



Human Resources Guide for Local Public Bodies

Revised January 2007
(updated to reflect A.R. 186/2008)

ISBN 978-0-7785-6102-6

Produced by:

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

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

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

Web sites:
foip.alberta.ca
pipa.alberta.ca

INTRODUCTION

This guide was developed to assist human resources staff in local public bodies to identify information that can be routinely released upon request. It also outlines considerations when disclosing information under **section 40** of the *Freedom of Information and Protection of Privacy Act*, and when responding to a formal request. Staff working for health care bodies should be aware that health information about employees of these public bodies may fall within the scope of the *Health Information Act*. Some information is provided at the end of this guide but you should consult with your FOIP/HIA contact for additional guidance.

Working within the human resources field, you will be accustomed to receiving requests for information about employees. You will also be familiar with the need to keep information and records secure and confidential. Your response to requests for personal information is always made with care and discretion.

The *Freedom of Information and Protection of Privacy Act* (referred to as the FOIP Act) provides a standard set of rules and procedures to follow when dealing with personal information. This guide will help you develop appropriate policies and practices for collecting, disclosing and protecting personal information.

You will not find binding rules or policy in these pages. These are contained in the FOIP Act itself and in the orders of the Alberta Information and Privacy Commissioner (IPC). The guide is not intended to be a complete explanation of the FOIP Act; rather it will provide some examples of the issues to be considered and guidance on how to treat the various kinds of records in your files.

The first part of the guide deals with the definitions you will need to understand, the types of requests you may receive, some suggestions regarding how the FOIP Act affects records management procedures, with particular reference to employee files, and what constitutes an unreasonable invasion of privacy.

The second part of the guide takes a look at each series of records found in a typical human resources department and discusses their protection and disclosure in light of the FOIP Act. Major personnel functions are listed in the table of contents. Each section contains:

- a description of the records normally held in human resources departments of public bodies;
- a description of records which may be routinely disclosed;
- consideration of exceptions that may apply to records when a FOIP request is received; and
- tips for dealing with requests and records.

Throughout the guide, reference is made to orders made by Information and Privacy Commissioners in British Columbia and Ontario. It is important to remember that the legislation in those provinces differs from Alberta. These references are illustrative only—they have no force or binding applicability in Alberta. If you are dealing with a request that requires consideration of one of the factors to which these orders refer, you may find it useful to read the order and the arguments for and against disclosure when making your decision.

One of the key principles of the FOIP Act is that individuals have a right to access information about themselves. In the vast majority of cases, you will make an employee's personal information available to the employee without requiring a FOIP request.

Remember that the FOIP Act is intended to supplement, not to replace existing business practices. Wherever possible, routine disclosure is preferable to having someone make a FOIP request for their own personal information. When a request is made, or when you are considering disclosure under **section 40**, it is unlikely that a complete record will be withheld. More usual is a line-by-line examination of the record in conjunction with your FOIP coordinator, and severing of the information, which cannot be disclosed.

You are encouraged to make use of other FOIP resources. These include the FOIP Act itself, the Government of Alberta *FOIP Guidelines and Practices, 2005* publication; *Managing Contracts under the FOIP Act, A Guide for Government of Alberta Contract Managers and FOIP Coordinators*; the government's web pages at foip.alberta.ca and your organization's own FOIP policies and procedures. This guide is intended to be used in conjunction with them; it does not replace or repeat the information contained in them.

Remember, too, the people available to help you, especially your FOIP coordinator, the staff of Access and Privacy, Service Alberta, and the staff of the Alberta Government department that supports your sector, such as Alberta Education, Alberta Health and Wellness, Alberta Seniors and Community Supports, and Alberta Solicitor General and Public Security.

This guide may be updated as human resources practices are further defined and as Commissioner's Orders are issued.

Freedom of Information and Protection of Privacy

Human Resources Guide for Local Public Bodies

Table of Contents

Chapter 1: General Information	1
1.1 Definitions.....	1
1.2 FOIP and Records Practices	1
1.3 Types of Requests.....	3
1.4 Unreasonable Invasion of Privacy	4
Chapter 2: Human Resource Records	7
2.1 Human Resource Planning.....	7
2.2 Classification	8
2.3 Pay and Benefits	9
2.4 Staffing	16
• Information about the job and the staffing process.....	17
• Application process	18
• Screening and interview process	19
• Reference and other checks	20
• Provision of reference information	22
• Offers of employment.....	23
• Abolishment and redeployment.....	23
• Resignation and termination	24
• Exchange of information between public bodies	24
2.5 Training and Development	24
2.6 Employee Relations.....	26
2.7 Workplace Health and Safety	30
2.8 Workplace Harassment	31
2.9 Violation of Law Information	33
2.10 Volunteers	33
2.11 Corporate Employee Records	34
• Performance appraisals and evaluations	36
• 360 degree appraisals.....	36
• Medical information	36
2.12 Health Information Act and Employee Records.....	37

Chapter 1

General Information

1.1 DEFINITIONS

FOIP is used throughout the guide as the acronym for “Freedom of Information and Protection of Privacy”.

The FOIP Act is Alberta’s *Freedom of Information and Protection of Privacy Act*.

The Commissioner is the Information and Privacy Commissioner for Alberta.

Employee is defined in **section 1(e)** of the FOIP Act as including a person who performs a service for the public body as an appointee, volunteer or student or under a contract or agency relationship with the public body.

FOIP request is an official request made under the FOIP Act and accompanied by the initial fee if required.

Local public body is defined in **section 1(j)** of the FOIP Act as an educational body, a health care body, or a local government body.

These include universities, the Banff Centre, technical institutes, public colleges, school boards, regional school authorities, charter schools, regional health authorities, provincial health boards, community health councils, subsidiary health corporations, hospitals, nursing homes,

municipalities, improvement districts, special areas, regional services commissions, drainage district boards, irrigation district boards, housing authorities, foundations and management bodies under the *Housing Act*, Metis settlements and the Metis Settlement General Council, police services, police commissions, committees and others.

Personal information is defined in **section 1(n)** of the FOIP Act as recorded information about an identifiable individual. This includes names, home and business telephone numbers and addresses, age, sex, marital status, family status, race, national or ethnic origin, color, religious or political beliefs, fingerprints, other biometric information, blood type, genetic information or inheritable characteristics, any identifying number or symbol, information about health and health care history, educational, financial, employment or criminal history, the individual’s own views or opinions and anyone else’s views or opinions about the individual.

Record is defined in **section 1(q)** of the FOIP Act, and means a record of information in any form and includes notes, images, audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software of any mechanism that produces records.

1.2 FOIP AND RECORDS PRACTICES

The FOIP Act contains a number of rules and procedures that will affect how you

create, organize and manage your records. Generally, individuals can access information about themselves, but not the personal information of others. Records in your public body should be:

- created to make analysis and presentation of information as easy and straightforward as possible;
- created so that information that is routinely available can be viewed or copied without supervision or restriction; and
- organized to make retrieval straightforward, bearing in mind the 30-day time limit for responding to requests imposed in the FOIP Act.

Remember that under the FOIP Act there is no such thing as an “unofficial” file. Supervisors often retain employee information in files within their office or work area. An employee may know of the existence of such records, while staff in Human Resources may not. If all records are not considered when responding to a request, there could be a complaint that you have not conducted an adequate search for records related to the employee.

Discourage creation of duplicate employee files, particularly containing original records, whenever possible.

FOIP’s Impact on Record-Keeping

- The personal information that you collect must relate directly to and be necessary for an operating program or activity of your public body (**section 33(c)**).
- When you are collecting personal information directly from an individual, you must inform the individual of the purpose of

collection; the legal authority for the collection; and the title, business address and telephone number of someone who can answer questions about the collection (**section 34(2)**).

- Any personal information that is used to make a decision about an individual must be retained for at least one year after use so that the individual has a reasonable opportunity to obtain access to it (**section 35(b)**). This includes references obtained on any candidates, resumés of unsuccessful candidates and any other information acquired during the hiring process or used in making other decisions about employees.
- If personal information is corrected or annotated, or linked to a request for correction that was not made, you must notify any other public body or third party with which you have shared this information in the prior year (**section 36(4)**).
- You must make reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure and destruction of records (**section 38**).
- Personal information must be disposed of in a secure manner to prevent accidental disclosure. This normally means secure shredding of paper records or, in the case of electronic records, taking steps to ensure the information cannot be recovered.
- The FOIP Act recognizes information in electronic format as a record. Therefore, you need to be sure those human resource systems such as Banner or People Soft have built-in safeguards to prevent unauthorized use, access, disclosure or disposal. These systems need to have clearly

defined hierarchies of users; to place limitations on access to sensitive and personal information, so that it is available only to the individual it is about and human resource professionals who need access; and to have data compartmentalized so that human resource information is not widely accessible.

One of the most important sets of records is the corporate employee file. In section 2.11, you will find a detailed review of some of the records on this file and some suggestions for managing them to make viewing and severing easier.

1.3 TYPES OF REQUESTS

FOIP requests for records, other than for an individual's own records, can be handled in two ways.

First, determine whether the enabling provisions of **section 40** may be used to disclose the information. Throughout this guide examples will be given of when and how **section 40** may apply.

If **section 40** does not apply, or you choose not to disclose the personal information, then the applicant must submit a FOIP request. Throughout the guide you will find examples of what to consider in dealing with such FOIP requests.

Requests by Individuals for Information About Themselves

Employees and former employees have a legal right to access any personal information about themselves that is held by your local public body subject

to limited and specific exceptions (**section 2(c)**). *Wherever possible this access should be provided without requiring a FOIP request.*

Employees may choose either to view the record or to receive a copy. Normally there would not be a fee for informal requests. Fees may apply to a formal FOIP request when photocopying costs (at 25¢ per page) exceed \$10 (FOIP Regulation, **section 12**).

When your staff does not personally know the individual, you should take steps to verify his or her identity before disclosing the records. If an individual is viewing records, ensure someone is present to protect the security of the records and, if requested, to explain or clarify the information.

FOIP Tip: *This right of access is not unconditional. If an exception to disclosure in Part 1 of the FOIP Act applies, then the personal information may be withheld subject to the proper exercise of discretion. (IPC Order 97-014).*

Requests for Correction to Personal Information

Employees and former employees have a legal right to request corrections to personal information about themselves held by your local public body (**section 2(d)**). This right usually means the right to correct factually incorrect information.

Section 36(2) states that the head of a public body must not correct an opinion, including a professional or expert opinion, although there may be a requirement to annotate such an opinion (**section 36(3)**).

Rules for dealing with requests for correction are found in **section 36** of the FOIP Act. There is no charge for requests for correction of personal information. The request should be in writing in a letter or on the official form.

Requests for Personal Information Made by a Third Party

A third party is any person or organization other than your local public body and applicant. Normally such requests must be submitted as FOIP requests to your FOIP coordinator. Exceptions to this would apply to:

- requests not considered to be an unreasonable invasion of personal privacy as outlined in **section 17(2)** of the FOIP Act and where routine disclosure under **section 40(1)(b)** has been recommended;
- requests made by officers or employees of your local public body where they have a need to know this information to do their job (**section 40(1)(h)**); and
- cases where disclosure of personal information is authorized under **section 40** of the FOIP Act.

Wherever possible, there should be a policy in place to handle these disclosures. A notation should be placed on the file indicating that a disclosure was made and to whom.

Other Requests for Access to Information

All records of a local public body are accessible on request unless they are specifically excluded from the

application of the Act or an exception to access applies.

Section 4 of the FOIP Act lists those records that are excluded. **Part 1, Division 2** of the FOIP Act outlines the mandatory and discretionary exceptions which may apply to records.

Requests for access to information must either be made on the approved form or in writing stating that the request is being made under the FOIP Act. Before a request can be processed, the initial fee of \$25 must be paid (FOIP Regulation, **section 11**). *Any requests received that fall into this category must be referred immediately to your FOIP coordinator.*

1.4 UNREASONABLE INVASION OF PRIVACY

When dealing with FOIP requests for human resource information, you will have to consider whether disclosure of this information is an unreasonable invasion of a third party's personal privacy. **Section 17** of the FOIP Act requires that you deny access if this is the case.

When making a determination, you must first decide if the information is, in fact, *personal information*. The definition given in the FOIP Act is not all-inclusive. The Commissioner has indicated that the definition is not exhaustive and that it also includes facts and events discussed, observations made and the context of the information if this can identify an individual (*IPC Order 96-019*).

If the personal information is about an employee and is contained in a report completed as a part of that person's job

responsibilities, it is not necessarily an unreasonable invasion of personal privacy to disclose it (e.g. credentials such as P.Eng.).

If you find that the information is personal information, then look at **section 17(4)** to determine if one of the provisions applies. If one does apply, then disclosing the personal information is presumed to be an unreasonable invasion of privacy. This does not mean that disclosure is automatically unreasonable, but will weigh in favor of a decision not to disclose the information should a request be made for a review of your decision (*IPC Orders 96-008 and 96-010*).

You must then consider all the relevant circumstances including those specifically listed in **section 17(5)**. If, after weighing all these considerations, you determine that there may be an unreasonable invasion of privacy, access to the information must be refused.

First, you should look closely at **section 17(2)** to determine what information can be disclosed safely without invading an individual's privacy:

- Personal information may be disclosed with the written consent of the individual for the specific disclosure (**section 17(2)(a)**);
- Disclosure is permitted if there is no other way to protect someone else's health and safety, or where there is an emergency and disclosure is the fastest, most direct way to protect someone else's health and safety (**section 17(2)(b)**);

- Certain employment information about public officials can be disclosed (**section 17(2)(e)**);
- The total amount paid under a contract, the names of the parties, the subject of the contract and certain terms and conditions that would be considered "standard" or "boilerplate" may be disclosed. This includes any contracts for goods and services, and may include employment services' contracts (**section 17(2)(f)**);
- Information about a permit, or similar discretionary benefit such as a teaching certificate or development permit but only the name of the recipient and nature of the permit or certificate may be disclosed (**section 17(2)(g)**);
- Discretionary benefits of a financial nature can be disclosed, but not background information supplied in order to enable the decision to be made (**section 17(2)(h)**);
- If the individual has been dead for 25 years or more, release of his or her personal information is not considered to be unreasonable. The applicant must supply evidence to prove the length of time the individual has been dead (**section 17(2)(i)**); and
- Attendance at or participation in a public event or receipt of an honour or award of your local public body may be disclosed (**section 17(2)(j)**). The disclosure must not be contrary to the public interest, must be limited to the personal information in **section 17(2)(j)**, and the individual must not have requested non-disclosure.

Considerations

Protect personal information:

Your obligation to protect personal information overrides any arrangement that may have been made regarding disclosure of information. Thus, any arrangement between you and an applicant concerning how or when information will be disclosed is superseded by the FOIP Act (*IPC Order 97-002*).

Requests for disclosure: Always consider **section 17** first when dealing with access requests for personal information. Because it is a mandatory section, the Commissioner will consider it when conducting a review of your decision, and will order severing if he considers it necessary to protect privacy.

Prior knowledge of the requested information: Whether the applicant has already seen the record or knows the information it contains does not matter. **Section 17** still applies to protect the personal information of a third party. (*IPC Order 96-009*).

If the applicant originally provided the information, disclosure of that information to the applicant may not constitute an unreasonable invasion of personal privacy (**section 17(5)(i)**).

Prior release of information:

Having released a third party's personal information previously does require that it is re-released later (*IPC Order 97-011*).

Accuracy of the information: If the record contains information about a third party that is likely to inaccurate or

unreliable, this would weigh against disclosing the record, as it would be an unreasonable invasion of the third party's personal privacy. (*IPC Order 97-002*).

Harm to a person's reputation: In considering the question of harm to a person's reputation, the consideration is not whether such harm is present or foreseeable, but only if it is or would be "unfair" to the individual involved (*IPC Order 97-002*).

Section 30 of the FOIP Act requires that you give written notice to a person if you are considering giving access to personal information described in **section 17**. Although there is no legal obligation to provide such notice when access is being refused, you may wish to give notice anyway. This allows individuals to consent to the disclosure of information that a local public body considers would be refused, or to provide additional information as to why the record should not be disclosed. This additional information will be useful in the review if the applicant makes a complaint.

This notice informs individuals that you have had a request for their personal information in case the Commissioner's Office advises the individual of the complaint.

Although you may provide a less formal notification, such as a telephone call, written notice is a better practice. Informal notification might take place when you are very certain of your grounds for refusing access and do not need representations from a third party to support this decision. This informal notification has no standing under the FOIP Act.

Chapter 2

Human Resource Records

This section of the guide describes records commonly found in human resource departments. It provides guidance on which records can normally be disclosed routinely, which require a FOIP request, and the considerations when handling such a request. It also suggests areas where written policies and procedures should be reviewed from a FOIP perspective in order to ensure compliance with the FOIP Act.

2.1 HUMAN RESOURCE PLANNING

Planning documents fall into three categories:

- plans which have not been implemented;
- plans which have been implemented or which form the basis of instructions to employees; and
- planning reports and monitoring records.

Routine Disclosure

The Act allows public bodies to refuse to disclose certain planning records (**section 24(1)(c)**). However, unless other exceptions apply you cannot refuse to disclose:

- plans which are 15 years old or older (**section 24(2)(a)**);

- statistical surveys (**section 24(2)(d)**);
- information that is the result of background research of a scientific or technical nature undertaken in connection with the formulation of a policy proposal, that is complete or on which no progress has been made for at least 3 years (**section 24(2)(e)**); and
- proposals for service delivery changes that affect employees once they form the basis of instructions or guidelines issued to employees or officers of your local public body (**section 24(2)(f)**).

FOIP Tip: *Implementation of a plan is generally deemed to have taken place when it is communicated in an authorized way to those expected to carry it out. Options considered before deciding upon the plan should not be routinely disclosed.*

Considerations

Section 24(1)(d): This should be considered if the plan has not yet been implemented.

Section 24(1)(g): This should be considered if the records could disclose a pending policy or budgetary decision.

Section 17(4)(d): This should be considered in order to sever personal information in monitoring reports or implementation reports.

Succession planning: Consider whether information in succession planning listings or charts should be disclosed to individuals if the plan is used as a basis of decision-making affecting those persons. This would favour disclosure to the affected individuals.

FOIP Tip: *The Commissioner has provided three criteria to be met when considering whether a record contains “advice” (IPC Orders 96-006 and 2001-002.) Although this applies specifically to **section 24(1)(a)** of the FOIP Act, the same considerations may be applied to plans. The planning documents should be sought or expected, or be part of the responsibility of a person by virtue of that person’s position, the plan should be directed toward taking an action, and the plan should be provided to someone who can take or implement the action.*

2.2 CLASSIFICATION

These records fall into the following categories:

- specifications, manuals and guidelines;
- position descriptions;
- organization charts;
- classification audits, assessments and decisions, including series reviews;
- appeals;
- training and instructional materials for classification and job description writing; and
- employee position numbers.

Section 17(2)(e) of the FOIP Act states that it is not an unreasonable invasion of personal privacy to disclose information about a person’s classification, salary range, discretionary benefits or employment responsibilities as an officer, employee or member of a public body. This includes job titles or positions even if these are unique within the public body (*IPC Order 2001-020*).

Routine Disclosure

- Specifications, manuals and guidelines should be available in your reading room (**sections 24(2)(f)** and **89**).
- Position descriptions can be released when the names of employees and any other personal information has been severed. Generic and benchmark position descriptions can be disclosed.
- Organizational charts should be available with employee name, job title and business telephone number.
- Audit reports and decisions can be released, providing incumbent-specific data such as information about promotions, demotions and salaries is removed.
- Classification series reviews can be disclosed after 15 years or after a decision has been implemented, whichever is sooner (**section 24(2)(a)**).
- Training materials can be disclosed.

Considerations

Section 17(4)(d): This should be considered to ensure that release of position descriptions does not reveal employee job history.

Section 24(1)(c): This should be considered to ensure that release of information on class series reviews does not prejudice negotiations with bargaining agents.

Position numbers: These should not be released when connected to an individual’s name, as the numbers may give access to pay and benefits information on reports.

Organizational charts: These should not contain salary, work schedules, appointment history or security status.

Classification appeal documents: Employees should be cautioned that any personal information contained in classification appeal documents might be disclosed through the exchange of briefs before and during a hearing process.

Endangerment factor: If asked for a complete list of employees, consider whether there may be an endangerment factor in releasing this information (**section 18(1)**). Information and Privacy Commissioners in both British Columbia and Ontario have upheld decisions by police forces not to release complete lists of officers because this could reasonably be expected to threaten the health and safety of an individual. They have, however, agreed that it is proper to confirm the employment status of individual officers on request.

In British Columbia, lists of employees and health professionals involved in dealings with abortions were not disclosed (*B.C. Order 199-97*).

FOIP Tip: *Even when releasing records routinely, check each page to be sure that no employee-specific personal information is released.*

2.3 PAY AND BENEFITS

These records fall into the following categories:

- information about the employee – home address, sex, age, identifying numbers, marital status, dependents, birth or marriage certificates, native treaty status or band number;
- information about the employee’s service – appointment type, employee types, commencement date, termination date;
- information about salary or wages – salary range, gross and net earnings, income tax information, source deductions, pension and retirement savings plan contributions, salary history, bank account number, union dues, bankruptcy or garnishee information, severance or separation allowances and agreements;
- information about benefits – vacation leave, sick leave, maternity leave, group plan premiums and options, group plan utilization, dependent coverage;
- medical information – general or extended illness reports, long term disability information, workers’ compensation information, medical assessments and reviews; and
- information about working hours – actual hours worked, schedules or duty rosters, attendance sheets and reports.

Disclosure of almost all of this information is presumed to be an unreasonable invasion of personal privacy under **section 17(4)**.

However, the Government of Alberta discloses salary information about some senior officials as part of its

accountability to Albertans, and this is allowed under **section 40(1)(e)** of the FOIP Act. **Section 17(2)(e)** allows for the disclosure of information about an employee's salary range and discretionary benefits, and **section 17(2)(h)** allows for disclosure of a discretionary benefit of a financial nature granted by a public body.

Routine Disclosure

- Salary ranges of employees. Since a salary grid could reveal actual salary, it is recommended that only a range be released.
- Working hours for a position, not an individual employee.
- Severance or separation allowance formulas.
- General information about the benefits offered to employees, but not specific details of any coverage unique to an individual or use of a benefit.
- Details of any discretionary benefit such as a bonus, incentive award or negotiated severance amount, provided such disclosure does not reveal the employee's actual salary or allow that to be calculated.

Disclosure Under Section 40 of the Act

Section 40 provides for a range of circumstances where it is permissible for a public body to disclose personal information without consent. These disclosures should be subject to a policy which would include the need to put a notation about the disclosure on the individual's file. Accuracy is important in this process because of the requirement in **section 36(4)** to notify persons to whom personal information

has been disclosed about corrections of the personal information.

All current disclosures of pay and benefit information should be examined against **section 40** to ensure compliance, and, whenever feasible, a statement indicating which specific provision applies should accompany disclosures of personal information.

Section 40(1)(b): Allows for disclosure if it would not be an unreasonable invasion of a third party's personal privacy under **section 17**. **Section 17(2)** indicates when a disclosure would not be an unreasonable invasion of privacy; **section 17(4)** indicates when a disclosure is presumed to be an unreasonable invasion of privacy; and **section 17(5)** sets out the relevant circumstances that must be considered in making a determination of unreasonable invasion of privacy.

Is disclosure necessary because there are compelling circumstances affecting anyone's health or safety (section 17(2)(b))?

If there are compelling reasons which would affect anyone's health or safety, personal information may be disclosed, providing written notice of the disclosure is given to the individual. Consult with your FOIP Coordinator if you believe you are faced with such a situation.

Section 17(2)(b) is intended to capture only immediate circumstances affecting health or safety. The words *there are compelling circumstances* have been interpreted to mean circumstances existing at the present time. For the purposes of this section, it is not sufficient for an applicant to show that the personal information reveals past

circumstances that affected someone's health and safety. Nor is it sufficient for the applicant to show that the information reveals a possible future threat.

In order to establish the relevance of this section, the applicant must show *present* compelling circumstances affecting anyone's health and safety (*IPC Order 97-002*).

Section 40(1)(e): Allows for disclosure to comply with an enactment of Alberta or Canada, or any treaty, arrangement or agreement made under such an enactment.

Examples of such disclosure would include release of information about union dues or other information required under a collective agreement to a bargaining agent, or information required for a job exchange program with another province or the federal government.

Section 40(1)(f): Allows for disclosure for any purpose in accordance with an enactment of Alberta or Canada that authorizes or requires the disclosure.

Examples would include disclosure under the *Income Tax Act*, *Public Health Act*, *Human Rights and Citizenship Act*, *Child Welfare Act*, *Workers' Compensation Act* and the *Employment Insurance Act*.

FOIP Tip: *Ask the person requesting the information to provide the specific statutory authority that requires or authorizes such disclosure, to state the specific information required, and obtain the request in writing or make a notation of the request on the file.*

Section 40(1)(h): Allows for disclosure to an officer or employee of the public body, or to a member of Executive Council, if the information is necessary for the performance of duties of the officer, employee or member. Note that a member of a council or governing body of a municipality may not meet the definition of "employee" or "officer".

Disclosure under this section must be based on more than a mere interest or concern on the part of the person seeking disclosure. Each case will need to be examined to determine whether there is a *need to know* the information.

Supervisors or those higher in the direct chain of command often have valid reasons to access employee information. A person responsible for investigating a potential criminal offence or harassment allegation may also have a valid reason.

Records usually available include employee number, information about the employee's service, salary, vacation leave and sick leave statistics and attendance information.

FOIP Tip: *It is useful to have a policy governing this access to records (see chapter 1.2 of this guide). Remember that discretion cannot be delegated to a secretary or administrative assistant but must be exercised by the responsible employee directly. A council or governing body of a municipality may not meet the definition of employee or officer.*

Benefit Plan administrators have access to detailed information on benefits to do their job. However, Ontario's Information and Privacy Commissioner has ruled that administrative convenience or minor cost savings in administering a benefit plan did not justify disclosure of

personal information to staff administering the plan. If your local public body provides administrative services on behalf of an insurer, you should examine the process closely.

Section 40(1)(i): Allows for disclosure to an officer or employee of a public body or to a member of Executive Council, if the disclosure is necessary for the delivery of a common or integrated program or service, as well as to the duties of the employee, officer or member.

A common program or service means a single program or service that is delivered by two or more public bodies. An integrated program or service means one that has several distinct components delivered by separate public bodies but that together comprise the complete program or service. Public bodies may share common clients, but that alone does not determine whether a program or service is a common program. Other attributes may be:

- legislative authority for the bodies to work together;
- common goals expressed in program description or business plan;
- formal agreement or terms of reference between public bodies explaining their roles and how the components fit together;
- joint planning between the public bodies;
- clear delineation of services being jointly delivered from those that are not; and
- collaboration or coordination in delivery.

For a more detailed explanation, see *FOIP Bulletin No. 8 on Common Programs and Services* distributed by Access and Privacy, Service Alberta.

Examples may include work placement or practicum programs, after school care, a library operated jointly by a school and a municipality, or services provided by one municipality to another municipality.

FOIP Tip: *It is useful to have a policy governing access to records for the purpose of delivering the program or service, keeping **section 40(4)** in mind. That subsection limits disclosure to the information necessary to enable the public body to carry out the purposes described in **sections 40(1), (2), and (3)** in a reasonable manner.*

Section 40(1)(l): Allows disclosure for the purpose of determining an individual's suitability or eligibility for a program or benefit.

Disclosure may be allowed in cases where personal information is needed to assess eligibility for long term disability insurance, pension benefits or employment insurance.

Section 40(1)(q): Allows disclosure to a public body or law enforcement agency in Canada to assist in an investigation of a law enforcement matter as defined in **section 1(h)**.

Disclosure under **section 40(1)(q)** is, in the absence of any statutory requirement, at the discretion of the public body. You should satisfy yourself that there are properly documented and reasonable grounds for requesting the information, consult with your own legal counsel and, if in doubt, require a search warrant,

subpoena or court order for the information.

FOIP Tip: *Always get the request in writing, asking for it to be faxed if the request is made over the telephone. After receiving the written request, telephone the office asking for the information and confirm that the person asking is at that office.*

Section 40(1)(s): Allows for disclosure so that the spouse, relative or friend of an injured, ill or deceased individual may be contacted.

This facilitates informing those who need to know in the event of a workplace accident or one that occurs in a school, post-secondary institution, health care body or other public body.

Section 40(1)(x): Allows disclosure for the purpose of managing or administering personnel of the Government of Alberta or the public body.

A disclosure may be for the purpose of *managing* personnel when it is related to the duties and responsibilities of those the information is about.

It may be for the purpose of *administering* personnel when it is related to staffing, classification or compensation, to a program of occupational health or safety, or to training and development (*IPC Investigation Report 2001-IR-006*).

As with other disclosures, you should take care to find out exactly what the requestor needs to know and disclose only that information. Examples of permitted disclosures would include transfer of information between

departments or agencies of a public body (e.g. between schools within a school jurisdiction) when an employee is transferred, as well as verification of information given by the employee to another department or agency within the public body.

Particular care should be taken when contemplating disclosing personal information to facilitate outsourcing programs or divesting operations to the private sector (*IPC Investigation Report 2001-IR-006*).

Section 40(1)(bb.1): Allows for disclosure of an individual's name and business contact information, when it does not reveal other personal information about the individual.

For example, the kind of business card information that is printed on a letterhead or a business card can normally be routinely disclosed.

This provision would allow a school to provide the bus driver's name and phone number to a parent, or a university to publish a staff directory. For more information, see *FOIP Bulletin No. 13 on Business Contact Information*.

Section 40(1)(cc): Allows for disclosure to the relative of a deceased individual if, in the opinion of the head of the public body, the disclosure is not an unreasonable invasion of the deceased's personal privacy.

The sensitivity of the information being sought and the relationship of the requestor to the deceased individual need to be very carefully considered. Examples include informing named beneficiaries of the benefits available to

them, providing a social insurance number or information about salary or wages.

Medical information should be carefully reviewed when considering release. There may be circumstances when the privacy rights of an individual are not diminished by death, and these may include the circumstances of the death (*Ontario Order M-206*).

If you work for a health care body, note that there is no provision in the *Health Information Act* for disclosure of medical information to a deceased's relative, except when needed to provide a health service to a descendant of the deceased.

This is different from disclosure to the administrator of an estate (**section 84(1)(a)** – see below).

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

Imminent means that the harm is likely to happen immediately or very soon. *Reasonable grounds* means that there is evidence that the danger or harm will happen unless the disclosure of personal information is made.

Examples of this would be disclosure by the police to a victim that a certain violent offender who has made threats has escaped from prison, or disclosure to a supervisor of a student residence that a certain student resident has threatened suicide.

Other Considerations

Could disclosure be harmful to the individual the information is about or to public safety (section 18)?

This section allows you to refuse to disclose to a person information about themselves in certain circumstances. This would only happen in exceptional circumstances and the opinion of a qualified medical professional should be obtained (**section 18(2)**). The FOIP Regulation, **section 6** details procedures to be followed.

Section 18(3): Note that the head may refuse to disclose information to an applicant that reveals the identity of an individual who provided information in confidence about a threat to an individual's safety or mental or physical health.

Is information evaluative or opinion material, provided in confidence and compiled for determining the individual's eligibility for a benefit (section 19)?

Confidential evaluations concerning benefits for persons on disability leave would fall into this category and you may decide not to make them available to the employee.

Batch reports: Some computer programs produce batch reports with pay and benefits information about several employees on the same sheet. Past practice may have been to place copies on each file – this is no longer appropriate. These reports should be severed before anyone views the records. Only the employee's own information should be on their file.

Administrator of an estate: Section 84(1)(a) provides for the personal representative of a deceased person to exercise the rights and powers of that person but only in relation to the administration of the estate. The executor of an estate, or someone representing the executor (such as a relative or lawyer) has limited rights to personal information under this section.

Information on entitlements such as death benefits, vacation pay, life insurance, etc. is necessary to allow the estate to be administered and closed. Other personal information, including information related to employment history, medical information and violation of law information must be carefully examined to ensure its disclosure would not be an unreasonable invasion of the personal privacy of the deceased.

Identification numbers: Employee numbers should not be disclosed in circumstances where they might be used to find personal information other than that normally contained on a business card.

Social insurance numbers are intended solely for income tax, employment insurance, student loans, Canada Pension Plan and social allowance purposes and should not be used for other purposes without authorization by the Government of Canada.

Numbers that identify individuals as treaty or band members should not be disclosed, as they would reveal racial or ethnic origin.

Personal health numbers are intended solely for identification purposes within

the health care system and should not be used for other purposes without consent. Under the *Health Information Act*, only custodians and persons authorized by the regulations under the Act have the right to require an individual to provide their personal health number.

Separation agreements, severance agreements, and pension benefits:

The Information and Privacy Commissioner considered boilerplate severance agreements in *Order 2001-020*, which dealt with the City of Calgary. The agreements contained information such as a recitation of the consideration for the agreement, a confidentiality clause, a clause about the agreement being the entire agreement, and a clause in which the third party releases the City from liability. These boilerplate clauses are not personal information within the meaning of **section 17** and can be released under the Act.

The records also contained personal information. This included:

- the name of the other party to the agreement;
- that individual's job title or position;
- the individual's employee number;
- that individual's signature;
- the date the individual's employment was to end;
- the date of the individual's retirement; and
- the severance paid to that individual.

The Commissioner stated that a severance package is an employment-related "benefit" for the purposes of **section 17(2)(e)** of the Act. Severance is a beneficial payment or an advantage that flows from the employment relationship to the employee, whether or not it is

actually paid before the relationship formally ends, and whether or not it is required by law.

A severance package is also a “discretionary” benefit when a public body exercises its discretion to negotiate mutually acceptable compensation with a third party. This creates the necessary element of a degree of discretion.

Given this finding, the Commissioner upheld the City of Calgary’s decision to disclose the job titles or positions, and the basic terms of the severance agreement, including precise sums.

Order 2001-020 required other personal information to be withheld as it constituted employment history (**section 17(4)(d)**) or would reveal the name of the individual together with other personal information (**section 17(4)(g)(i)** and **(ii)**). This applied to each third party’s name, signature, employee number, the date the employee’s employment with the City was to end, and the date the employee was to retire.

In *Order F2003-002*, pension benefits were found to be a “discretionary benefit” because the City’s council had discretion whether or not to award pension benefits, even though the City’s administration had no discretion. However, the pension recipients’ names, signatures and retirement dates were not disclosed.

When considering severance and separation agreements, consideration should be given to whether disclosure of such information:

- is desirable for the purpose of subjecting the activities of your public body to public scrutiny (**section 17(5)(a)**);
- where disclosure could damage anyone’s reputation (**section 17(5)(h)**);
- whether the information was supplied in confidence (**section 17(5)(f)**): and,
- whether it could cause harm to your local public body in negotiating future settlements (**section 25(1)(c)(iii)**).

In all cases, consultation with the third party is recommended using the procedures laid out in **sections 30** and **31** of the FOIP Act.

Attendance reports or sick leave utilization: Some local public bodies post information on utilization of sick leave or days absent from work. It may be possible to argue that this is necessary for the management of personnel (**section 40(1)(x)**), but this may be challenged given the definition of *manage* in *IPC Investigation Report 2000-IR-006* and investigated as a breach of privacy. Consider whether the same results could be achieved by posting utilization reports on an aggregate basis for a unit, branch or school, without personal identifiers.

2.4 STAFFING

These records fall into the following categories:

- information about the job and staffing process – job profile, candidate profile, advertising materials and expenditures, staffing options, consultant inventories and information;

- application process – unsolicited resumés, applications and resumés, confirmation of receipt of application, summaries of resumés, phone records, confirmation of qualifications;
- screening and interview process – candidate lists, screening and interview panel members, screening factors and sub-factors, screening results, tests, interview schedules, expenses, assessment process, interview plans, decisions and advice, interview notes, ratings, rankings, certifiable applicant lists;
- reference and other checks – confirmation of checks made, names of references contacted, results of checks, criminal record checks, driver’s abstract checks, firearms checks, medical information;
- offers of employment or rejection – letters of offer, letters to unsuccessful candidates, contracts for service;
- abolishment and redeployment – seniority lists, abolishment or surplus inventory, eligibility determination, referrals, job search results from outplacement agencies, severance and separation agreements; and
- resignation and termination – letters of resignation or termination, exit interviews.

This section also deals with providing reference information.

Requests for this information may come from employees who have been successful in a competition and from unsuccessful candidates. Generally speaking, personal information about the individual requestor is made

available, while information about other candidates is not.

In some cases consideration will have to be given to **section 19** (Confidential Evaluations) and **section 24** (Advice from Officials) before making a decision about disclosure.

INFORMATION ABOUT THE JOB AND THE STAFFING PROCESS

Routine Disclosure

- Profile of the job and description of the ideal candidate are public information.
- Factual information about staffing options (e.g. permanent versus temporary) can be disclosed once a decision has been made on the course to follow (**section 24(1)(d)**).
- Any personal information should be severed unless it refers to the individual requesting the records.
- Any records relating to delegation of staffing authority, excluding any evaluative material about individuals (**section 17(2)(e)**).
- Advertising material, expenditures on advertising and media strategy.
- Consultant inventory.

Considerations

Records dealing with staffing strategies: These should be examined carefully. These could contain information about appointing candidates without a competition, whether to limit the competition and so on. Until a decision has been made and the chosen option exercised, these records may be excepted from disclosure under **section 24(1)(d)**. Once the decision has been made, they may be severed if they meet

the Commissioner's test for "advice" under **section 24(1)** (*IPC Order 96-006*).

Information in records dealing with human resource

consultants: These should be examined to ensure that information is not disclosed that would reveal business or commercial information supplied in confidence which, if disclosed would harm the business interest of a third party. The FOIP Act provides a three-part test in **section 16** to determine whether disclosure would harm third party business interests and all three parts must be satisfied if disclosure is to be refused. If you and your FOIP Coordinator believe the records meet the requirements of **section 16**, the consultant must be contacted before any information is disclosed (**section 30**).

FOIP Tip: *Even if it is clear that the records meet the three-part test, consider contacting third parties and seeking their opinions on your decision. Confirmation from a third party that the individual believes the disclosure could harm his or her interests will strengthen your case in the event of a request for a review of your decision not to release the records.*

APPLICATION PROCESS

Applying for a job is a private matter. Job candidates can be vulnerable to harm, not only during the course of the staffing action but also after the staffing has been completed, especially if the results were disappointing. You need to be careful to withhold information that can confirm or deny the status of an individual with regard to a competition. For example, even disclosing a part of a candidate's expense claim would reveal

that he or she had applied and been interviewed for a job. Routine disclosure is not recommended for these records.

Considerations

Unsolicited resumés: These should be considered either as transitory records or given specific retention periods and disposed of in a secure manner within a short time frame after receipt. The provincial government retention and disposition schedule enables them to be destroyed after six months. Unless it is clear that the writer wishes the resumé to be circulated, care should be taken in providing the resumé to other staff even though such disclosure may be permitted on a need to know basis under **section 40(1)(h)** or **(i)** in the case of common or integrated programs.

Summaries of resumés: These may be made for panel members or decision-makers. The applicant has the right to examine his or her own summary for accuracy and may request corrections (**section 36**).

Records of telephone

conversations: These may be considered as transitory records unless they form a part of the decision-making process. Remember, however, that they are accessible while they exist.

Records which confirm

qualifications: These may be collected either from the candidate or from other sources (**section 34(1)(n)**).

They should be shared only with those who have an absolute need to see them – a statement of confirmation should suffice for most purposes.

SCREENING AND INTERVIEW PROCESS

Routine Disclosure

- Names of screening or selection panel members, including job titles (**section 17(2)(e)** and **section 40(1)(b)**).
- Screening criteria.
- Factors and sub-factors used in interview assessments can be disclosed after the interview has taken place.
- Interview plans and questions can be disclosed if disclosure would not harm contractual negotiations after the interview has taken place (**section 26(1)(c)(iii)**).
- Ratings and rankings can be disclosed provided no personal identifier is disclosed (i.e. numerical information only).
- Candidates are entitled to see all of their own personal information, provided that all information about other candidates is severed from the records. There are some exceptions to this noted below.

Considerations

Candidate lists: These lists must be severed of all personal information relating to candidates other than the requestor.

Examination or test questions: The FOIP Act does not apply to questions that are to be used on examinations or tests (**section 4(1)(g)**). Note that the section employs the future tense – it may be necessary to show that the questions are going to be used in future tests. Ontario’s Information and Privacy Commissioner has ruled that

questions are public information once they are used even if they may be used again (*Ontario Order P-351*).

Test results: If candidates for a position write tests, the results of those tests may be accessible, subject to severing of personal information. Following an inquiry in British Columbia, the public body under review adopted a policy of releasing test answers after severing the name of the candidate, ratings of specific answers (other than pass/fail) and identifiable details of the individual (*B.C. Order 52-95*).

Interview schedules: These schedules must be severed of all personal information other than that of the requestor.

Assessment factors and sub-factors: These may be excepted from disclosure under **section 24(1)(b)** providing there is evidence to prove that they are under review up to the point of the interview.

Interview panel discussions and advice: If the discussions and advice of the interview panel are recorded, **section 24(1)(a)** and **(b)** may apply when considering disclosure. This applies to personal information about the applicant.

Panelist notes: If a summary of the panel’s views is made, notes made by panelists are considered transitory and should be disposed of in a secure manner. If no summary is made and decisions are based on the notes themselves, they must be retained for *at least* one year.

Candidate lists: Lists of certifiable candidates may be withheld until

references have been checked as recommendations (**section 24(1)(a)**).

REFERENCE AND OTHER CHECKS

Confidentiality in staffing matters is not always understood in the same way by all the parties involved. This understanding is critical as some records can only be withheld when it is established that the information was received in confidence (**section 19**). It is strongly recommended that, when you wish to indicate that information is being exchanged in confidence, you make this explicit during the exchange and on the records in question.

Otherwise, when collecting or providing reference information you should make it clear to the other party that the opinions being given will be accessible to the candidate in most instances (**section 2(c)**). “Off the record” remarks noted about a candidate made by a former supervisor who was not named by the candidate as a referee were found by the Commissioner to be reference information. The fact that there were made “off the record” was taken to mean they were made in confidence (*IPC Order F2003-007*). It is only necessary that a public body collect information in confidence, not that the applicant be aware that the information is being collected in confidence (*IPC Order F2003-020*).

FOIP Tip: *You cannot guarantee confidentiality under the FOIP Act but you can make a commitment to describe the material as confidential and to follow security measures against accidental disclosure to emphasize that you are treating the material as confidential.*

In collecting reference information, you have two responsibilities: to ensure that candidates are treated ethically while successfully gaining additional information about these prospective employees. Complete information is required in order to avoid potentially damaging outcomes.

Other kinds of records, such as criminal or child welfare record checks should only be collected when an employment offer is being considered or extended. Such checks should not be required of a candidate’s spouse (*IPC Investigation Report F2002-IR-011*). Health information collected to screen prospective employees should be limited to what is necessary for the hiring decision. If additional information is required to provide health services for employees, that information should be collected after the individual is hired (*IPC Investigation Report F2002-IR-010*).

Section 34(1)(n) allows a local public body to collect personal information indirectly for the purpose of managing or administering personnel matters. This gives you the authority to collect, without specific consent, reference information from any party. Remember, however, that at this stage you are seriously considering this person as an employee and might want to consider how such action would affect your relationship.

Routine Disclosure

- You can confirm to candidates that reference checks were made without disclosing the content of the information.

- Names of references should be provided to individuals about whom the information is gathered.
- When a common set of questions is used in gathering information, these can be provided to any requestor.
- You can confirm to individuals what other checks were made and, subject to considerations outlined below, the contents of those checks.

Considerations

Section 17(4)(f): This states that disclosure of personal recommendations or evaluations, character references or personnel evaluations are presumed to be an unreasonable invasion of privacy. This does not apply to the names of those contacted (which may be an unreasonable invasion of privacy under **section 17(4)(g)**), only to the contents of the reference.

The following test should be used to determine whether personal information constitutes *personal evaluations* or *personnel evaluations*:

- Was the particular evaluation done by a person who had authority to do that evaluation?
- Was an assessment either made according to measurable standards or based upon professional judgment? The professional judgment criterion can be satisfied if it is shown that knowledge, training and experience has been applied in making the assessment.

If both of these questions are answered in the affirmative this test will be satisfied and the information in question will qualify as *personal evaluations* or *personnel evaluations* (IPC Order 97-

002). Thus, if reference information is taken from a performance appraisal conducted according to standard procedures it may fall into this category. If the information is provided as an opinion based on observation then it will not fall into this category although some other provision of **section 17** may apply.

Section 19: Public bodies may refuse to disclose personal information that is:

- evaluative or opinion material,
- when the information is provided, explicitly or implicitly, in confidence, and
- the information was supplied for the purpose of determining suitability, eligibility or qualifications for employment or for the awarding of contracts.

As all three parts of this test must be met, it is important to be able to show that the information was provided in confidence and was used for assessing the qualifications or abilities of the candidate. The exception applies whether the person who provided the reference is an employee of your local body or not. In *Order F2002-008*, the Commissioner upheld the use of the exception when an employee is applying for a new position within the public body, and the referee is the individual's supervisor.

Unsolicited material, such as references attached to an application or opinions provided without a request, is not shielded under this provision.

FOIP Tip: *Since this is a discretionary exception, you should document evidence that shows how you exercised discretion in case there is a request by the applicant for a review by the Commissioner of your decision.*

Although **section 34(1)(n)** allows you to collect personal information necessary for managing or administering personnel matters, some types of personal information checks should only be done if you can demonstrate the necessity for them to assess the candidate's suitability or fitness for the job. The candidates should be aware when criminal records checks, driver's abstract checks, medical or fitness checks or checks with regard to firearm certificates will be carried out.

FOIP Tip: *Because of the sensitive nature of information gathered through these additional checks, it is suggested that this information be kept confidential and only disclosed to those persons within the organization who have a need to know.*

PROVISION OF REFERENCE INFORMATION

The FOIP Act provides a framework for provision of reference information to other persons. **Section 40(1)(x)** allows you to provide reference information about a current or former employee only to another department or agency within your public body.

Personal information, such as attendance, performance, or salary history cannot be provided to any outside party without the specific consent of the individual (**section 40(1)(d)**).

Confirmation of the individual's claimed service record (start date and end date) is not an unreasonable invasion of privacy. Confirming an individual's salary to an interested

employer, or an institution such as a bank, requires prior consent.

Any information provided must be maintained for a year and is accessible to the individual on request.

FOIP Tip: *Employees need to provide consent to enable their supervisor or other public body employees to provide a reference to a potential employer outside their public body. The candidate can either provide the consent to their supervisor and other referees, or he or she can provide the consent to the potential employer. In the latter situation, the supervisor providing the reference should ask for confirmation that consent was given.*

Consent must be received in writing unless the public body has established "rules" to accept consent electronically or orally in accordance with section 7 of the FOIP Regulation. For more information about the requirements for obtaining consent in writing, in electronic form and orally, see Bulletin No. 17 on Consent and Authentication.

Sometimes employees or students will ask for "generic" references from supervisors, human resource staff or teaching staff. The fact that they have asked does not meet the consent requirements of the FOIP Regulation (**section 7**). One suggestion is to begin such letters with a sentence such as:

"At his request and with his complete knowledge of these contents, I am writing to you about..."

The letter of reference can then be given to the person requesting it or shown to that person for approval prior to being sent.

FOIP Tip: *Although **section 40(1)(x)** allows for the provision of reference information to another department or agency of your public body, it is strongly recommended that a public body obtain the consent of the employee before providing sensitive information such as medical information, information about fitness or disabilities, information about a person's criminal history, or information related to religious or political beliefs. It is also recommended that a public body consider the circumstances of each case when responding to such requests, particularly if it is evident that the individual has deliberately chosen not to provide the public body (his/her employer) as a reference.*

OFFERS OF EMPLOYMENT

Routine Disclosure

- The records that fall within this category would be routinely available to the individual they are about.
- Announcements about new employees are public information.
- Disclosure of the total amount and some other details of a fee for service contract is not an unreasonable invasion of personal privacy (**section 17(2)(f)**).

Considerations

Announcements about new employees or appointments to boards: These should be made with the consent of the individual. The easiest way to do this is to obtain consent or approval on the text of the announcement before release.

Fee for service contracts: These need to be carefully considered to ensure that the information about the individual is actually personal information. Personal information about sole proprietors is considered to be personal information if that person actually provides the service.

ABOLISHMENT AND REDEPLOYMENT

Routine Disclosure

The information about an individual is available to that individual, but care must be taken to ensure that all identifiable information about other individuals is severed from the records.

Considerations

Employee evaluations: Any evaluations about employees which meet the three-part test of **section 19** may be withheld from disclosure.

Collective bargaining agreements: Some collective bargaining agreements have clauses based on seniority. Posting or disclosure of seniority lists could be deemed to be an unreasonable invasion of privacy (**section 17(4)(d)**) unless it is specifically authorized in an agreement or contract approved by employees. It is suggested that only the minimum information needed to satisfy the requirement be disclosed.

Future employment potential: Ontario's Information and Privacy Commissioner has ruled that information about a person's future employment potential does not constitute employment history (*Ontario Order P-621*).

Information collection: You should be careful in collecting any information, such as job search results from outplacement agencies, once the employee has terminated service.

Release of severance or separation agreements: Careful consideration must be given to release of severance or separation agreements. Basic terms of the agreement, including precise sum of the severance, may be disclosed under **section 17(2)(e)** (*IPC Order 2001-020*).

For further information see Chapter 2.3 of this guide.

RESIGNATION AND TERMINATION

Considerations

Letters of resignation or termination: These carry the same privacy protection requirements as letters of application or disciplinary records.

Exit interviews or exit surveys: These may be used with departing employees. You need to have a clear policy on the purpose and uses of the information gathered during such surveys or interviews and ensure that the employee understands this. Where possible, the information should be anonymous. If this is not possible, personal identifiers should be severed when it is being shared within the public body. *B.C. Order 111-96* dealt with this subject and contains useful information and advice about policy and practice.

EXCHANGE OF INFORMATION BETWEEN PUBLIC BODIES

When an employee moves from one local public body to another local public body, to the provincial government or to an agency, which operates independently within a municipality, you may be asked to transfer information in human resource records. In such circumstances it is necessary that the records be reviewed to ensure that only information absolutely necessary is transferred. Individual consent must normally be obtained for such transfers.

2.5 TRAINING AND DEVELOPMENT

These records fall into the following categories:

- course design and materials – terms of reference, learning objectives, contractor information and proposals, contents of course, leader's and participant's manuals;
- participant information – course lists, learning contracts, expense claims, evaluations;
- leave, bursary and sabbatical program information and approval criteria; and
- individual employee information – course or leave requests, courses attended, programs of studies, exchange agreements, return service commitments, competency profile, evaluative material.

The records are a mix of general information and personal information that may be withheld under **section 17(4)(d)** as employment and educational history.

Routine Disclosure

- General material about training courses such as terms of reference, general learning objectives, etc.
- Course materials, subject to consideration below regarding licences or proprietary interest.
- General information about educational leave, bursary and sabbatical programs, including criteria for application and/or acceptance.

Considerations

Contractor information and proposals: These are subject to **section 16** review. This provides a three-part test for confidential third party proprietary information. Third party notice should be given under **section 30**.

Contracts for course development and delivery: These can be disclosed subject to severing of pricing information and bearing in mind that you may have to negotiate similar contracts in the future (**sections 16(1)** and **25(1)(c)**).

Training materials: You need to determine whether your public body has a proprietary interest that has a monetary value (**section 25(1)(b)**).

Section 25(1) deals with the potential for financial loss to your local public body. You will need to prove reasonable intent to market the materials

Participant information: This is all regarded as personal information subject to **section 17(4)(d)**. If you

intend making course lists available for any purpose other than registration or for reference by the instructor, you should include a notice on the registration form or participant listing form so that the participants know of this intent in advance (**section 34(2)**). This includes making the list available to other participants.

FOIP Tip: *Course participant lists should never contain information other than that found on a business card.*

Course evaluations: These can be disclosed unless they are obtained for the purpose of evaluating the person or organization delivering the course for future employment or contracting (**section 19**).

In such cases the evaluations would have to be provided in confidence to your local public body, not to the instructor.

Post-secondary educational institutions can disclose teaching and course evaluations completed by students for the purpose of assisting students in selecting courses (**section 40(3)**).

Individual employee information: This is considered to be personal information subject to **section 17(4)(d)**. Because some types of staff exchanges, educational leave or sabbatical leaves are discretionary benefits, you would have to consider releasing some information under **section 17(2)(g)**. This would likely include:

- the name of the individual receiving the benefit;
- the nature and scope of the benefit; and
- the time period involved.

It would not include financial details such as salary paid. If a return service commitment is waived, it too could be considered a discretionary benefit, this time of a financial nature (**section 17(2)(h)**).

Instructor/trainer evaluation of employees: Evaluations of employees provided by instructors or trainers would normally be accessible to the individual employee unless they meet the test of **section 19**.

2.6 EMPLOYEE RELATIONS

These records fall into the following categories:

- collective bargaining process and results – input to collective bargaining, information about negotiations, memorandum of agreement, collective bargaining agreement, and mediation and arbitration information and decisions;
- bargaining agent relations – information about exclusions from bargaining unit, union dues and refunds, union stewards lists, time off for union business, and employer-employee committees;
- grievances – designated grievance officers, delegated authorities, employee grievance forms and supporting documents, decisions on grievances, including decisions by boards; investigation notes, and witness statements;
- disciplinary actions; and
- complaints from the public about employees.

Routine Disclosure

- Signed memorandum of agreement or collective bargaining agreements.
- Arbitration decisions.
- Decisions on exclusions of positions from bargaining unit – with any personal information severed.
- Lists of designated grievance officers and delegated authorities (**section 17(2)(e)**).
- Decisions of designated grievance officers are made available to the person who lodged the grievance and the bargaining agent if a request is made to comply with **section 40(1)(o)**.
- Union stewards lists (**section 17(2)(e)**).

Considerations

Collective bargaining: Input into the collective bargaining process may be considered as advice from officials and be withheld under **section 24(1)**. Details of this input, as well as information about the negotiations and the positions being taken by your local public body, may also be withheld under **section 25(1)(c)(iii)** as disclosure could reasonably be expected to interfere with these negotiations.

Disclosure of personal information: Sometimes during the collective bargaining process, it may be necessary to disclose personal information to describe how a particular benefit package would affect employees or when issues being negotiated relate directly to specific individuals. It may also be necessary to access personal information about employees to prepare a position or understand an issue. Wherever possible this information

should be used or disclosed in a way that removes personal identifiers.

FOIP Tip: *When personal information is used in this way it is a consistent use of the information. However, it is not a regular or described use of this information and should be noted on the record.*

Legal privilege: Information used during the collective bargaining process may also be subject to legal privilege (**section 27(1)**). The Commissioner has provided criteria for use in determining when records meet the requirements of this provision (*IPC Orders 96-015, 96-017 and 2000-019*).

FOIP Tip: *In considering solicitor-client privilege, each document must be considered separately. The confidentiality of the information is important, so such records should not have been copied outside of the local public body. Finally, the whole document must be withheld – severing is not an option.*

Mediation/arbitration: Applications for mediation or arbitration, and the information contained in briefs to mediators or arbitrators, should also be considered for exception under **section 25(1)(c)(iii)**. Some of this information will be shared with other parties to the mediation or arbitration process as a part of that process, but personal information should be severed to comply with “need to know” provisions wherever possible during that sharing.

Individual employees can be third parties whose labour relations information, in the form of interviews or statements, would be provided in confidence to a mediator or other person inquiring into a grievance or

other labour relations dispute. Consideration should be given to whether **section 16(1)(a)(ii), (b) and (c)(iv)** applies to this information (*IPC Order 2000-003*). If all three sections apply then you must sever as this is a mandatory exception to disclosure.

Exclusion of positions from a bargaining unit: Information concerning exclusion of positions from a bargaining unit may be shielded from disclosure under **section 24(1)(d)** as plans that have not yet been implemented. Once the decision has been implemented, these records would be subject to release.

Union dues and refunds: Information about union dues and refunds is available to the individual employee in relation to his or her own deductions. This information is also provided to the bargaining agent when dues are deducted from employees as a part of the payroll system. Where this happens, personal information should be kept to a minimum.

Union-related time off: Information about time off for union business is available to the individual concerned, to the supervisor if there is a need to know (**section 40(1)(h)**) and to a designated officer of the bargaining agent with the individual’s authorization (**section 40(1)(o)**).

Employer-employee committees or employer-union committees: These may be used for a variety of purposes concerning health and safety, working conditions and benefits. Personal information should only be disclosed on a need to know basis under **section 40(1)(x)** unless authorized by statute or a collective agreement.

Grievance procedures: A collective agreement usually sets out procedures to be followed at each stage of the process and who should be involved. Employees should expect that personal information necessary to resolve a grievance would be shared with employee representatives, grievance officers and arbitration boards. This process would meet the definition of consistent purpose set out in **section 41**. The collective agreement may also have wording in it that sets an expectation of confidentiality for disciplinary matters.

FOIP Tip: *If a collective agreement does not explicitly authorize the employer to disclose personal information, the employer's ability to disclose such information about third parties other than the grievor is less clear. These individuals may not even be aware of the grievance and therefore cannot have reasonably expected their information to be disclosed. Consent may be necessary.*

Grievance investigation notes: These should be carefully prepared to meet the Commissioner's test for advice under **section 24** if you intend to shield them from disclosure as advice from officials.

Disciplinary proceedings and investigations: Disciplinary proceedings and investigations may be considered to be a law enforcement matter if they are undertaken to enforce compliance with standards, duties and responsibilities of employees as defined in an Act, Regulation or bylaw of the public body.

A breach of employment duties that would render an applicant subject to

disciplinary action would not be a violation of "law" because those duties are not set out by a law that provides for penalties or sanctions if the duties are breached. A penalty or sanction would be imposed pursuant to conditions of employment rather than a "law" (*IPC Orders 2000-019 and 2000-023*). The records compiled during such proceedings may not constitute advice or deliberations unless they pass the Commissioner's test outlined in *IPC Order 96-006*. Transcripts of statements, incident reports and records of facts normally cannot be shielded from disclosure under **section 24**.

Decisions of a health professional body, or any other body at an appeal of a decision of a health professional body, dealing with regulated health professionals working for health care bodies may be subject to the *Health Information Act*.

Personal information: Personal information about third parties, including witnesses or others involved in the investigation, would normally be severed either under **section 17(4)(b)**, where the information is an identifiable part of a law enforcement record, or under **section 17(4)(g)**, where the third party's name appears with other personal information of the third party or if disclosure of the name itself would reveal third party personal information.

Special attention needs to be given to whether or not the personal information needs to be disclosed to ensure a fair determination of an applicant's rights (**section 17(5)(c)**) and whether the information provided was supplied in confidence (**section 17(5)(f)**).

Results of disciplinary action:

These may be a matter of public record. For example, school boards are required to pass all motions in public with respect to the termination or transfer of an individual. Wherever possible such public records should preserve the anonymity of the individual by using non-identifying information.

FOIP Tip: *If the deliberations on such matters are held in camera then the substance of those deliberations may be withheld under **section 23(1)** (see also **section 18** of the Regulation).*

Recommendations contained in a report or courses of action recommended to the board would reveal the substance of discussions (*B.C. Order 62-95*). Remember that background information cannot always be withheld, as it may not reveal the substance of deliberations.

Hearings: Hearings may be recorded for record-keeping purposes. If the applicant is present throughout an oral hearing, it is unlikely that he or she can be denied access to the audiotapes of the same proceedings, subject to exceptions in the FOIP Act. The Information and Privacy Commissioner of British Columbia has issued two orders on this subject (*B.C. Orders 204-97 and 205-97*) in which he required the tapes to be severed.

He further stated that tape recordings of whole proceedings cannot be claimed as notes or *aides-memoire* and, therefore, as not subject to the Act.

FOIP Tip: *If a verbal reprimand is given to an employee, it is suggested that the record contain nothing more than a notation that the reprimand was*

given and the subject matter. Placing the substance of the conversation on the record will make it available to the employee who can dispute the summary and request correction.

Complaints from the public about employees

The information within the complaint will likely constitute *personal information* of the employee under **section 1(n)(viii)**. The employee, then, has the right to access this information unless one of the exceptions in **Part 1, Division 2** of the FOIP Act applies.

You will also have to make decisions on whether provision of the personal information of the complainant constitutes an unreasonable invasion of that individual's privacy. Finally, you will have to make decisions on whether the personal information of either party should be disclosed to anyone else under **section 40**.

Considerations

Section 1(h)(i) and (ii) defines "law enforcement" as a "police, security or administrative investigation including the complaint giving rise to the investigation that leads or could lead to a penalty or sanction". To meet the definition, the duties or matters being complained about would have to be set out in an Act, Regulation or bylaw of a public body.

Does your policy on complaints include a statement about "confidentiality"? In some instances the complainant may ask that the complaint records be kept confidential and not be shared with other individuals. Your public body may not be able to do this because personal information may

have to be disclosed to enable investigation of the complaint and to provide answers to the complainant. **Section 17(4)(b)** allows for disclosure of personal information in a law enforcement record to the extent that disclosure is necessary to dispose of the law enforcement matter or to continue an investigation.

Does your policy specifically indicate who will be provided with copies of the complaint so that the complainant knows this at the time of making the complaint?

This may be governed by Codes of Conduct or Ethics that apply to your local public body.

Does your policy contain any guidelines that would apply to disclosing the identity of the complainant to the person about whom the complaint is made?

Generally speaking it would be reasonable to provide this information. However, you should consider whether or not it could reasonably be expected to threaten anyone's safety or mental or physical health (**section 18(1)(a)**); whether it would harm the investigation (**section 20(1)(a)**) or would reveal the identity of a confidential source of law enforcement information (**section 20(1)(d)**).

Complaint investigations:

Complaints generally lead to investigations, whether formal or informal. Once information is accepted and recorded it may be requested under the FOIP Act. When an individual participating in the investigation does not require personal information, the personal identifiers should be removed from any records made available to that

individual if practical to do so (**section 17**).

Legal representatives and union officials:

Legal representatives and union officials are entitled to access personal information of their clients if the client provides written authorization for that access or appoints them as his or her agent (**section 84(1)(f)** and **section 40(1)(o)**).

Investigation reports: Reports prepared during and as a result of an investigation should, wherever possible, shield the identity of witnesses, reporters and others involved by using identifiers that cannot reveal their identity (e.g. X, Witness 1). There may be exceptions to this policy when the identity of the individual is essential to an understanding of the issue or the fair determination of someone's rights. In such cases, it should be clear to the individuals that their identity will be revealed, and to whom.

Copies of investigation reports:

You may be asked for copies of investigation reports by a complainant, particularly for the records provided by respondents. Unless release of personal information about the complainant would be harmful to anyone's safety or mental or physical health (**section 18(1)**), or would harm a law enforcement matter (**section 20(1)**) this should be released. Personal information about the respondent should be severed.

2.7 WORKPLACE HEALTH AND SAFETY

These records fall into the following categories:

- work site audit and inspection reports – safety inspections, air quality or environmental quality reports, ergonomic assessments;
- accident reports – employee and supervisor reports, investigation reports; and
- WCB documentation – reports and correspondence to the Workers’ Compensation Board.

Routine Disclosure

- Personal information can be disclosed to the individual it is about.
- Audit and inspection reports, providing individual employee personal information is severed.
- WCB cost statements, providing any third party names are severed from the printout.

Considerations

Medical information: Medical information may be withheld from an employee if it could reasonably be expected to cause immediate and grave harm to the mental or physical health of the employee. You must seek the advice of a medical professional if you are considering this action (**section 18**).

Testing or auditing procedures or techniques: These may be withheld if disclosure could reasonably be expected to prejudice the use or results of particular tests or audits (**section 26**).

WCB records: Employees requesting their own WCB records should be advised to request information from the Board. However, they cannot be denied access to the personal information you

have in these records in your custody or under your control.

Accident reports: These should be anonymized if there is no *need to know* the individual’s personal information.

Health care bodies: Any records that contain “diagnostic, treatment and care information” about individuals will be subject to the *Health Information Act*.

2.8 WORKPLACE HARASSMENT

These records contain very sensitive information and could result in either law enforcement proceedings or human rights investigations. This area of human resource information has been the most frequent cause of reviews by Information and Privacy Commissioners in British Columbia and Ontario.

You should regularly review your local public body’s policy and procedures to ensure they comply with the FOIP Act.

Generally speaking, the purpose of an investigation into harassment is to provide justice for the complainant, the alleged harasser and those asked to provide evidence. It is highly invasive for any parties involved without, in addition, subjecting them to public attention that will not serve the purpose of the investigation.

Considerations

Does your policy clearly indicate what information will be shared between the complainant and the respondent? Disclosure of the name of the complainant may, in some circumstances, be an unreasonable

invasion of privacy, while in others, disclosure of the name without any other personal identifiers may be acceptable. Note that the complaint itself may be a “law enforcement record” (**section 1(h)**) and so disclosure of the complaint might be an unreasonable invasion of personal privacy under **section 17(4)(b)**.

Section 17(5)(f): In *Order F2003-014*, the Commissioner upheld the public body’s decision to withhold notes and interviews collected during a harassment investigation. The Commissioner found that the personal information collected during interviews had been supplied in confidence. This was evident from the public body’s policy documents and in recorded interviews. The Commissioner found it would be an unreasonable invasion of privacy to disclose information that was collected in confidence.

Section 17(5)(h): Unfair damage to an individual’s reputation must be considered when dealing with these cases, especially if the investigation is not completed, the case is still under review or the allegation was unfounded.

Section 17(5)(e) and section 18: These provisions should be considered, especially if there is or has been any evidence of threatening behavior on the part of the respondent. It may still be possible to disclose information with personal identifiers removed, depending on the format of the record and the intertwining of information.

Section 17(5)(c): Fair determination of an applicant’s rights must be considered, especially if the applicant is taking legal action. If an investigation

exceeded its terms of reference or was otherwise deemed to be flawed, then this would be a relevant circumstance to consider for disclosure of the report of that investigation (*B.C. Order 78-96*).

Publication of complaint: If a complainant has made public the fact that a complaint has been lodged, then it is probably reasonable to disclose details of the complaint. However, each record still needs to be carefully examined to ensure there is no unreasonable invasion of a third party’s privacy.

In other provinces, commissioners have allowed for a zone of confidentiality with respect to matters related to both the investigation of harassment complaints and the conduct of subsequent or related disciplinary proceedings.

In British Columbia, the Commissioner has been careful to protect the integrity of the investigative and decision-making process. Identifying information of the parties to the investigation will not be disclosed but the policies and procedures of a hearing are subject to some degree of public scrutiny. An applicant outside the process will not be permitted access to the complainants’ names and the substance of their complaints, including handwritten interview notes or investigation reports.

An applicant’s right to access information about themselves may be qualified since the privacy of the individuals involved in the complaint is very important. Thus, a respondent is unlikely to have access to the names of complainants or any other information that could identify them.

It is suggested that you place emphasis on protection of privacy when dealing with these records.

2.9 VIOLATION OF LAW INFORMATION

These records fall into the following categories:

- information about an employee's criminal history – this may be derived from a criminal records check; and
- information compiled as a part of an investigation into a possible violation of law – whether the investigation is concluded or still in progress.

Considerations

Any information about a person's criminal history is considered to be *personal information* and can only be disclosed with consent or in accordance with other provisions of **section 40**.

Reference checks: Criminal record information or violation of law information generally should not be disclosed in a reference check unless the employee has consented and it is relevant to the position being applied for.

Law enforcement investigations:

The information can be disclosed without consent to another public body or law enforcement agency 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 (**section 40(1)(q)**).

Information compiled as part of an investigation into a possible violation of law cannot be disclosed except to the extent that disclosure is necessary to continue the investigation or to dispose of the matter (**section 17(4)(b)**).

FOIP Tip: *Always consult with your legal advisor if a request is made for information regarding any violation of law.*

2.10 VOLUNTEERS

The FOIP Act defines *employee* in relation to a public body as including a person who performs services for the public body as a volunteer (**section 1(e)**). It is recommended that relationships with volunteers should be formalized and that they understand their obligations under the Act respecting the protection of personal information. A confidentiality undertaking may be a good idea.

Increasingly, volunteers carry out tasks formerly done by paid employees in local public bodies. They are in direct contact with clients, students and patients. They often collect personal information from these individuals and provide that information to employees of the local public body. They may also be in positions where they are required to use personal information and protect that information.

It is recommended that you treat volunteers the same way as you treat other employees. This means providing basic training about protection of privacy. It also means ensuring that the personal information collected from volunteers is done in compliance with the FOIP Act,

and is protected in the same way as the personal information of paid employees.

In this context, appointed members of governing boards or advisory boards are considered as volunteers or appointees. Their personal information is subject to the same rules and procedures and they can have information disclosed to them under **section 40(1)(h) or (i)**.

Considerations

- Be sure that you collect only that information needed to ensure that the volunteer can accomplish the tasks assigned and which is required to manage your volunteer program.
- Be sure that you have consent to disclose any personal information used in volunteer recognition programs.
- Maintain records about volunteers with the same concern for privacy as you have for paid employees, and have similar retention and disposition procedures for those records.
- Include a section on FOIP in your volunteer training and any manuals provided for use by volunteers.

2.11 CORPORATE EMPLOYEE RECORDS

Corporate employee records (often called the “official” file) will usually contain the complete employment history of an individual, from initial application for employment through commencement, annual appraisals, promotions and demotions, transfers and resignation or termination.

Some government departments in Alberta and other provinces have found it useful to divide these files to make access easier and avoid having to sever records when third parties use them. It would be time-consuming to retroactively convert these records, but consideration should be given to dividing the files as they are used:

- Information that is generally accessible to anyone can be placed in one section of the file. This would include such things as the position description and classification information.
- Information that would be accessible to a supervisor or other employee with a need to use that information can be placed in a second section. This would include such things as emergency contact information, performance appraisals, attendance records and disciplinary information.
- The remainder of the material is normally available only to the individual employee and should be secured. This would include such things as benefit use records, medical information, insurance information and next of kin records.

FOIP Tip: *Although the Commissioner has not yet ruled on access to employee records, it is expected that need to know will be rather narrowly interpreted as it has been in other provinces. The person asking to see the records should have to prove that there is a real need to see the information – “fishing” expeditions are to be discouraged.*

An employee could request that sensitive personal information in his/her file be removed prior to it being accessed by another individual. This might include medical information provided in the past

to a person who is the individual's current supervisor.

Many of these corporate employee records have been described and the FOIP implications outlined in previous sections of this guide. The following additional categories will be covered in this section:

- performance appraisals and evaluations;
- qualifications and specializations;
- recognition awards and payments;
- newsletters;
- charitable donations;
- social functions;
- safety certificate records;
- employee assistance records; and
- medical information.

Professional staff in educational bodies often have special qualifications or specialist diplomas or degrees. The Information and Privacy Commissioner in British Columbia has held that these constitute personal information and cannot be disclosed without consent (*B.C. Order 139-96*). Their basic degree or licensing requirement may be disclosed.

Personal information disclosed during the giving of awards should always be approved by the individual before disclosure. The amount of an award can be disclosed under **section 17(2)(h)** as long as it is done in such a way as not to reveal actual salary information.

Section 17(2)(j)(iii) and **section 17(2)(j)(iv)** would permit the disclosure of an employee's attendance at or participation in a public event or activity related to the public body or the receipt of a honour or award granted by

or through the public body unless the employee has requested that the information not be disclosed. This section does not permit the disclosure of other honours and awards listed on a resume. In the same way, inclusion of personal information about an employee in a newsletter should always be reviewed with the employee prior to publication and consent obtained to its publication. This includes any photograph of an employee.

When an employee gives consent to payroll deduction it is reasonable to assume that the consent extends to providing some personal information to the charity for which the deduction is being made. This information should be held to the minimum needed to enable the charitable organization to fulfil its purpose, and should not include any identifying numbers.

Release of information to enable contact about social functions whether organized officially by the public body or by some type of social committee given sanction to organize such functions can be considered disclosure for a consistent purpose. However, this would not extend to giving out birth dates for the purposes of celebrating birthdays, information about births, deaths or other family events. Such information is best gathered within the work unit on an informal, consensual basis and used in an informal manner.

Employees may have achieved special safety training, including such things as hazardous materials courses, safe driving courses or first aid courses. This information is considered to be a part of educational and employment history and is subject to the same protection as other

information which falls into this category. If these qualifications are essential to the performance of the individual, then they can be disclosed under **section 17(2)(e)** or they may have to be disclosed where there are health and safety reasons for such disclosure.

Many local public bodies offer employee assistance programs to employees in the areas of alcohol and substance abuse; psychological counselling; bereavement or trauma counselling and stress. Disclosure is an unreasonable invasion of privacy under **section 17(4)(a)**. Disclosure of detailed medical or psychological information about themselves to employees should be done on the advice of a medical professional and, if possible, with a qualified person present to explain or interpret the information.

PERFORMANCE APPRAISALS AND EVALUATIONS

Appraisals and evaluations can take many forms, and the way in which they are treated under the FOIP Act will depend upon the purpose and use of the documents.

If the appraisal or evaluation is carried out using a standardized methodology or form, and/or with clear definitions and instructions, then the resultant record will fall into the definition of personnel evaluations in **section 17(4)(f)** and its disclosure would be an unreasonable invasion of privacy.

Generally appraisals and evaluations are carried out in order to assess employee performance, help employees to improve performance and allow decisions to be made on remuneration.

Employees have access to their appraisals, and supervisors also have access to them. Appraisals from previous positions in the same public body are accessible to supervisors of the employee in his or her current position.

FOIP Tip: *It might be helpful to have a written policy describing who, in the chain of command, has access to an appraisal record.*

Sometimes polls or surveys are used to evaluate individuals or services generally. When the identity of the individuals responding to the survey is not needed by persons reviewing this information, the results should be anonymized.

The identity of the person who does an appraisal or evaluation is that person's own personal information. In determining whether to release the identity of the appraiser or evaluator, consideration should be given to **section 17**, and in rare cases, **section 18**. You might want to consider a policy on this subject and obtain consent from the person doing the appraisal to the release of his or her name and business title.

360 DEGREE APPRAISALS

Where peers, subordinates, clients and supervisors are asked to assess an individual's performance, in a confidential, formal evaluation process, the head of a public body may refuse to disclose identifying information of the evaluators or assessors, except for supervisors (**sections 19(2)** and **(3)**).

MEDICAL INFORMATION

Local public bodies may require prospective employees to have a medical examination as a condition of being

offered a job. In other cases, agreements dealing with extended medical leave or stress leave may require an opinion from a qualified practitioner on whether or not an employee is fit to resume work. Health professionals who are working on contract to the local public body may provide these examinations or opinions.

If a medical opinion is provided in confidence to a public body for the purposes of determining an applicant's eligibility or suitability for employment, the public body may refuse to disclose the information to the individual it is about (**section 19(1)**).

Employees may also provide medical information in confidence to the local public body. This may take the form of applications for insurance, justification for sick leave or other absences, results of any testing required by the job, counseling or psychological testing, ergonomic testing or information connected with a disability.

This information is not accessible to other employees or supervisors without consent (**section 17(4)(a)**). It should be segregated from other information and stored securely.

For employees of custodians pursuant to the *Health Information Act* (e.g. regional health authorities, physicians, long term care centers, Alberta Health and Wellness etc.), all health information is subject to the Act.

2.12 HEALTH INFORMATION ACT AND EMPLOYEE RECORDS

Alberta's *Health Information Act* (HIA) applies to certain human resources information in the custody or under the control of custodians pursuant to HIA. This information falls into the following categories:

Diagnostic, treatment and care information as defined in section 1(1)(i) of HIA. This includes information about the physical or mental health of an individual; health services provided to an individual; results of tests or examinations of a body part or bodily substance; information about drugs provided to an individual; information about health care aids, devices, products, equipment or other items provided to an individual and the amount of any benefits paid or payable in respect of a health service provided to an individual.

Registration Information as defined in section 1(1)(u) of HIA. This includes demographic information, including the individual's personal health number, location and telecommunications information; residency information; health service eligibility information and billing information.

Health Services Provider Information as defined in section 1(1)(o) of HIA. This includes name, business and home addresses and telephone numbers, gender, date of birth, information about the type of health services provider and licence number; educational and competency information; restrictions that apply to the individual's right to provide health services; decisions of a health professional body regarding the

individual's right to provide health services; profession and job classification and employment status.

A health services provider is anyone who provides health services as defined in HIA and will include all regulated health professionals, and those employed in regulated health disciplines, working in health care bodies.

For health services providers, the following types of information found in human resource records will fall under the *Health Information Act*:

- Name, gender, date of birth, home and business address, telephone number, electronic address and facsimile number.
- Unique identification number assigned to the individual for the purpose of the operations of the public body and that uniquely identifies the individual in relation to that public body.
- Job classification.
- Profession, type of health services provider and licence number.
- Educational information, including entry level competencies attained in a basic education program and post-secondary degrees, diplomas or certificates, and continued competencies, skills and accreditation including specialty or advanced training.
- Information related to decisions of a health professional body.
- Employment status and the number of years the individual has practiced in the profession.

Disclosure of this information is subject to section 37 of HIA. Consult with your

FOIP/HIA contact before routinely disclosing this information.

For all employees, the following types of information will fall under the *Health Information Act*:

- General or extended illness reports;
- Long term disability information;
- Medical assessments and reviews;
- Health information collected during the staffing process;
- Accident reports and investigation reports into workplace health and safety if they contain identifying health information;
- WCB documentation;
- Workplace harassment reports if they contain information about the physical or mental health of the individual;
- Health information gathered for the purposes of insurance applications;
- Counselling or psychological testing information;
- Ergonomic or other information associated with a disability.

Disclosure of this information to third parties is subject to section 35 of HIA. This is more restrictive than section 40 of the FOIP Act and you should consult with your FOIP/HIA contact. Routine disclosure is not recommended.

Disclosure to the employee that the information is about is subject to exceptions set out in section 11 of HIA. Records would be reviewed in the same way as for a FOIP request by the individual.