel within a public body or across the Government of Alberta.

Disclosure of personnel information is discussed in more detail in the publication produced for local public bodies by Access and Privacy, Service Alberta, entitled *Human Resources Guide for Local Public Bodies*.

Disclosure to enforce maintenance orders

Section 40(1)(y) This provision permits the disclosure of personal information about individuals to the Director of Maintenance Enforcement for the purposes of enforcing a maintenance order under the *Maintenance Enforcement Act*.

The information disclosed may be about an individual who is the subject of a maintenance order or an individual who is the beneficiary of a maintenance order. For example, the Director of Maintenance Enforcement may require information about the current registration of a student at a post-secondary institution in order to determine whether a parent is required to continue to provide financial support for that individual.

Sections 12 and 13 of the *Maintenance Enforcement Act* require the list of personal information (e.g. financial information, an identification number issued by a province) to be disclosed to the Director of Maintenance Enforcement by government departments, provincial agencies (e.g. post-secondary institutions) as well as business organizations (including municipalities). Only the requested information that is listed in that Act should be disclosed by a public body and collected by the Director.

The provisions also require provincial agencies to withhold support payments (e.g. student loan funds) to beneficiaries of provincial programs who have defaulted on maintenance support payments for a specified period of time. The provincial agency may be required to provide information about the beneficiary before paying out the funds.

Under this provision, a public body can only disclose personal information to the Director of Maintenance Enforcement or someone delegated to act on his or her behalf. A public body should require that the request be made in writing.

Disclosure to an officer of the Legislature

Section 40(1)(z) This provision permits the disclosure of personal information to an officer of the Legislature if the information is necessary for the performance of the duties of that officer. *Officers of the Legislature* are the Auditor General, the Ombudsman, the Chief Electoral Officer, the Ethics Commissioner and the Information and Privacy Commissioner (**section 1(m)** of the Act).

Disclosure of personal information under **section 40(1)(z)** must be necessary for the performance of the duties of the officer of the Legislature. If the reason for the disclosure is not clear from the request, public bodies should seek an explanation as to why the personal information is needed.

Section 13(1) of the *Election Act* requires the Chief Electoral Officer to establish a register of electors from which lists of electors may be compiled. Section 13(2) states that the register of electors may be created and revised using personal information held by a public body if, in the opinion of the Chief Electoral Officer, the information is necessary for the purposes of creating or revising the register.

In addition, section 13(2.1) requires public bodies to provide personal information from their records to the Chief Electoral Officer, if requested. The information in the register is limited to residential address, mailing address, postal code, surname, given name, middle initial, telephone number, gender, day, month and year of birth and any unique identifier assigned by the Chief Electoral Officer. Public bodies providing this information may charge a reasonable fee for providing the information but the fee may not exceed the actual costs of producing the information.

Section 13(2)(b.1) and section 13(2.1) of the *Election Act* in combination with **section 40(1)(z)** of the *FOIP Act* requires a public body to disclose personal information, as defined in the *FOIP Act*, requested by the Chief Electoral Officer for the purpose of creating or revising the register.

It should be noted that the *Election Act* does not require the disclosure of health information, including health registration information, as defined in the *Health Information Act*, by a public body that is also a custodian under the *Health Information Act*. **Section 40(1)** of the *FOIP Act* permits the disclosure of *personal information*; the Act does not apply to *health information* that is subject to the *Health Information Act* (**section 4(1)(u)** of the *FOIP Act*).

Information may also be disclosed under **section 40(1)(z)** for the purpose of a review of a privacy complaint by the Information and Privacy Commissioner, or an investigation by the Ombudsman at the request of an individual. As with many of the permitted disclosures, a best practice would be to ask the officer to put the request in writing so the public body would have on file a record to support any subsequent disclosure to the officer.

Disclosure for supervision of an individual by a correctional authority

Section 40(1)(aa) This provision permits the disclosure of personal information about an individual for the purpose of supervising the individual while he or she is under the control or supervision of a correctional authority. The individual may be in a correctional

institution or may be under the supervision of a correctional authority in the community.

If a community service organization is providing services to an individual who is under the control or supervision of a correctional or parole authority, this provision would permit, but not require, a public body, such as Alberta Solicitor General and Public Security, to disclose personal information to the service organization about an individual's history, release or supervision. The information disclosed would have to be necessary for the service being provided. The organization would be prohibited from any subsequent or secondary disclosure of that information, unless the disclosure was authorized by law.

Supervision includes any community disposition requiring supervision of an offender, including probation, bail supervision, parole, temporary absence, and ordered community service work, as well as supervision of individuals held in a correctional institution.

Disclosure of information available to the public

Section 40(1)(bb) This provision permits personal information to be disclosed when that information is available to the public. It applies to information that has been published in any form or which constitutes or is a part of a record that is publicly available.

The provision covers situations where the information to be disclosed is already in the public domain; the public body need not have necessarily *collected* the information from a public source.

It is important, however, to assess carefully just how public the information is. For example, just because personal information about an individual has been published in the media does not mean that the information should automatically be treated as public and disclosed freely. If a public body is contemplating making this type of disclosure, it should take into consideration the possibility that the individual involved might still find such disclosure an unreasonable invasion of his or her privacy (see *IPC Order 99-032*).

Particular caution should be exercised when disclosing information that is publicly available on the Internet. A public body should ensure that any personal information that it is considering disclosing under **section 40(1)(bb)** was collected in accordance with **section 33** of the Act, that indirect collection was authorized under **section 34(1)** and that, if the information was used to make a decision directly affecting an individual, the public body made every reasonable effort to ensure the accuracy and completeness of the information, as required by **section 35(a)**.

Examples of public information that might be disclosed under this provision include:

- individual employee information in a corporate telephone directory available for purchase or freely available on the Internet;
- biographical information about board appointees published in a newsletter;
- details of a personal service contract approved in a council meeting;
- a retirement notice or information of a school superintendent mentioned in public board minutes; and

- information in court decisions published in law reports (see *IPC Order 98-001*).

Disclosure of business contact information

Section 40(1)(bb.1) This provision permits a public body to disclose personal information 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 e-mail address, and
- does not reveal other personal information about the individual or personal information about another individual.

This provision permits, but does not require, public bodies to disclose the names and business contact information of individuals (including e-mail address) if doing so would not reveal other personal information.

For example, a public body may

- publish an employee directory on its website;
- distribute a list of consultants providing professional services in the public body's area of operations, for example, at the request of another public body or a business;
- provide a list of participants in a consultation process involving a public body's business stakeholders; or
- provide a list of e-mail addresses of a public body's contractors and business partners to an IT service provider offering coordinated e-mail service to several public bodies.

For further information see FOIP Bulletin No. 13: *Business Contact Information*, published by Access and Privacy, Service Alberta.

Disclosure to a relative of a deceased person

Section 40(1)(cc) This provision permits a public body to disclose personal information to the surviving spouse, adult interdependent partner or relative of a deceased individual if, in the opinion of the head of the public body, disclosure would not be an unreasonable invasion of the deceased individual's personal privacy.

Spouse refers to a husband or wife of the deceased.

Adult interdependent partner means a person who

- lived with the deceased in a relationship of interdependence
  - for a continuous period of not less than three years, or
  - of some permanence, if there is a child of the relationship by birth or adoption,

or

- entered into an adult interdependent partner agreement with the other person under section 7 of the *Adult Interdependent Relationships Act* (section 3 of that Act).

Relationship of interdependence means a relationship outside marriage in which any two persons share one another's lives, are emotionally committed to one another, and function as an economic and domestic unit (section 1(f) of the *Adult Interdependent Relationships Act*). In determining whether two persons function as an economic and domestic unit, a public body must take all the circumstances of the relationship into account. A list is included in section 1(2) of the *Adult Interdependent Relationships Act*.

A *relative* in this context refers to a person connected by blood or marriage such as a mother, father, son, daughter, brother, sister of the deceased and may also include in-laws. Public bodies should consider any relevant guidelines about the interpretation of the term *relative* that may exist in applicable legislation.

Section 40(1)(cc) allows the head of a public body discretion to disclose personal information about a deceased individual, taking into consideration both the test for unreasonable invasion of personal privacy (**section 17**) and the relationship between the deceased and the individual to whom the information may be disclosed, including, for example, the relationship of the individual to the deceased at the time of death.

Privacy for a deceased individual normally continues for a period of 25 years (see **section 17(2)(i)**). **Section 40(1)(cc)** permits a public body to disclose information to a relative prior to the expiry of the 25-year period if the disclosure would not be an unreasonable invasion of the deceased individual's personal privacy, taking into consideration the factors in **section 17(5)** and other relevant circumstances.

Particularly important factors to consider are whether

- the disclosure is desirable for the purpose of subjecting the activities of the Government of Alberta or a public body to public scrutiny;
- the personal information is relevant to a fair determination of the requesting individual's rights;
- the personal information was originally supplied by the requesting individual;
- the personal information was supplied in confidence;
- disclosure may endanger the physical or mental well-being of any other living member of the family;
- there are grounds to believe that another member of the family does not want the information disclosed to the relative;
- the personal information is likely to be inaccurate or unreliable;
- the information contains medical, psychological or social work case reports or data which it is reasonable to believe would prove harmful to family relationships; and
- disclosure may harm the reputation of the deceased.

Evidence of the relationship of the person to the deceased individual should be produced before personal information is disclosed. This should consist of reliable documentation of the relationship (e.g. a birth or marriage certificate). As well, if a public body is not certain that the individual is deceased, the person seeking disclosure must provide reliable evidence that the individual is dead (e.g. a death certificate or obituary notice).

For further information about disclosure of personal information about deceased persons, see FOIP Bulletin No. 16: *Personal Information of Deceased Persons*, published by Access and Privacy, Service Alberta.

Disclosure to the legal representative of an inmate

Section 40(1)(dd) This provision permits the disclosure of personal information to a lawyer or student-at-law who is acting for an inmate under the control or supervision of a correctional authority. The disclosure of personal information without the individual's consent may be necessary for the legal representative to properly represent an inmate, for example, in a first appearance hearing.

For information on the meaning of supervision, see the discussion on **section 40(1)(aa)** above.

Disclosure to avert imminent danger to health or safety

Section 40(1)(ee) This provision permits disclosure of personal information if the head of a public body believes, on reasonable grounds, that disclosure will avert or minimize an imminent danger to the health or safety of any person.

Imminent danger means a danger that is likely to arise immediately or very soon.

This provision permits the disclosure of the personal information of *any individual*, not only an individual who endangers health or safety or an individual whose health or safety is endangered. This is one of the few provisions of **section 40(1)** that requires an exercise of discretion by the head of the public body.

The head of a public body will have to consider all the circumstances and all the information in the public body's possession about an individual when making a decision. Past behaviour of the individual is one factor that may assist in decision-making.

Examples of information that might be disclosed under this provision include:

- information about the escape or release of a violent offender to a past victim; and
- information about a student's threat of suicide to residence supervisors on a college campus.

Disclosure for administration of the Motor Vehicle Accident Claims Act

Section 40(1)(ff) This provision permits disclosure of personal information to the Administrator of the *Motor Vehicle Accident Claims Act* or to an agent or lawyer of the Administrator.

Section 40(1)(ff) is intended to allow the Administrator to deal with claims made under that Act. It permits police services and other public bodies, such as Alberta Infrastructure and Alberta Transportation, to disclose any information gathered about an accident to the Administrator once a claim has been lodged.

Disclosure of alumni records for fund-raising purposes

Section 40(2) This provision permits post-secondary educational institutions to disclose information in their alumni records for the purposes of their own fund-raising activities.

Disclosure may be made to any person acting on behalf of the post-secondary institution in raising funds. This includes alumni associations, foundations, private fund-raising organizations, and other persons raising funds on behalf of the institution. In this context, "person" means a legal entity capable of entering into an agreement.

The person to whom the disclosure is made must have a written agreement with the post-secondary institution. The agreement must

- allow individuals a right of access to their own personal information disclosed under the agreement; and
- provide that the person using the information will discontinue using that information if an individual so requests.

The agreement should also contain other clauses to ensure compliance with the privacy protection provisions of the Act.

Section 40(2) is intended for situations where the post-secondary wants to disclose alumni information to a separate, arms-length body. It is not intended for situations where the alumni information is transferred to an office that is *part of* the post-secondary body.

Section 40(2) also does not apply where the body is providing services to the post-secondary institution under a contract or agency relationship. In these situations, the post-secondary would retain control of the information.

This provision complements the provision in **section 39(2)**, as outlined in section 7.6 of this chapter. See also FOIP Bulletin No. 5: *Fund-Raising*, published by Access and Privacy, Service Alberta.

Disclosure of teaching and course evaluations

Section 40(3) This provision permits disclosure of personal information contained in student evaluations of instructors and courses at post-secondary educational institutions.

Disclosure is limited to evaluations completed by students. It does not extend to evaluations of courses by faculty members. The amount of personal information disclosed is limited to that which would assist a student in selecting courses. If the evaluation includes information not relevant to selection of a course (e.g. the

evaluated course is no longer offered or the evaluation is otherwise not current), it cannot be disclosed.

Post-secondary educational bodies should ensure that information about teaching and course evaluations is valid and up-to-date before it is disclosed, and should establish written policies to ensure that the practice is carried out in a responsible manner.

Extent of disclosure

Section 40(4) This provision limits the disclosure of personal information to what is necessary to carry out the purposes described in **section 40(1)**, **(2)** and **(3)**.

For example, a public body communicating the result of an investigation might need to consider whether each party needs all the personal information relevant to the investigation or whether a separate letter or e-mail is required for each party (see *IPC Investigation Report F2004-IR-002*).

The extent of disclosure also arises when there are threads of e-mails. When notifying an employee about an incident, it may not be necessary for the employee to receive the entire chain of e-mails between a complainant and various staff members (see *IPC Order F2005-014*).

7.8 Consistent Purposes

Section 41 states that for the purposes of **sections 39(1)(a)** and **40(1)(c)**, a use or disclosure of personal information is consistent with the purpose for which the information was collected or compiled if the use or disclosure

- has a reasonable and direct connection to that purpose; and
- is necessary for performing the statutory duties of or for operating a legally authorized program of the public body that uses or discloses the information.

Section 41 balances the protection of individuals' privacy against the need of public bodies to use and disclose personal information effectively to carry out program activities and fulfil their legislated mandates.

Section 39(1)(a) allows a public body to *use* personal information for a purpose that is consistent with the purpose for which the information was originally collected.

In most cases the public body using the information will be the public body that collected it. However, if the personal information has been collected for the purposes of delivering a common or integrated program or service, the public body using the information may not be the public body that originally collected it.

See section 7.7 of this chapter for further information on common or integrated programs and services (**section 40(1)(i)**). See also FOIP Bulletin No. 8: *Common or Integrated Programs or Services*, published by Access and Privacy, Service Alberta.

Section 40(1)(c) allows a public body to *disclose* personal information for a purpose that is consistent with the purpose for which the information was originally collected.

In most cases this provision will apply to disclosure outside the public body. The new purpose for using or disclosing must be consistent with the purpose for which the information was collected or compiled.

A use or disclosure has a *reasonable and direct connection* to the original purpose if there is a logical and plausible link to the original purpose. A consistent use should grow out of or be derived from the original use; it should not be an unrelated or secondary use of the information, otherwise known as "function creep."

A use or disclosure is *necessary for performing the statutory duties of, or for operating a program of, the public body* if the public body would be unable to carry out its program without using or disclosing the personal information in the way proposed.

A consistent use or disclosure must meet both of the above conditions to be valid.

Examples of a consistent purpose

Evaluation of a program

Public bodies will have a regular need to evaluate the operation and success of their programs. This is particularly true of new programs or those that have changed in some way. **Section 41** allows a public body to select clients or participants who can participate in that evaluation through questionnaires or interviews.

Verification of ownership

Local government bodies issue permits for such things as development of a property, demolition and burning. These permits are issued to the owner of a property. **Section 41** allows the staff who approve the permit to verify ownership from the assessment roll.

Expansion of a program

Public bodies set criteria for participation in programs. If the criteria are broadened, individuals who were originally rejected may become eligible. This provision allows a public body to determine eligibility on the basis of the original submissions from these individuals rather than collecting the information again. It also enables the public body to do cost projections with respect to the expanded eligibility parameters. Although "dummy" data may often be used for such purposes, there may be times when real or live data is needed.

In *IPC Order 2001-038*, the Commissioner found that a school board's disclosure of a child's personal information for the purpose of setting up and administering an e-mail system was consistent with the original purpose for collection – namely, to register the child in school. However, disclosure of that information for advertising, marketing and revenue generation were not consistent purposes.

Public bodies are required to maintain a record of all uses of personal information, including all consistent uses and disclosures, in order to be able to provide complete, current and accurate descriptions of the personal information banks in their custody or under their control for the use by the public (section 87.1(2)(d)).

7.9 Disclosure for Research or Statistical Purposes

Section 42 of the Act enables a public body to disclose personal information for a research purpose, including statistical research, only if

- the research purpose cannot reasonably be accomplished unless that information is provided in individually identifiable form or the research purpose has been approved by the Information and Privacy Commissioner;
- any record linkage is not harmful to the individuals the information is about and the benefits to be derived from the record linkage are clearly in the public interest;
- the head of the public body has approved conditions relating to the following:
  - security and confidentiality,
  - the removal or destruction of individual identifiers at the earliest reasonable time,
  - the prohibition of any subsequent use or disclosure of the information in individually identifiable form without the express authorization of that public body;

  and
- the person to whom the information is disclosed has signed an agreement to comply with the approved conditions, the *FOIP Act* and any of the public body's policies and procedures relating to the confidentiality of personal information.

Section 42 enables research to take place while at the same time ensuring that privacy is protected. This is accomplished by the strict conditions set out above. Prior to disclosing personal information for research purposes under this provision, a public body must ensure that all four requirements are met.

For a *research purpose* means for the purpose of a systematic investigation or study of materials or sources in order to establish facts or to verify theories.

Statistical research is research based on the collection and analysis of numerical data using, in this case, quantifiable personal information to study trends and draw conclusions.

The *FOIP Act* does not expressly prohibit disclosure of information other than personal information for a research purpose under a confidentiality agreement. Public bodies should seek legal advice as to whether disclosure of, for example, confidential third party business information for a research purpose could expose the body to the risk of legal action on the part of the third party.

Individually identifiable information

Information is in *individually identifiable form* if unique identifiers are attached to the information such that the information can identify a particular individual. The identifiers might be an individual's name, address, telephone number, date of birth or social insurance number. Small population cells or contextual information may also allow for the identification of an individual.

Section 42(a) makes provision for situations where

- the research purpose cannot reasonably be accomplished unless the information is provided in individually identifiable form; or
- the research purpose has been approved by the Commissioner.

The first part of this provision allows public bodies to disclose personal information for research in circumstances where the research cannot be completed without access to the information in individually identifiable form. The onus is on the public body to understand research methods generally and the proposed project specifically, to determine whether identifiable information is truly needed to accomplish the research. The second part of the provision allows public bodies to disclose personal information for research if the Commissioner has approved the research purpose. Approval by the Commissioner ensures that the research purpose is subjected to impartial scrutiny.

The researcher would submit the research proposal to either the public body or the Commissioner in writing, clearly explaining the nature of the research, the information involved and the reason for the request. A detailed proposal enables the public body or the Commissioner to evaluate the necessity for identifiable information, any potential harm to individuals, the academic credentials, skill and reputation of the researcher, and proposed security for the records containing the information.

Record linkage

Section 42(b)

Section 42(b) places controls on any record linkage performed during a research project.

Record linkage is a form of data matching involving the systematic comparison of sets of information, often personal, to establish relationships among data. Within the research context, it often involves the creation of a new database allowing the statistical correlation of research variables. Record linkage can be a useful tool for quantitative analysis in research projects.

Record linkage for research purposes is the matching of sets of personal information to achieve the objectives of the research project, generally with no intention of making decisions about the research subjects' rights or privileges. The matching is a means of linking the right information to the right people in a representative sample used in a study. This makes it distinct from the kind of record linkage for individual profiling that is used in some marketing strategies, for example.

Record linkages permitted under section 42 are only for research purposes and no decision that directly affects an individual may be made as a result of such linkage.

The provision requires that a linkage *not be harmful*. This means that a linkage must not have an adverse affect on the individuals under study – that is, the information disclosed must not result in damage to an individual's reputation, or denial of a job, benefit or service.

Linkages also need to be considered in terms of the *benefits derived* from them. The benefits of the research and linkage must outweigh the privacy concerns regarding the disclosure of personal information to the researcher. The research and linkage must be clearly in the public interest. That is, the benefits must apply to a wide public and not to just one or two individuals. The written research proposal should outline why this research, using this information, is needed at this time.

Approval of conditions

Section 42(c) **Section 42(c)** provides that a disclosure for research purposes may take place only if the public body is aware of and has approved the researcher's proposed practices for handling personal information.

Security refers to protecting or guarding the personal information used in a research project from unauthorized access or disclosure, theft or other danger. Good security may require such measures as locked filing cabinets, computer controls and access codes, restricted work areas, and encryption or encoding of data, depending on the sensitivity of the data involved and the threat and risk associated with it.

Confidentiality refers to the condition whereby personal information is kept private and safe from unauthorized access, use or disclosure. It means that there is no disclosure, orally or otherwise, other than to those working on the project. For sensitive personal information, disclosure should be on a "need-to-know" basis. Not everyone on the project team would have a need to know all of the information. Data should be accessed and manipulated in a contained setting before being broadly available to the team.

Removal or destruction of individual identifiers means the deletion of identifying information, such as name, address, social insurance number or other numerical identifier, or the destruction of the identifiers in whatever way is appropriate to the medium on which the information is stored. This must be done in such a way as to render the information anonymous, for example, by assigning a randomly generated research project identifier in place of the actual individual identifier.

Removal of identifiers is to take place at *the earliest reasonable time*. This will vary with the circumstances of each project and the comparisons the researcher is making between different sets of data. However, the researcher and the public body should agree on a specific date by which time a researcher must strip off all identifiers. This would be when all the different sets of information have been combined and are ready for analysis.

Prohibition on any subsequent use or disclosure means a prohibition on any further use or disclosure of the personal information by the researcher for any purpose, including any other research or statistical purpose. The personal information can be used only for the project for which the information was originally disclosed, unless the public body explicitly authorizes another research use. This prohibition includes a ban on the use of the information to sell products or services to the subjects of the study and a ban on the sale or gift of the information to a charity in order to help solicit donations.

Agreement to comply with approved conditions

Section 42(d)

Section 42(d) provides that the researcher must sign a detailed research agreement. This agreement must include all the provisions set out in **section 9** of the FOIP Regulation, namely:

- personal information disclosed can be used only for a research purpose set out in the agreement or for which written authorization has been given by the public body;
- the names of those persons who will be given access to the personal information must be provided;
- the researcher must bind these persons, through an agreement, to adhere to the same conditions as the researcher;
- information must be kept in a secure location;
- how and when the identifiers will be removed or destroyed must be specified;
- contact with the individuals to whom the information relates is prohibited without prior written authorization from the public body;
- no use or disclosure can be made of the information in a form that identifies individuals without prior written authorization from the public body;
- information cannot be used for an administrative purpose directly affecting an individual;
- notification of the public body is required if any conditions of the agreement are breached; and
- failure to meet the conditions may result in cancellation of the agreement and leave the researcher open to charges under **section 92(1)** of the Act.

The public body may want to add audit provisions to the agreement so that the security and confidentiality measures of the researcher can be reviewed.

The model **Proposal for Access to Personal Information for Research and Statistical Purposes Form** and the related **Agreement** in Appendix 5 are suitable for an individual or group of researchers that is not part of any public body. If another public body proposes research, a personal information sharing agreement would likely be more appropriate (see section 9.7 of Chapter 9).

7.10 Disclosure of Information in Archives

Part 3 of the *FOIP Act* (**section 43**) provides for the disclosure of information without a FOIP request by the Provincial Archives of Alberta or the archives of a public body.

This section is intended to support research and related activities by allowing access to archival holdings, subject to a limited number of restrictions. **Section 43** is *enabling*. It permits the archives to disclose information under specified conditions; it does not require the archives to disclose information.

The section does not affect access to records that were unrestricted before the *FOIP Act* came into force (**section 3(b)**).

Section 43 does not apply to records deposited in the Provincial Archives of Alberta or the archives of a public body by or for a person or entity other than a public body (**section 4(1)(j)**). These are generally referred to as *private records*. For example, if an individual has made a gift of records to the Provincial Archives, subject to an agreement with respect to access, the *FOIP Act* does not prevent the Provincial Archives from complying with the terms of that agreement.

Section 43(1) applies to all public body archives.

The Provincial Archives of Alberta or the archives of a public body

The role of the Provincial Archives of Alberta and other public body archives is to select, preserve and make available the non-current records of public bodies that have been preserved because of their enduring value. This includes legal, evidential, financial, and historical value.

The *archives of a public body* means an agency, other than the Provincial Archives of Alberta, that is authorized to perform archival functions on behalf of that public body.

The archives of a public body may be

- a public body's own archives, in which case the records will remain in the custody or under the control of that public body (e.g. the archives of most post-secondary institutions);
- the archives of another public body, to which records may be transferred under **section 3(e)**, in which case the records will normally be in the custody and under the control of the archives; or
- an archival facility that operates under a contract or agency relationship with the public body, in which case custody may be transferred but control must be retained.

The Provincial Archives of Alberta and the archives of public bodies may disclose information, including personal information, in their records, subject to certain conditions set out in **section 43(1)(a)** and **(b)**.

Disclosure of personal information

Section 43(1)(a)

This provision supplements **section 40(1)**, which also allows for the disclosure of personal information without a FOIP request. Disclosure under this provision depends upon the age of the record.

If personal information is in a record that is *less than 25 years old*, the archives cannot disclose it under **section 43(1)(a)**. The archives must either apply a relevant provision in **section 40(1)**, such as disclosure in accordance with an enactment that authorizes or requires the disclosure (**section 40(1)(f)**), or ask the person seeking the information to submit a FOIP request.

If the personal information requested is in a record that has been in existence for *25 years or more*, the archives may disclose the information under **section 43(1)(a)** if the disclosure

- would not be an unreasonable invasion of privacy under **section 17**; or
- is in accordance with **section 42** (which specifies conditions for disclosure of personal information for a research purpose).

Section 4.3 of Chapter 4 sets out guidelines for applying **section 17**.

If the personal information is about an individual who has been dead for 25 years or more, and satisfactory proof of that fact is provided, disclosure would not be an unreasonable invasion of privacy under **section 17(2)(i)** and the personal information may be disclosed under either **section 43(1)(a)(i)(A)** or **section 40(1)(b)**.

If the person requesting disclosure cannot prove that the individual has been dead for at least 25 years, and it is determined, after application of the other provisions of **section 17**, that the disclosure would be an unreasonable invasion of a third party's privacy, the archives can disclose the information only in accordance with **section 42**, which requires a research agreement.

Information about research agreements and the application of **section 42** is provided in section 7.9 of this chapter. If disclosure is made under **section 42**, the archives must have a written agreement in accordance with **section 9** of the FOIP Regulation.

If the personal information is in a record that has been in existence for *75 years or more*, the archives may disclose that information without restriction under the *FOIP Act.*

Disclosure under **section 43(1)(a)** may be subject to the restrictions of legislation that is paramount over the *FOIP Act*. The effects of other Acts is discussed at the end of this chapter.

Disclosure of information other than personal information

Section 43(1)(b) This provision allows archives to disclose information, other than personal information, in a record that is 25 or more years old. **Section 43(1)(b)** supplements **section 88**, which allows the heads of public bodies to specify certain categories of information that may be made available to the public without a FOIP request.

Section 43(1)(b) is intended to establish greater transparency for archives, which tend to hold large volumes of records collected by public bodies. This transparency benefits not only public bodies that transfer the custody and control of their records to archives, but also the researchers who use the collections.

Section 43(1)(b) requires the Provincial Archives or the archives of a public body to assess the information that is being considered for disclosure and determine whether disclosure could still result in harm or whether disclosure may be prohibited for some other reason.

Information may be disclosed under this provision if

- disclosure would not harm the business interests of a third party within the meaning of **section 16**;
- disclosure would not harm a law enforcement matter within the meaning of **section 20**; and
- the information is not subject to any type of legal privilege under **section 27**.

Details on the application of **section 16** are provided in section 4.2 of Chapter 4. If the information is in a record that has been in existence for 50 years or more, then **section 16** does not apply.

Details on the application of **section 20** are provided in section 4.6 of Chapter 4.

Details on the application of **section 27** are provided in section 4.13 of Chapter 4.

As a best practice, when public bodies transfer records to archives, they should identify any records that may be subject to restrictions imposed by other Acts. They should also identify any records to which the exceptions in the *FOIP Act* for disclosure harmful to the business interests of a third party or harmful to law enforcement may apply, as well as any records that may be subject to legal privilege (where known).

Accepted archival practice involves the accessioning of records according to organizational principles and standards that assist researchers in using the records. Archives may find it helpful to have policies in place that explain the relationship between their procedures and practices and the provisions of the *FOIP Act*. For example, if it is decided to apply **section 43(1)** to open a particular collection in the archives, the policy may set out the criteria that are used to determine that information in the record series meets the test of being 25 or more years old.

Effect of other Acts

Archives may disclose information in records as described above provided the information is not subject to a confidentiality provision of another Act or regulation of Alberta that is paramount over the *FOIP Act* or an enactment of Canada that is paramount over the *FOIP Act* (by virtue of federal paramountcy).

Section 5 of the *FOIP Act* provides rules for applying the Act when the relationship between the *FOIP Act* and another enactment does not allow both to operate in their entirety at the same time. If another Act or a regulation under the *FOIP Act* expressly states that a provision of another enactment prevails despite the *FOIP Act*, the *FOIP Act* does not apply. The other enactment applies, on its own terms.

If a provision of the *FOIP Act* is inconsistent or in conflict with a provision of another enactment, and neither the other Act nor the FOIP Regulation says that the other provision prevails despite the *FOIP Act* the *FOIP Act* prevails to the extent of the inconsistency.

This provision is particularly significant for archives because much of the legislation prohibiting disclosure of information that is paramount over the *FOIP Act* does not set time limits on the prohibition. For example, there are no time limits on the prohibitions on disclosure in the paramount sections of the *Child, Youth and Family Enhancement Act* or the *Maintenance Enforcement Act*.

Public bodies transferring records to archives should identify any records that are subject to any restriction or prohibition on disclosure under legislation that is paramount over the *FOIP Act* and any time limits that apply.

For further information on the effect of paramountcy, see FOIP Bulletin No. 11: *Paramountcy*, published by Access and Privacy, Service Alberta.

7.11 Record of Purposes

Public bodies should ensure that all uses and disclosures of personal information that are routine in nature and occur frequently are described in generic terms in the description for the appropriate personal information bank in the directory of personal information banks. This fulfils the requirement set out in **section 87.1(2)(d)** to notify the public about such uses and disclosures. Public bodies must ensure that the directory is kept as current as is practicable, and that access to the directory is available to the public at an office of the public body, or on the public body's website (**section 87.1(4)**).

Section 87.1(3) Under this provision, if personal information is used or disclosed by a public body for a purpose that is not included in the directory of personal information banks, the head must

- keep a record of the purpose and either attach or link that record to the personal information; and
- ensure that the purpose is included in the next publication of the directory.

There are a number of ways to meet the requirement to attach or link a record of purpose to the personal information. For paper files, when the request is for information about one or more individuals, a copy of the official request for use or disclosure of the personal information, together with the signature of the official or employee agreeing to such use or disclosure, can be attached to individual files. When the request is for a large number of files, a control file can be created, containing the same information.

If an individual whose information is contained in the file series requests his or her personal information, the part of the control file containing information about the individual must be considered for disclosure along with the other personal information.

If the use or disclosure involves computer files, a tag or other indicator should be inserted in the system linking the user to information regarding the request for and decision to allow the use or disclosure. The requirement to consider the disclosure of information in a control file applies in this case as well.

For further information on directories of personal information banks, see section 2.7 of Chapter 2 and the *Guide to Identifying Personal Information Banks*, published by Access and Privacy, Service Alberta.