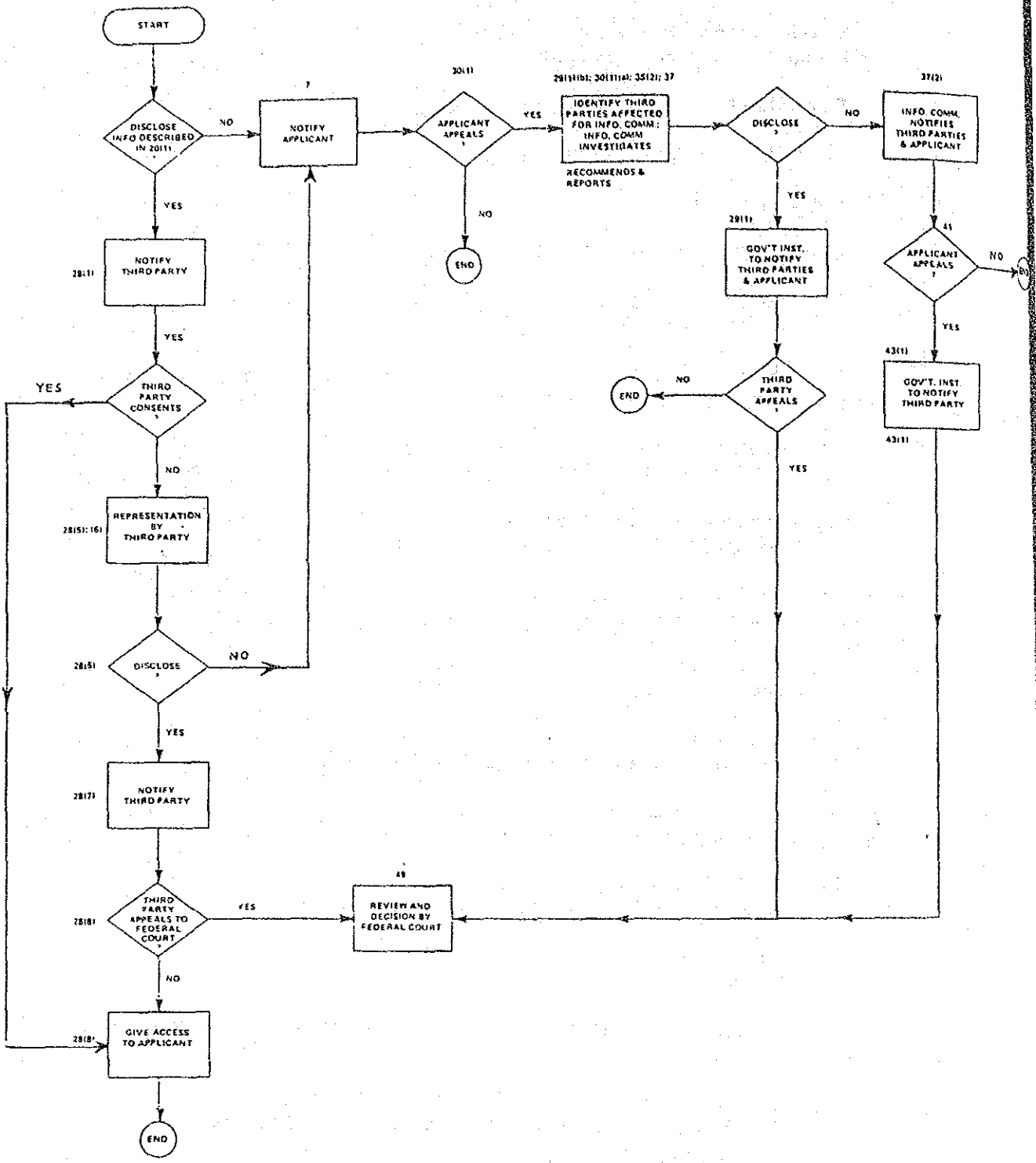
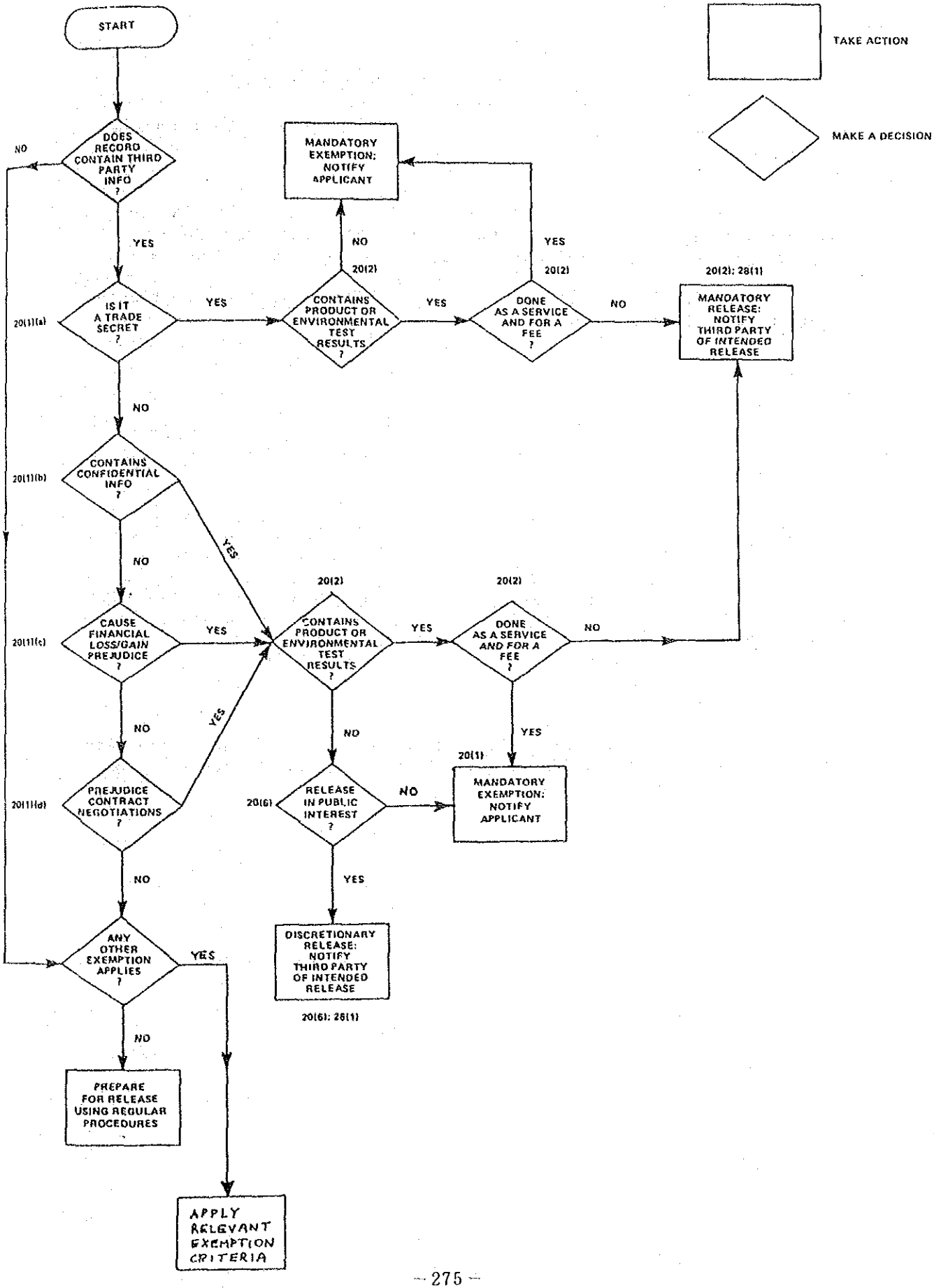
THIRD PARTY NOTIFICATION AND INTERVENTION



THIRD PARTY EXEMPTION APPLICATION PROCEDURES



MODEL LETTER 'A'

NOTICE TO THIRD PARTY OF INTENTION TO DISCLOSE

Request reference No:

Dear:

This (Department/Agency/Commission/Board, etc.) has in its possession records that contain information which (belongs to/was supplied by/relates to) you/your Company.

On (date) pursuant to the Access to Information Act we received a request for the following record(s):

_____

_____.

Although we have reason to believe that these records might contain

(information as described in paragraph 28(1)(a), (b) or (c)), we do not have sufficient information in our files to substantiate this. Thus, as required by the Act, we intend to disclose the record on (date).

You have 20 days from the mailing date of this Notice to make written representations to the undersigned as to why the record should not be disclosed. If you have not responded by the expiry of the 20-day period, the record will be disclosed on the date set out above. Any representations you make will result in a review of our decision to disclose the record.

Copies of sections 20 (the exemption for third party information) and 28 (the provision dealing with notification of third parties) are enclosed for your convenience.

Yours truly,

Access to Information Coordinator

Enclosures

MODEL LETTER 'B'

NOTICE TO THIRD PARTY OF INTENTION
TO DISCLOSE IN THE PUBLIC INTEREST

Request reference No:

Dear:

This (Department/Agency/Commission/Board, etc.) has in its possession records that contain information which (belongs to/was supplied by/relates to) you/your Company.

On (date) pursuant to the Access to Information Act we received a request for the following record(s):

_____

_____.

Although the information contained in the record(s) falls within section 20(1) ((b), (c) or (d)) of the Act, it is our opinion that its disclosure would be in the public interest as it relates to public health, public safety or protection of the environment and that public interest outweighs in importance any financial loss or gain to, prejudice to the competitive position of a interference with contractual or other negotiations of a third party. Therefore, pursuant to subsection 20(6) of the Act, we have decided to comply with the request to disclose.

You have 20 days from the mailing date of this Notice to make written representations to the undersigned as to why the record should not be disclosed.

If you have not responded by the expiry date of the 20-day period, the record will be disclosed on (date).

Copies of sections 20 and 28 of the Act are enclosed for your convenience.

Yours truly,

Access to Information Coordinator

Enclosures

MODEL LETTER 'C'

NOTICE TO THIRD PARTY OF INTENTION TO DISCLOSE
FOLLOWING REPRESENTATIONS BY THIRD PARTY

Request reference No:

Dear:

On (date) this (Department/Agency, etc.) received your representations in response to our Notice dated _____, 19__.

We have considered your views and have decided that the records for which access have been requested are not exempt from disclosure under subsection 20(1) of the Access to Information Act.

We are entitled to request a review of this decision by the Federal Court - Trial Division, pursuant to section 44 of the Act. That request for review must be made within 20 days of the mailing date of this Notice.

If you do not request a review of this matter, the person who requested the record will be given access to it on (date).

A copy of section 44 of the Act is enclosed for your convenience.

Yours truly,

Access to Information Coordinator

Enclosure

MODEL LETTER 'D'

NOTICE TO THIRD PARTY OF INTENTION TO DISCLOSE
IN THE PUBLIC INTEREST FOLLOWING REPRESENTATIONS BY THIRD PARTY

Request reference No:

Dear:

On (date) this (Department/Agency/Commission/Board, etc.) received your representations in response to our Notice dated _____, 19__.

We have considered your views and have decided that the public interest in disclosure clearly outweighs in importance any prejudice to your interests. Thus, we intend to disclose the record(s) on (date).

You are entitled to apply to the Federal Court - Trial Division for a review of this decision pursuant to section 44 of the Act. That request for review must be made within 20 days of the mailing date of this Notice.

If you do not request a review of this matter, the person who requested the record will be given access to it.

A copy of section 44 of the Act is enclosed for your convenience.

Yours truly,

Access to Information Coordinator

Enclosure

MODEL LETTER 'E'

NOTICE TO THIRD PARTY OF DECISION NOT TO DISCLOSE
FOLLOWING REPRESENTATIONS BY THIRD PARTY

Request reference No:

Dear:

On (date) this (Department/Agency, etc.) received your representations in response to our Notice dated _____, 19__.

We have considered your views and have decided that the record(s) to which access has been requested is exempt under paragraph 20(1) _____ of the Access to Information Act. Thus, the record(s) will not be disclosed.

The applicant has been informed of this decision.

However, under the Access to Information Act the applicant has one year from the time access was requested to complain to the Information Commissioner concerning this refusal to disclose.

You will be advised if there are further developments in this matter.

Yours truly,

Access to Information Coordinator

MODEL LETTER 'F'

NOTICE TO APPLICANT OF DECISION TO DISCLOSE
RECORD ON RECOMMENDATION OF INFORMATION COMMISSIONER

Request reference No:

Dear:

As a result of the recommendation of the Information Commissioner regarding your complaint we have reviewed our earlier decision with respect to the record(s) you requested and have decided to disclose (it/them).

Third parties which may be affected by the disclosure have been notified of the decision to disclose and have 20 days to apply to the Federal Court - Trial Division for a review of this matter. Accordingly, the record(s) will be disclosed to you on the expiry of this period unless an application to the Court is made by a third party.

You will be advised of any such request.

Yours truly,

Access to Information Coordinator

MODEL LETTER 'G'

NOTICE TO THIRD PARTY OF COMPLAINT TO INFORMATION COMMISSIONER

Request reference No:

Dear:

This (Department/Agency, etc.) has in its possession records that contain information which (belongs to/was supplied by/relates to) you/your Company.

On (date) pursuant to the Access to Information Act, we received a request for the following record(s):

_____

_____.

We decided that the records were exempt from disclosure under paragraph 20(1) _____ of the Act.

However, the applicant has complained to the Information Commissioner who will be undertaking an investigation of the matter. If the Commissioner makes a preliminary decision to recommend that the records be disclosed, you will be contacted by the Commissioner's office and will be given an opportunity to make representations as to why the record(s) should not be disclosed.

You will be advised of further developments in this matter.

Yours truly,

Access to Information Coordinator

MODEL LETTER 'H'

NOTICE TO THIRD PARTY OF INTENTION TO DISCLOSE
RECORD ON RECOMMENDATION OF INFORMATION COMMISSIONER

Request reference No:

Dear:

Please refer to our Notice dated _____, 19__.

The Information Commissioner has completed his investigation of this matter and has recommended that the record(s) be disclosed.

As a result of that, we have reviewed our earlier decision not to disclose the record(s) requested and we have decided to disclose it.

You are entitled to apply to the Federal Court - Trial Division for a review of this decision pursuant to section 44 of the Access to Information Act. That request for review must be made within 20 days of the mailing date of this Notice.

If you do not apply for a review of this matter within the 20-day time limit, the record(s) will be disclosed to the applicant.

A copy of section 44 of the Act is enclosed for your convenience.

Yours truly,

Access to Information Coordinator

Enclosure

MODEL LETTER 'I'

NOTICE TO THIRD PARTY OF DECISION TO DISCLOSE
RECORD ON RECOMMENDATION OF INFORMATION COMMISSIONER

(NO PREVIOUS NOTICE)

Request reference No:

Dear:

This (Department/Agency, etc.) has in its possession records that contain information which (belongs to/was supplied by/relates to) you/your Company.

On (date) pursuant to the Access to Information Act, we received a request for the following record(s):

_____

_____

We decided that the records are exempt from disclosure under paragraph 20(1) _____ of the Act.

However, following a complaint by the applicant and an investigation by the Information Commissioner's office, the Information Commissioner has recommended that the record(s) be disclosed.

As a result of this, we have reviewed our earlier decision not to disclose the record(s) requested and we have decided to disclose it.

You are entitled to apply to the Federal Court - Trial Division for a review of this matter pursuant to section 44 of the Act. That request for review must be made within 20 days of the mailing date of this Notice.

If you do not apply for a review of this matter within the 20-day time limit, the record will be disclosed to the applicant.

A copy of section 44 of the Act is enclosed for your convenience.

Yours truly,

Access to Information Coordinator

Enclosure

MODEL LETTER 'J'

NOTICE TO THIRD PARTY OF APPEAL BY APPLICANT OR INFORMATION COMMISSIONER TO FEDERAL COURT

Request reference No:

Dear:

Please refer to our Notice dated _____, 19__.

Following a complaint by the applicant to the Information Commissioner and an investigation by the Commissioner, we decided to abide by our earlier decision that the record(s) requested is/are exempt from disclosure under paragraph 20(1) _____ of the Access to Information Act.

The (applicant or Information Commissioner) has applied to the Federal Court - Trial Division for a review of this matter.

Under section 43 of the Act you have a right to appear as a party to the review.

Yours truly,

Access to Information Coordinator

MODEL LETTER 'K'

NOTICE TO APPLICANT OF APPEAL BY THIRD PARTY TO FEDERAL COURT

Request reference No:

Dear:

Please refer to our Notice dated _____, 19__.

Please be advised that (name) who would be affected by the disclosure of the records you have requested has applied to the Federal Court - Trial Division for a review of this matter under section 44 of the Access to Information Act.

Under section 44 of the Act you have a right to appear as a party to the review.

Yours truly,

Access to Information Coordinator

MODEL LETTER 'I.'

NOTICE OF INTENTION TO
DISCLOSE TESTING RESULTS UNDER SS. 20(2)

Request reference No:

Dear:

This (Department/Agency/Commission, etc.) has in its possession records that contain information which (belongs to/was supplied by/relates to) you/your Company.

On (date) pursuant to the Access to Information Act we received a request for the following record(s):

Although the information contained in the record(s) falls within paragraph 20(1) ((b), (c) or (d)) of the Act, in our view, the record(s) contain(s) the results of product or environmental testing carried out by or on behalf of this institution and, therefore, under subsection 20(2) of the Act we cannot refuse to disclose it.

You have 20 days from the mailing date of this Notice to make written representations to the undersigned as to why the record(s) should not be disclosed. Your representations must be confined to the following:

(1) that the record(s) does not contain the results of product or environmental testing carried out on behalf of a government institution, or

(2) that the testing was done as a service to a person, a group of persons or an organization other than a government institution and for a fee.

If you have not responded by the expiry date of the 20-day period, the record(s) will be disclosed on (date).

Copies of section 20, the exemption for third party information and section 28, the provision dealing with notification of third parties, are enclosed for your convenience.

Yours truly,

Access to Information Coordinator

Enclosures

MODEL LETTER 'M'

NOTICE TO THIRD PARTY OF INTENTION TO DISCLOSE
UNDER SS. 20(2) FOLLOWING REPRESENTATIONS BY THIRD PARTY

Request reference No:

Dear:

On (date) this (Department/Agency/Commission/Board, etc.) received your representations in response to our Notice dated _____, 19__.

We have considered your views but reconfirm our position that the information which has been requested falls under subsection 20(2) and that it should be disclosed.

You are entitled to apply to the Federal Court - Trial Division for a review of this matter pursuant to section 44 of the Access to Information Act. That application for review must be made within 20 days of the mailing date of this Notice.

If you do not apply for review, the person who requested the record(s) will be given access to it.

A copy of section 44 of the Act is enclosed for your convenience.

Yours truly,

Access to Information Coordinator

Enclosure

Treasury Board Canada

Interim Policy Guide:
Access to Information Act and The Privacy Act

Part III - Privacy

Table of Contents

		Page(s)
.1	Introduction	1-12
.1.1	Purpose and scope	1-2
.1.2	Application	2
.1.3	Authorities and cancellations	2
.1.4	Roles and responsibilities	3-7
.1.4.1	Parliament	3
.1.4.2	Department of Justice	3-4
.1.4.3	President of the Treasury Board	4-5
.1.4.4	Government institutions	5-6
.1.4.5	Privacy Commissioner	6-7
.1.4.6	Federal Court	7
.1.5	Definitions	7-12
.2	Collection, retention and disposal of personal information	13-24
.2.1	General principles	13
.2.2	Collection of personal information	14-19
.2.2.2	Information not to be collected unless relevant to programs	14-15
.2.2.3	Direct collection where information to be used for administrative purpose	15-17
.2.2.4	Informing individual of purpose of collection and other particulars	17-19
.2.3	Accuracy of personal information used for administrative purpose	19-20
.2.4	Retention and disposal of personal information	20-24

.2.4.1	Purpose	20
.2.4.2	Framework for the scheduling, retention and disposal of personal information	20-23
.2.4.3	Minimum two year retention	23
.2.4.4	Additional provisions	23-24
.3	Use and disclosure of personal information	25-59
.3.1	General principles	25-26
.3.2	Purpose	26
.3.3	Use of personal information	26-27
.3.4	Disclosure of personal information	27
.3.5	Process for obtaining consent	28-32
.3.5.1	Consent at of time of collection	28
.3.5.2	Consent subsequent to collection	29
.3.5.3	Consent by minors	30
.3.5.4	Consent by incompetents	30
.3.5.5	Consent in respect to deceased individuals	30-31
.3.5.6	Consent by representative of individual	31-32
.3.6	Consistent use	32-33
.3.7	Permissible disclosures of personal information	33-55
.3.7.1	Original purpose and consistent use	34-35
.3.7.2	Act of Parliament or regulation	35-36
.3.7.3	Subpoenas, warrants, court orders and rules of court	36-37
.3.7.4	Attorney General for use in legal proceedings	37
.3.7.5	Federal investigative bodies	37-40
.3.7.6	Provinces, foreign states and international bodies	40-42
.3.7.7	Members of Parliament	42-43
.3.7.8	Audit purposes	43
.3.7.9	Archival purposes	44
.3.7.10	Research or statistical purposes	44-45
.3.7.11	Native claims research	45-46
.3.7.12	Payment of a benefit and collection of a debt	46-47
.3.7.13	Public interest	47-55

.3.8	Disclosure by the Public Archives	55-58
.3.9	Information publicly available	55-58
.3.10	Addresses and mailing lists	58-59
.4	Accounting for use and disclosure of personal information	60-65
.4.1	General principles	60
.4.2	Purpose	60
.4.3	Statement of purposes	60-61
.4.4	Routine uses not included as primary or consistent uses	61-62
.4.5	Retention of use and disclosure record	62-64
.4.6	Consistent uses not previously accounted for	64-65
.5	Right of access to personal information	66-80
.5.1	Purpose	66
.5.2	Informal access	66
.5.3	General requirements for processing formal requests	67-69
.5.4	Notices	69-71
.5.5	Exemption Application procedures	71-74
.5.6	Method of access	74-75
.5.7	Language of access	75-76
.5.8	Corrections and notations	76-80
.6	Excluded Records	81
.7	Exemptions - Privacy	82-115
.7.1	General principles	82-86
.7.2	Purpose	86
.7.3	Authorization	87
.7.4	Severability	87-88
.7.5	Consultation	88-89
.7.6	Exemptions	90-115
.7.6.1	Exempt banks (section 18)	90-93

.7.6.2	Information obtained 'in confidence' (section 19)	93-95
.7.6.3	Federal-provincial affairs (section 20)	95-96
.7.6.4	International affairs and defence (section 21)	96-100
.7.6.5	Law enforcement, investigations and security of penal institutions (section 22)	100-108
.7.6.6	Security clearances (section 23)	109-110
.7.6.7	Individuals under sentence (section 24)	110-111
.7.6.8	Safety of individuals (section 25)	111
.7.6.9	Information about another individual (section 26)	112-113
.7.6.10	Solicitor-client privilege (section 27)	113-114
.7.6.11	Medical record (section 28)	114-115
.8	Review of decisions under the Privacy Act	116-126
.8.1	General principles	116
.8.2	Purpose	116
.8.3	Review by the Privacy Commissioner (sections 29-35)	116-121
.8.4	Review of exempt banks by Privacy Commissioner	121-122
.8.5	Review of compliance with sections 4 to 8 by the Privacy Commissioner	122
.8.6	Review by the Federal Court	123-125
.8.6.1	Order to remove file from exempt bank	125-126

Appendices

A	Schedule of government institutions under the Privacy Act and heads of institutions
B	Privacy Regulations
C	Forms and form components: Use and disclosure of personal information
D	Model letters and forms relating to the right of access under the Privacy Act

.1 Introduction

.1.1 *Purpose and scope*

The purpose of Part III of Chapter 410 is to assist in the interpretation of the Privacy Act, to set forth the requirements which institutions must carry out to give effect to its provisions, and to prescribe directives and guidelines to be followed by institutions as a matter of government policy.

The Act (section 2) extends the laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to such information.

Part III of this Chapter contains two important codes which deal with the protection of privacy. The first governs the collection, retention and disposal of personal information. The second controls the use of personal information and its disclosure to persons other than the individual to whom the information pertains. The latter code is reinforced by measures designed to ensure a full accounting of all use and disclosure of personal information.

The right of access to information about themselves which the Act accords to individuals is described. The process for responding to requests for access made under the Act is explained, including such matters as time limits, manner and language of access, and rights of correction and notation of personal information.

Certain material which is excluded from the application of the Act is described. Material subject to the Act, broadly referred to as information about an identifiable individual that is recorded in any form, is defined.

Limited and specific exceptions to the right of access, called exemptions, are explained. Guidance is given to institution to assist them in deciding, in the light of these exemptions, whether or not to grant access to personal information requested under the Act. The principle of severability, requiring that access be given to any non-exempt part of personal information requested, is covered.

The concluding section deals with the independent review of government decisions made under the Act. It describes the two-tier system established for this purpose and relates the review roles of the Privacy Commissioner and the Federal Court.

The scope of this Part of the Chapter does not include the requirement of section 11 of the Act for the publication at least once a year of an index containing descriptions of personal information under the control of government institutions. Chapter 411 - Inventory of information addresses this requirement.

Also excluded from the scope are the provisions of paragraph 71(1)(b) and subsections 71(3) to (5) of the Act respecting the registration, approval and review of personal information banks. Chapter 415 - Information collection covers these matters.

.1.2 *Application*

Part III of this Chapter applies to government institutions listed in section 3 of the Privacy Act subject to subsection 71(2) of the Act.

.1.3 *Authorities and cancellations*

Part III of this Chapter is issued under the authority of the Privacy Act. It is also authorized by the Financial Administration Act by which the Treasury Board may act on all matters relating to administrative policy in the Public Service of Canada. Treasury Board minute 787442 applies.

Previous policy on privacy, contained in the following chapters, is cancelled:

- Chapter 415 - Disclosure and use of personal information; and
- Chapter 420 - Access to personal information.

.1.4 *Roles and responsibilities*

The purpose of this article is to describe the roles and responsibilities of Parliament, the Department of Justice, Treasury Board, government institutions, the Privacy Commissioner and the Federal Court in the operation and review of the Privacy Act. Reference is made, where applicable, to sections of the Act which authorize the roles and responsibilities outlined, and to other areas of this policy which deal more fully with the nature and extent of the particular requirements.

.1.4.1 *Parliament* designates or establishes a committee to be responsible for:

(a) undertaking a comprehensive review of the provisions and operation of the Act within three years after it comes into force (subsection 75(2) of the Act);

(b) reporting to Parliament the results of this review, including any changes recommended, within one year after undertaking it (subsection 75(2)); and

(c) reviewing the administration of the Act on a permanent basis (subsection 75(1)).

.1.4.2 *Department of Justice* is responsible for:

(a) maintaining a broad overview of the application of the Act in relation to the intentions of the government and the expectations of the public;

(b) advising the designated Minister on any administrative questions giving rise to broad policy issues;

(c) providing legal interpretation and advice respecting the provisions and operation of the Act;

(d) gathering case and precedent information for use in the provision of legal interpretation and advice; and

(e) coordinating the preparation of the government for the parliamentary review of the provisions and operation of the Act.

.1.4.3 *President of the Treasury Board*. The President of the Treasury Board is the designated Minister under the Act and has the following responsibilities:

(a) preparation and distribution to institutions of directives and guidelines governing the operation of the Act and the regulations (paragraph 71(1)(d));

(b) annual publication of the Index of Personal Information (section 11);

(c) prescribing such forms as may be required for the operation of the Act and the regulations (paragraph 71(1)(c));

(d) prescribing the form of, and what information is to be included in, annual reports to Parliament by heads of institutions (paragraph 71(1)(e));

(e) reviewing the manner in which personal information banks are maintained and managed to ensure compliance with the provisions of the Act and the regulations (paragraph 71(1)(a));

(f) reviewing the utilization of existing personal information banks and proposals for the creation of new banks by government institutions that are departments as defined in section 2 of the Financial Administration Act (subsections 71(3) and (5)); and

(g) approving the establishment and substantial modification of personal information banks by government institutions that are departments as defined in section 2 of the Financial Administration Act (subsections 71(4) and (5)).

The Treasury Board Secretariat supports the President in the discharge of these responsibilities as Designated Minister and in addition:

- provides advice to institutions on any aspect of the administration of the Act and on regulations and policies pursuant to it; and
- prepares a consolidated annual report on the administration of the Act across the government.

.1.4.4 *Government institutions*. The head of each institution is responsible for administration of the Act within the institution in accordance with requirements of the Act, and with regulations and directives and guidelines pursuant to it. While the head of the institution is accountable for carrying out these responsibilities, he or she may, by order, designate one or more officers or employees of the institution to exercise or perform any of the duties, powers or functions assigned to the head by the Act.

The Privacy Coordinator in each institution is responsible for coordinating the discharge of the institution's responsibilities. The responsibilities of each institution are:

- to submit to the Designated Minister a description of banks and classes of personal information, including with respect to banks a statement of the purposes and uses of the information, and retention and disposal standards applying to it, in accordance with the requirements of section 11 of the Act and Chapter 411 - Inventory of information;
- to respond to requests for personal information under the Act: to grant or refuse access, to correct or make notations to information, to issue notices to applicants, and to give general assistance to individuals seeking information about themselves;

- to defend its decisions to grant or refuse access before the Privacy Commissioner and the Federal Court, and to ensure that the staff and the personal information of the institution are available to the Commissioner during the course of an investigation;
- to ensure that personal information is not used or disclosed to persons other than the individual to whom it pertains except in accordance with the Act and this policy, and that the institution's practices for collecting, retaining and disposing of personal information are fully consistent with the provisions of the Act, the Regulations and this policy; and
- to report annually to Parliament in accordance with section 72 of the Act and any instructions issued pursuant to paragraph 71(1)(e) of the Act.

.1.4.5 *Privacy Commissioner*. The Privacy Commissioner is the first level of the two-tier system established for the independent review of decisions made under the Act. The public may complain to the Commissioner on any of the grounds specified in subsection 29(1) of the Act. The Commissioner investigates such complaints and may also initiate them. In addition, the Commissioner may conduct investigations of personal information banks designated as exempt banks under section 18, and of compliance with the provisions of sections 4 to 8 respecting the collection, retention, disposal, use and disclosure of personal information.

In carrying out investigations, the Commissioner has the power to compel the attendance of witnesses, to require the production of evidence, and to examine any recorded information to which this Act applies. In reporting the findings of investigations, the Commissioner has the power to make recommendations concerning any matter which has been investigated, but cannot order the head of the institution to implement any recommendation.

In addition to the above responsibilities, the Privacy Commissioner may be asked by the Minister of Justice to carry out special studies on any of the matters set forth in subsection 60(1) of the Act.

The full nature and extent of the role of the Privacy Commissioner and particulars of the Commissioner's review function are discussed in articles .8.1 to .8.5 of this Part of the Chapter,

.1.4.6 *Federal Court*. Where an individual has been refused access to personal information requested under subsection 12(1) of the Act, and where complaint to the Privacy Commissioner has not resulted in the granting of access, the individual may request the Federal Court-Trial Division to review the matter. The Privacy Commissioner may apply to the Court for a review of any file contained in a personal information bank designated as an exempt bank under section 18. While many matters may be investigated by the Privacy Commissioner, only refusal of access and exempt banks may be reviewed by the Court. The Court may order the head of an institution to disclose personal information, or to remove a file from an exempt bank.

The role of the Court in relation to the Act is described in some detail in articles .8.1, .8.2, .8.6, and .8.7 of this Part of the Chapter.

.1.5 *Definitions*

An Access to Personal Information Request Form means a form prescribed by the Designated Minister for the purpose of requesting access to personal information under the control of a government institution.

Administrative purpose in relation to the use of personal information about an individual means the use of that information in a decision-making process that directly affects that individual.

An applicant is an individual who is requesting access to personal information about him or herself, who is requesting correction be made or a notation be attached to information about him or herself, or who is exercising his or her rights under the Act to review by the Court.

A complainant is an individual who is making a complaint to the Privacy Commissioner on any of the grounds set forth in subsection 29(1) of the Act.

A Correction Request Form means a form prescribed by the Designated Minister for the purpose of requesting a correction of personal information under the control of a government institution.

Court means the Federal Court-Trial Division.

The Designated Minister for the purposes of the Act is the President of the Treasury Board.

Excluded information means information to which the Act does not apply and consists of library or museum material made or acquired and preserved solely for public reference or exhibition purposes; material placed in the Public Archives, the National Library or the National Museums of Canada by or on behalf of persons or organizations other than government institution; and confidences of the Queen's Privy Council for Canada.

An exemption is a provision of the Act which entitles the head of the institution to refuse to disclose information in response to a request received under the Act. Each exemption is discussed in detail in section .7 of this Part of the Chapter.

Government institution means any federal government department, ministry of state, body or office listed in Section 3 of the Privacy Act (see Appendix A). Whenever, the term 'government institution' is referred to in this policy responsibility for the decisions involved lies either with the head of the institution or an employee of the institution delegated by the head to make such decisions.

Head of a government institution is the Minister of a department or ministry of state or, in any other case, the person designated by Order in Council to be the head of the institution for the purposes of the Act (see Appendix A).

The Index of Personal Information is a publication produced by the Designated Minister in accordance with section 11 of the Act. It contains, for each government institution subject to the Act, an index of all personal information banks and all classes of personal information under the control of the institution. Chapter 411 - Inventory of information provides a detailed description of the Index.

A Notation Request Form means a form prescribed by the Designated Minister for the purpose of requesting that a notation be made on personal information under the control of a government institution to the effect that a correction was requested but not made.

Personal information means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing:

(a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual;

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;

(c) any identifying number, symbol or other particular assigned to the individual;

(d) the address, fingerprints or blood type of the individual;

(e) the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations;

(f) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence;

(g) the views or opinions of another individual about the individual;

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e), but excluding the name of the other individual where it appears with the views or opinions of the other individual; and

(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual;

but, for the purposes of sections 7, 8, and 26 of the Privacy Act and section 19 of the Access to Information Act, does not include:

(j) information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including:

- the fact that the individual is or was an officer or employee of the government institution;
- the title, business address and telephone number of the individual;
- the classification, salary range and responsibilities of the position held by the individual;
- the name of the individual on a document prepared by the individual in the course of employment; and
- personal opinions or views of the individual given in the course of employment;

(k) information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, the name of the individual and the opinions or views of the individual given in the course of the performance of such services;

(l) information relating to any discretionary benefit of a financial nature, including the granting of a licence or permit, conferred on an individual, including the name of the individual and the exact nature of the benefit; and

(m) information about an individual who has been dead for more than twenty years.

The use of the phrase 'recorded in any form' at the beginning of this definition means that all physical media, including photographs, sound recordings or audio-visual presentations, representing identifiable individuals, constitute personal information and are, therefore, subject to the provisions of the Privacy Act.

Personal Information Bank means a collection or grouping of personal information under the control of a government institution which has been used, is being used or is available for use for an administrative purpose, or is organized or intended to be retrieved by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

The Privacy Commissioner is an official appointed under the Act who has the powers of an ombudsman. The role and functions of the Commissioner are set forth in articles .8.1 to .8.5 of this Part of the Chapter.

The Privacy Coordinator is the officer for each government institution who coordinates all activities relating to the operation of the Act, and the regulations, directives and guidelines pursuant to it, within the institution.

Under the control: Personal information is under the control of a government institution when that institution is authorized to grant or deny access to it, to govern its use and, subject to the approval of the Dominion Archivist, to dispose of it. Regarding the question of physical possession, personal information held by an institution, whether at headquarters, regional, satellite or other office, either within or outside Canada, is presumed to be under its control unless there is evidence to the contrary. Personal information held elsewhere on behalf of an institution is also under its control.

Part III

.2 Collection, retention and disposal of personal information

.2.1 *General principles*

Sections 4, 5, and 6 of the Privacy Act, section 4 of the Privacy Regulations (see Appendix B) and this policy together constitute a code governing the collection, accuracy, retention and disposal of personal information.

The code applies to all personal information obtained or compiled by the government institutions about anyone, irrespective of the source of the information, or the purposes for which it is used.

The code embodies the following general principles:

- personal information is not to be collected by government institutions unless it is relevant to an authorized program or activity (section 4 of the Act);
- personal information to be used to make a decision directly affecting an individual is as a rule to be collected directly from the individual to whom it relates (subsections 5(1) and 5(3));
- the individual is normally to be informed of the purpose of collection and intended uses of the information, and is to be apprised as well of whether response is required by law or is voluntary and of rights of access to the information (subsections 5(2) and 5(3));
- personal information to be used to make a decision directly affecting an individual is to be as accurate, up-to-date and complete as possible (subsection 6(2));
- the interests of individuals are to be protected in planning and effecting the retention and disposal of personal information (subsections 6(1) and 6(3) of the Act and section 4 of the Regulations).

The articles which follow outline the components of this code, aid in the interpretation of the provisions on which it is based, and indicate the obligations of institutions in meeting its requirements.

.2.2 *Collection of personal information*

.2.2.1 The purpose of article .2.2 is to assist in the interpretation of the provisions of sections 4 and 5 of the Privacy Act relating to the collection of personal information, to set forth the requirements which institutions must carry out to give effect to these provisions and to prescribe directives and guidelines to be followed by institutions as a matter of government policy.

The scope of the article is restricted to the restraints imposed by these sections of the Privacy Act on the collection of personal information. Overall policy on the collection of information, including certain other constraints on the collection of personal information relating to the registration, approval and review of personal information banks, is contained in Chapter 415 - Information collection.

The term 'collection' as used in this article refers to all personal information collected as a result of a request or requirement of a government institution.

.2.2.2 *Information not to be collected unless relevant to programs*. Section 4 of the Privacy Act provides that no personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution.

The intent of this provision is to promote the protection of privacy by restricting the collection of personal information by government institutions to those situations in which the information is clearly required for an appropriately authorized operating program or activity.

To give effect to this provision, institutions must have parliamentary authority for the program or activity concerned. Such authority is usually given by an Act of Parliament or regulations made thereunder, or by the approval of expenditures proposed in estimates and authorized by an Appropriation Act.

The provision further requires institutions to confirm that it is necessary to collect personal information to satisfy the needs of a particular program or activity. In this regard:

(a) where personal information is not needed, for example where summary data alone will be produced from the activity, personal information should not be collected; and

(b) where personal information is necessary, the information collected should be restricted to the minimum needed for the program or activity.

.2.2.3 *Direct collection where information to be used for administrative purpose*. Subsection 5(1) of the Privacy Act provides that a government institution shall, wherever possible, collect personal information that is intended to be used for an administrative purpose directly from the individual to whom it relates except where the individual authorizes otherwise or where information may be disclosed to the institution under subsection 8(2) of the Act. A further exception, contained in subsection 5(3) of the Act, applies where direct collection would result in inaccurate or misleading information.

The provision requires institutions, wherever possible, to collect personal information which they plan to use to make a decision directly affecting an individual from the individual to whom the information relates. The provision is designed to increase the individual's control over and knowledge of such information and to promote the collection of accurate, up-to-date and complete information.

The limiting phrase wherever possible is intended to allow for collection from another source where, for example, the individual to whom the information pertains is incapacitated or deceased, or the government wishes to pay a benefit or recover a debt and cannot locate the individual concerned, despite reasonable effort to do so. The limiting phrase does not permit collection from another source simply because it is easier or less costly to obtain the information in this way than to collect it from the individual to whom it relates.

Exceptions to requirement for direct collection. Subsection 5(1) of the Act sets out two exceptions to the requirement that an institution must collect personal information that is intended to be used for an administrative purpose from the individual concerned.

Where individual authorizes indirect collection. The first exception allows collection from another source where the individual so authorizes. In seeking such authorization, institutions should inform individuals of the nature and purpose of the information it proposes to collect and the source from whom it intends to collect the information. Individuals should also be informed either that refusal to authorize collection from another source will not result in any adverse decision about them or, if the information desired is essential to making a decision directly affecting the individual, of the consequences of refusing to authorize collection of the information. Authorization of the individual should be secured in writing whenever this is feasible.

Where information has been previously collected and is disclosable. The second exception pertains to information previously collected from the individual by another institution. In such circumstances, the exception allows an institution to receive information which it wishes to use to make a decision directly affecting an individual from another institution which has already collected the information and which is permitted to disclose the information to it under subsection 8(2) of the Act. The exception is designed to avoid the unnecessary response burden which would be imposed on individuals if they were asked the same questions by different government institutions. The exception is also intended to ensure, with provision having been made to permit disclosure of information by one institution to a second institution under subsection 8(2), that under subsection 5(1) the second institution is not prohibited from receiving the information. Direction and guidance on the application of this exception is provided in article .3.7 of this Part which covers permissible disclosures of personal information.

Where inaccurate or misleading information would result. Subsection 5(3) of the Act sets out a further exception to the requirement that an institution must collect personal information that is intended to be used for an administrative purpose from the individual concerned. This further exception permits collection of personal information from a source other than the individual to whom the information pertains where direct collection might:

(a) result in the collection of inaccurate information; or

(b) defeat the purpose or prejudice the use for which information is collected.

This exception should be used sparingly. Before resorting to the exception, an institution should be certain that the direct collection of information would bring about the damaging consequences indicated. The exception is designed primarily for use by investigative bodies listed in Schedules II, III and IV of the Privacy Regulations (see Appendix B) in those instances where the attempt to collect certain information from the individual being investigated would jeopardize the investigation.

.2.2.4 *Informing individual or purpose of collection and other particulars*. Subsection 5(2) of the Privacy Act provides that a government institution shall inform any individual from whom the institution collects information about the individual, of the purpose for which the information is being collected. An exception, contained in subsection 5(3) of the Act, applies where so informing the individual would result in the collection of inaccurate or misleading information.

The provision recognizes the individual's right to know and understand the purpose for which information about him or her is to be collected, and the use which is to be made of the information. Also, when the individual is not required by law to supply the information, such knowledge and understanding permit the individual to make an informed choice as to whether or not to provide it.

To fulfill the requirements of the provision, institutions must inform any individual from whom information about that individual is to be collected of the purpose of collection.

As a matter of administrative policy, this requirement is extended to include individuals from whom information about other individuals is being collected. Accordingly, *institutions shall inform any individual from whom information about another individual is to be collected of the purpose of collection*.

In addition, *institutions shall inform any individual from whom personal information is to be collected*:

(a) whether response is required by law or is voluntary;

(b) where response is voluntary, that refusal to respond will not result in any adverse decision about the individual or, if the information desired is essential to making a decision directly affecting the individual, of the consequences of refusing to respond;

(c) where the information pertains to the individual from whom it is being collected, that the individual has rights of access to and protection of the personal information under the Privacy Act;

(d) where the information being collected pertains to another individual and may not qualify for exemption from access by that other individual under the Privacy Act, that the information requested may be accessible to the other individual; and

(e) of the registration number of the personal information bank in which the information to be collected is to be contained.

Exception to requirement to inform individual of purpose of collection where inaccurate or misleading information would result. Subsection 5(3) of the Privacy Act allows an institution not to inform an individual from whom the institution collects personal information about the individual, of the purpose for which information is being collected where so informing the individual might:

(a) result in the collection of inaccurate information; or

(b) defeat the purpose or prejudice the use for which information is collected.

The exception authorized by this provision of the Act applies where personal information is to be collected from the individual to whom the information pertains. The exception should be employed infrequently. Before resorting to it, an institution should be certain that informing the individual of the purpose of collection would result in the adverse consequences indicated. The exception is designed for use by investigative bodies listed in Schedules II, III, and IV of the Privacy Regulations (see Appendix B) in those instances where collection of information from the individual being investigated rather than from another source is feasible, but where the investigative body cannot inform the individual of the purpose of collection without compromising the investigation. The exception is also intended to apply when a survey is being conducted and where informing the individual of its purpose would prejudice its accuracy or otherwise impair the validity of its results. Employment of this exception for any other reason must be approved by the Designated Minister prior to collection of the information. The approval process is set forth in Chapter 415 - Information collection.

The above exception also applies, as a matter of administrative policy, where personal information is to be collected from one individual about another individual. In this application, the exception is designed primarily for use by investigative bodies listed in Schedules II, III, and IV of the Privacy Regulations (see Appendix B) in those cases where it is necessary to collect information from an individual other than the one being investigated and where to inform the individual from whom the information is to be collected of the purpose of collection would jeopardize the investigation. Any other use of this exception is subject to approval by the Designated Minister in the manner outlined above.

.2.3 *Accuracy of personal information used for an administrative purpose*

Subsection 6(2) of the Privacy Act provides that a government institution shall take all reasonable steps to ensure that personal information that is used for an administrative purpose by the institution is as accurate, up-to-date and complete as possible.

The intent of this subsection of the Act is to minimize the possibility that a decision directly affecting an individual will be made on inaccurate, obsolete or incomplete information.

.2.4 *Retention and disposal of personal information*

.2.4.1 *Purpose* Article .2.4 is intended to assist in the interpretation of the provisions of subsections 6(1) and 6(3) of the Privacy Act and section 4 of the Privacy Regulations relating to the retention and disposal of personal information, and to set forth the requirements which institutions must carry out to give effect to these provisions.

The requirements are to be incorporated in records retention and disposal schedules to be developed by government institutions and approved by the Dominion Archivist. Personal information is to be retained and disposed of in accordance with these schedules. The process for scheduling records for retention and disposal and for retaining and disposing of records in accordance with schedules is described in policy contained in Chapter 460 - Records management and in Chapter 461 - Management of EDP data.

Subarticle .2.4.2 prescribes the framework within which the scheduling, retention and disposal of all personal information is to take place, while subarticle .2.4.3 elaborates one of the components of this framework applying to the retention of personal information used to make a decision directly affecting an individual after it is so used.

.2.4.2 *Framework for the scheduling, retention and disposal of personal information*. Subsection 6(3) of the Privacy Act provides that a government institution shall dispose of personal information in accordance with the regulations and in accordance with any directives or guidelines issued by the Designated Minister in relation to the disposal of such information.

The intent of this provision is to ensure, in planning and effecting the disposal of personal information, that institutions protect the interests of individual to whom the information relates as well as keeping in mind the usual considerations of value of the information to the institution, and its archival or historical value.

No regulations have been made under subsection 6(3) of the Act. Since the Act is explicit in providing that institutions shall dispose of personal information in accordance with any directives or guidelines issued by the Designated Minister, the directives set out below have the force of law.

Government institutions shall schedule personal information for retention and disposal in accordance with the following principles:

(a) where personal information was collected prior to the coming into force of the Privacy Act and is not relevant to an authorized operating program or activity of the institution (as described in subarticle .2.2.2), the information shall be disposed of;

(b) where further retention of personal information might unfairly prejudice the interests of the individual to whom the information relates, it shall be disposed of;

(c) where personal information has been used to make a decision directly affecting an individual, the information shall be retained for at least two years after the last time the information was so used unless the individual consents to its earlier disposal (see note following these directives for elaboration);

(d) where a request for access to personal information has been received, the information shall be retained until such time as the individual has had the opportunity to exercise all his or her rights under the Act;

(e) where an emergency exists at a Canadian post abroad, the head of the post, or the senior officer in charge, may order the destruction of personal information in order to prevent the removal of the information from the control of the institution; and

(f) subject to (a) through (e), when personal information is no longer required for the purpose for which it was obtained or compiled by the institution, the information shall be disposed of.

Schedules for retention and disposal of personal information shall also indicate the manner of disposal, as follows:

(a) where personal information has been designated by the Dominion Archivist as having archival or historical value, the information shall be transferred to the control of the Public Archives; and

(b) where personal information has not been so designated, it shall be destroyed.

Government institutions shall retain and dispose of personal information in accordance with schedules incorporating all the requirements of the preceding two directives following the approval of such schedules by the Dominion Archivist.

Note: Requirement (c) in the first of the preceding directives needs some elaboration.

First, as mentioned, an individual may consent to the disposal of personal information used to make a decision directly affecting him or her prior to the passage of two years since the last time the information was so used. This could occur where the individual demonstrates, on requesting and receiving access to information, that the information is incorrect, and where the most appropriate means of correction is disposal. It could also apply if, before the expiry of the two-year period, the information is no longer required for the purpose for which it was obtained or compiled by the institution, as reflected in the appropriate records retention and disposal schedule, and the individual's agreement to disposal is secured. Consent of the individual must be obtained in writing.

Second, it should be noted that where personal information used for an administrative purpose is contained in personnel records of former employees of government institutions or of former members of the Canadian Armed Forces, the information is to be retained by the institution(s) concerned for one year after termination of employment, and then is to be transferred to the control of the Public Archives for the second year of this minimum two-year retention period.

Third, prior to disposing of personal information that has been used to make a decision affecting an individual, institutions must verify that the information has not been so used during the preceding two years. Verification may be done by a careful examination of all documentation due for disposal, and consultation, where any doubt exists, with officials who may have used the information concerned for an administrative purpose.

.2.4.3 *Minimum two year retention* Subsection 6(1) of the Privacy Act provices that personal information that has been used by a government institution for an administrative purpose shall be retained by the institution for such period of time after it is so used as may be prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the information.

Section 4 of the Privacy Regulations (see Appendix B) establishes this period as a minimum of two years unless the individual consents to earlier disposal. The section also requires that, where a request for access has been received, the information must be retained until such time as the individual has had the opportunity to exercise all his or her rights under the Act. Notwithstanding these provisions, the head of a Canadian post abroad, or the senior officer in charge, may order the destruction of the information in an emergency in order to prevent the removal of the information from the control of the institution.

.2.4.4 *Additional provisions* In addition to the provisions contained in article .2.4, the following provisions elsewhere in this Part of the Chapter affect the retention and disposal of personal information:

- institutions must, in accordance with subsection 9(1) of the Privacy Act, retain a record of any use of personal information contained in a personal information bank or any purpose for which such information is disclosed where the use or purpose is not included in the statements of uses and purposes set forth in the Privacy Index, and must attach the record of use or disclosure to the personal information (see article .4.5); and
- a request for disclosure and a record of any information disclosed pursuant to such a request under paragraph 8(2)(e) of the Privacy Act shall be retained for a period of at least two years following the date on which the request was received by the institution (see section 7 of the Regulations in Appendix B and subarticle .3.7.5).

Part III

.3 Use and disclosure of personal information

.3.1 *General principles*

Sections 7 and 8 of the Privacy Act constitute a code governing the use and disclosure of all personal information under the control of government institutions.

Whereas Subsection 52(2) of Part IV of the Canadian Human Rights Act applied only to personal information collected from an individual and used in a decision-making process relating directly to that individual, sections 7 and 8 the Privacy Act apply to all personal information controlled by government institutions, that is not publicly available, regardless of its source or nature. The legislation has been developed in recognition of the principle that the right of the individual to privacy includes the right to control the use and disclosure of information about him or herself and, when exceptions to this principle exist, to know what use can be made of the information and to whom and for what purposes the information may be disclosed.

Three important factors must be kept in mind when interpreting the use and disclosure code in sections 7 and 8:

(a) the code does not take precedence over specific statutory prohibitions regulating the use and disclosure of personal information (e.g. section 241 of the Income Tax Act) but only applies where no other such statutory provisions exist;

(b) the code only permits the use and disclosure of personal information for the purposes specified in subsection 8(2) - it does not require them. Therefore, no right of access to such information is granted to third parties (i.e. another government institution, person, group of persons or organization) by this provision. Instead, it is left to the discretion of the government institution involved whether or not it will use or disclose the information for a permitted purpose; and

(c) it is government policy to balance the requirement for privacy with the need for government institutions to ensure the optimum use of personal information for any purpose permitted by the Privacy Act, in order to promote general efficiency in government operations, eliminate unnecessary collection of information, reduce the response burden on individuals and facilitate the sharing of data for research or statistical purposes.

.3.2 *Purpose*

The purpose of this section of Chapter 410 is to assist in the interpretation of the use and disclosure provisions of the Privacy Act and to set out directives and guidelines which are to be applied by government institutions as a matter of government policy. Together, the statutory provisions and the policies based on them provide a framework to aid government institutions in making decisions relating to the use and disclosure of personal information. Government institutions with significant holdings of such information should develop practices and procedures which complement these statutory provisions and policies and adapt them to the particular information under their control.

.3.3 *Use of personal information*

Section 7 of the Privacy Act sets out the general rule for the use of personal information under the control of a government institution. Such information shall not, without the consent of the individual to whom it relates, be used by an institution except:

(a) for the purpose(s) for which it was obtained or compiled by the institution;

(b) for a use consistent with the purpose(s) for which it was obtained or compiled; or

(c) for a purpose for which personal information may be disclosed under subsection 8(2).

Use refers to the employing of personal information within a government institution to accomplish certain purposes. An institution is limited in how it uses such information to the purpose(s) for which it obtained or compiled the information; uses consistent with that purpose (see article .3.6 below) and to purposes for which information may be disclosed under subsection 8(2). This latter provision incorporates into the uses allowed by the Privacy Act those permissible disclosures outlined in subsection 8(2) (see article .3.7 below) and enables institutions to undertake such disclosures. In other words, it enables an institution which controls personal information to use that information for any purpose for which it could disclose it to another institution or third party. Any other uses of personal information can only occur with the consent of the individual to whom the information relates (see article .3.5 below). The consistent uses provided for here are subject to the limitations outlined in articles .3.6 and .4.6.

.3.4 *Disclosure of personal information*

Subsection 8(1) of the Privacy Act sets out the general rule governing the disclosure of personal information by government institutions. Disclosure refers to the release of personal information, by any method whatever (e.g. physically transmitting the information or allowing it to be examined), to any person or body, inside or outside of a government institution which has control of the information, not specifically authorized under any other Act or regulation to obtain access to the information. *Disclosure of personal information by a government institution is only allowed either with the consent of the individual to whom the information relates or in accordance with one of the categories of permitted disclosures to third parties outlined in subsection 8(2) of the Act.* Any disclosure of personal information to which these conditions do not apply is an unauthorized disclosure of such information.

.3.5 *Process for obtaining consent*

Consent by an individual to the use or disclosure of personal information for purposes beyond those permitted under sections 7 and 8 of the Privacy Act, may be sought either at the time of collection of the information or subsequently, when a specific need arises.

.3.5.1 *Consent at time of collection*

When consent is sought at the time of collection of the information, institutions must give each individual the opportunity to indicate informed consent or refusal for such use or disclosure. Documents used to collect personal information which will be used or disclosed for purposes other than those permitted under sections 7 and 8, must include:

(a) a description of the specific type(s) of information involved;

(b) a description of the nature of the use or disclosure for which consent is sought;

(c) a statement that refusal to consent to such use or disclosure will not prejudice the individual in any way or result in any adverse consequences for the individual in connection with the particular primary administrative purpose(s) being served by collection; and

(d) a consent/refusal statement with space for the signature of the individual or authorized representative and the date.

All uses or disclosures for which consent is sought at the time of collection of personal information must be included in the relevant personal information bank description published in the Privacy Index.

.3.5.2 *Consent subsequent to collection*

When consent is sought for any use or disclosure subsequent to collection of personal information, an institution shall employ a form which meets the minimal requirements contained in Appendix C. Individuals may, however, indicate their consent by personal written authorization. In all cases a government institution shall consider consent to be given only:

(a) on receipt of a signed consent form indicating the agreement of the individual or his or her authorized representative (for authorized representative see sub-articles .3.5.3, .3.5.4, .3.5.5, and .3.5.6) to the use or disclosure; or

(b) on receipt of a written authorization from the individual or his or her representative (see sub-articles .3.5.3, .3.5.4, .3.5.5, and .3.5.6) authorizing that the information be used or disclosed in a specified manner.

Sometimes consent for a use or disclosure is requested subsequent to collection of the information to facilitate the processing of an application or claim from an individual. Refusal to agree to that use or disclosure may mean that the application or claim concerned cannot be considered because of lack of information essential to making a decision. In such circumstances, the need for the information must be clearly explained to the individual in writing and he or she given the opportunity to supply the information, where this is appropriate.

When an individual fails to indicate whether or not he or she consents to a particular use or disclosure, an institution shall consider this a refusal of consent. In some cases, however, where, in the opinion of the head of an institution, there is an overriding public interest, the information may be considered for disclosure under one of the categories of permissible disclosures in sub-section 8(2), such as paragraph 8(2)(m) (see article .3.7.13).

.3.5.3 *Consent by minors*

Section 10 of the Privacy Regulations (see Appendix B) provides that rights or actions under the Privacy Act and its regulations, including the giving of consent, may be exercised on behalf of minors by a person authorized by or pursuant to the law of Canada or a province to manage the affairs of minor.

This regulation does not prevent consent being obtained from individuals under the age of majority when such individuals have the ability to understand the subject matter in respect of which consent is requested and are able to appreciate the consequences of giving or withholding consent. When this is the case, consent should be sought from the minor. However, in situations where, in the opinion of the institution, there is a reasonable uncertainty that these conditions apply, the institution should, when the individual is age sixteen or younger, obtain consent from the parent or guardian who has legal custody of the minor. While the age of majority varies from province to province, age sixteen is chosen in this instance as being an age when minors could reasonably be expected to be capable of giving consent.

.3.5.4 *Consent by incompetents*

Section 10 of the Privacy Regulations (see Appendix B) provides that rights or actions under the Privacy Act and its regulations, including the giving of consent, may be exercised on behalf of incompetent individuals (i.e. individuals incapable of managing their own affairs) by a person authorized by or pursuant to the law of Canada or a province to manage the affairs of that person.

.3.5.5 *Consent in respect to deceased individuals*

Section 10 of the Privacy Regulations (see Appendix B) provides that rights or actions under the Privacy Act and its regulations, including the giving of consent, may be exercised on behalf

of deceased persons by a person authorized by or pursuant to the law of Canada or a province to manage the affairs of the deceased, but only for the purposes of such administration.

The Privacy Act applies to personal information relating to individuals who have been dead less than twenty years. When consent is required for the use or disclosure of information pertaining to such individuals for purposes of administering his or her estate, it should, whenever feasible, be obtained from the executor or administrator of the individual's estate. Where this is not possible, the head of a government institution having control of the record may wish to exercise his or her discretion under the permissible disclosure provisions of subsection 8(2). In such situations paragraph 8(2)(m), disclosure where the public interest clearly outweighs invasion of privacy or disclosure would clearly benefit the individual, may become the most appropriate provision for determining whether or not the information will be used or disclosed (see sub-article .3.7.13).

.3.5.6 *Consent by representative of an individual*

Section 10 of the Privacy Regulations (see Appendix B) provides that the rights or actions under the Privacy Act or its regulations, including the giving of consent, may be exercised on behalf of any individual, other than a minor, incompetent or deceased person (see sub-articles .3.5.3 to .3.5.5 above), by any person authorized in writing by the individual to whom the information pertains.

This provision allows representatives such as lawyers to act on behalf of individuals in the giving of consent. *In all such situations, government institutions shall ask the representative to produce written authorization signed by the individual to whom the information pertains empowering the representative to act on his or her behalf in such matters.* In the case of lawyers, such authorization may be comprised of authorization in writing by an individual empowering the lawyer to act in all matters involving the individual. The 'Appointment of Representative Form' included in Appendix C may be used to aid in

fulfilling the requirements of this article but its use is not mandatory and authorization by signed letter is equally acceptable as use of the form.

.3.6 *Consistent use*

Sections 7 and 8 of the Privacy Act provide that personal information may be used or disclosed by a government institution, without the consent of the individual to whom it relates, for a purpose directly related to the purpose(s) for which the information was obtained or compiled. Such related purposes are termed consistent uses. For a use or disclosure to be consistent it must have a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled.

A number of examples below offer guidance to institutions in determining when a use or disclosure of personal information may be considered consistent. These are as follows:

(a) use of such information in the development or expansion of a government program or activity directly related to the original purpose for obtaining or compiling the information. (For example, if an institution is expanding a benefit program to cover a clientele with the same individuals as that of the original program, then personal information used in the original program may be used in the expanded one without obtaining the consent of each individual affected);

(b) uses of such information which form part of an evaluation or statistical reporting process for an existing program or to provide analytical data for the development of new programs or activities related to the purpose(s) for which the information was originally obtained or compiled;

(c) the disclosure of personal information by Correctional Services to the National Parole Board where the latter is considering the release of an inmate from custody and needs such information to assist in making the decision;

(d) the disclosure of information to an investigative body for the purpose of detemining whether an offence has been committed in connection with the Act under which the information was provided. By way of example:

- disclosure of an application filed under the Family Allowance Act for the purpose of determining whether of an offence under that Act has been committed; or
- disclosure of an application filed for a passport in order to determine whether a false declaration has been made which could lead to a prosecution for fraud under the Criminal Code; and

(e) the disclosure of information which has been customarily released into the public domain through the media. An example is the disclosure of the names of accident victims after next of kin have been notified or the names of persons charged with an offence by an investigative body.

Requirement to account for consistent uses

To enable the Designated Minister to fulfill the requirements of section 11 of the Privacy Act respecting publication of the Privacy Index, each government institution must include, in its descriptions of its personal information banks, statements of all consistent uses for which information in any bank is used or disclosed (see article .4.3). Subsection 9(3) of the Act (see article .4.6) provides for notification of the Privacy Commissioner and amendment of the personal information bank description when institutions use or disclose personal information in a manner which, while consistent with the purposes for which it was obtained or compiled, could not be anticipated and is, therefore, not reflected in the Privacy Index.

.3.7 *Permissible disclosures of personal information*

Subsection 8(2) of the Privacy Act sets out circumstances under which personal information under the control of a government institution may be disclosed to third parties (i.e. to another government

institution, person, group of persons or organization) in certain circumstances without obtaining the consent of the individual to whom the information relates.

It is emphasized, however, that subsection 8(2) only permits disclosure of personal information to third parties. It does not create a general right of access for third parties to personal information. Therefore, it is not mandatory for an institution to release personal information requested by a third party under any one of the thirteen categories of subsection 8(2) even when it is the subject of a request under the Access to Information Act. Personal information should be disclosed by a government institution only after it has carefully balanced the arguments favouring disclosure against the potential threat to an individual's privacy posed by the disclosure. Such disclosures should be governed by the interpretations and policies elaborated in this section and the detailed institutional practices and procedures referred to in article .3.2 of this Part.

It should be noted that in stating that the provision is 'subject to any other Act of Parliament', subsection 8(2) clarifies that specific statutory prohibitions against the disclosure of personal information take precedence over the discretionary disclosures permitted under subsection 8(2). Thus, specific prohibitions against disclosure in such statutes as the Income Tax Act and the Statistics Act are unaffected by this provision.

Each paragraph of subsection 8(2) is interpreted separately. The government policies which complement and assist in the interpretation of each paragraph then follow.

.3.7.1 *Original purpose and consistent use*

Paragraph 8(2)(a) of the Privacy Act provides that personal information under the control of a government institution may be disclosed to a third party for the purpose for which the information was obtained or compiled by the government institution or for a use consistent with that purpose.

This paragraph gives government institutions the discretion to disclose personal information to another government institution, person, group of persons or organization if to do so is necessary to accomplishing the purpose for which the information was obtained or compiled or for a use consistent with it. The consistent uses provided for here are subject to the limitations outlined in articles .3.6, .4.3 and .4.6.

.3.7.2 *Act of Parliament or regulation*

Paragraph 8(2)(b) of the Privacy Act provides that personal information under the control of a government institution may be disclosed to a third party for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure.

In effect, this paragraph incorporates all other authorizations regarding the disclosure of personal information in federal statutes and regulations.

Such authorizations are sometimes specific and sometimes broad in nature. The Canada Elections Act, which authorizes the posting of electors' names and addresses for the general public to inspect, is an example of a specific authorization. On the other hand, the Unemployment Insurance Act, 1971, which authorizes disclosure of information as the Minister deems advisable, is an example of legislation which gives a broad authorization.

Where the statutory authority is broad and personal information has been released thereunder, an appropriate entry shall be made in the Privacy Index that includes:

(a) the statutory authority and regulation (where applicable) governing disclosure;

(b) the type of information disclosed;

(c) the purpose of the disclosure;

(d) the third party receiving the information; and

(e) any conditions respecting use of the information.

Departments are directed that when developing legislation and regulations which deal with the disclosure of personal information, consultation with the Information Law and Privacy Section, Department of Justice must take place prior to submission of the appropriate documentation for approval by the Governor-in-Council or, where applicable, prior to the approval of ministerial regulations.

.3.7.3 *Subpoenas, warrants, court orders and rules of court*

Paragraph 8(2)(c) of the Privacy Act provides that personal information under the control of a government institution may be disclosed for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information. The person or body other than a court may include quasi-judicial bodies and commissions of inquiry.

Normally, government institutions will wish to comply with a subpoena or warrant. There are instances, however, when this will not be the case and, indeed, where it would not be proper to disclose the particular personal information involved. (Government institutions should, when a subpoena or warrant is received, consult with their legal advisor to ensure the validity of the subpoena or warrant and to determine the proper form of compliance.) When responding to a subpoena, it is sufficient for the government institution to produce certified copies of the records required, unless the subpoena stipulates otherwise. When these copies do not become part of the court's records, the government institution should request their return, either for proper disposal or reintegration into its filing system.

.3.7.4 *Attorney General for use in legal proceedings*

Paragraph 8(2)(d) of the Privacy Act provides that personal information under the control of a government institution may be disclosed to the Attorney General of Canada for use in legal proceedings involving the Crown in right of Canada or the Government of Canada.

This provision covers those situations where personal information is required by the Attorney General to conduct a case before the courts or a quasi-judicial body in which the Government of Canada or the Crown in right of Canada is a party.

.3.7.5 *Federal investigative bodies*

Paragraph 8(2)(e) of the Privacy Act provides that personal information under the control of a government institution may be disclosed to an investigative body specified in regulations (see section 5, Privacy Regulations, Appendix B), on the written request of the body, for the purpose of enforcing any law of Canada or any province or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be disclosed.

This is a permissive provision which does not grant federal investigative bodies any right of access to personal information. Rather, the provision leaves to the discretion of the government institution involved the ultimate decision whether or not to disclose personal information to such investigative bodies. Disclosure under this provision is permissible only to those limited number of federal investigative bodies named in regulations.

Disclosure to federal investigative bodies is strictly regulated. Personal information should be disclosed only to aid a specific enforcement or investigative activity and never in response to a vague and indeterminate inquiry. Under the terms of paragraph 8(2)(e) personal information can only be provided to federal investigative bodies pursuant to a written request, which specifies the information being requested and the reason why disclosure is requested. Requests by such bodies may be made either by letter or on the Request for Disclosure to Federal Investigative Bodies Form (see Appendix C). In either case the request must contain:

(a) the name of the individual to whom the information relates;

(b) the date of the request;

(c) a description of the information requested;

(d) a statement of the specific purpose to be served by the disclosure of the particular personal information;

(e) the name of the federal investigative body and the name, title and signature of the officer making the request; and

(f) space for the name, title and signature of the official charged with making the disclosure and the date of disclosure.

When the request is signed and dated by an official of the government institution that has control of the information, it becomes a record of disclosure.

Because of the potential impact of this type of disclosure on personal privacy, *only the most senior officials in each institution shall have the authority to approve the disclosure of personal information to federal investigative bodies. Government institutions shall provide annually to the designated Minister a list, by title, of those officials authorized to approve such disclosures. Further, institutions undertaking disclosures of personal information to federal investigative bodies shall develop internal directives governing such disclosures*.

These internal directives must either replace or incorporate all present agreements relating to the disclosure of personal information to investigative bodies. They should distinguish among the various types of personal information under the control of an institution (e.g. between non-sensitive biographical data and more sensitive information such as medical files), incorporate the principles of all present agreements which remain applicable, establish guidelines governing when and under what conditions personal information may be disclosed to

federal investigative bodies and ensure full accountability of the supplying institution for such disclosures. In distinguishing among various types of personal information, special attention should be paid to identifying information which was obtained or compiled for research or statistical purposes (e.g. standing statistical data banks) or with the clear understanding that no such disclosure of the information would be made. (Institutions should disclose this type of personal information only in the most exceptional circumstances where the need for disclosure clearly outweighs the undertaking of confidentiality.)

Retention of requests for disclosure and records of disclosure

Subsection 8(4) of the Privacy Act provides that the head of a government institution shall retain a copy of every request received by the government institution under paragraph 8(2)(e) for such period of time as may be prescribed by regulation, shall keep a record of any information disclosed pursuant to the request for such period of time as may be prescribed by regulation and shall, on the request of the Privacy Commissioner, make such copies and records available to the Privacy Commissioner.

Section 7 of the Privacy Regulations (see Appendix B) stipulates that a copy of all requests for disclosure to federal investigative bodies and all records of disclosure made in consequence of such requests must be kept for a minimum of two years.

These provisions establish a monitoring system for the Privacy Commissioner in regard to the disclosure of personal information to law enforcement bodies. Access to this information will allow the Commissioner to review such disclosures of personal information, investigate complaints by individuals and report on any abuse of this disclosure provision. *Copies of all requests for disclosure from and all personal information disclosed to law enforcement bodies shall be maintained in a unique personal information bank set up for this purpose*. Individuals may request access to information about themselves in such banks, but much of the information contained in them will qualify for exemption from such access under section 22 of the Privacy Act.

*In order to ensure that no law enforcement or investigative activity is compromised by the disclosure of such requests and information, the institution which has control of this type of information shall:

- clearly mark all personal information in the bank with a notification that a section 22 exemption under the Act may apply to it;
- consult with the investigative body which requested disclosure of the information before making a determination to exempt or diclose it in response to a request; and
- when responding to any such access requests under section 16 of the Act in any way, except to grant access to the information, employ Model Letter H contained in Appendix D.

These provisions should be read in conjunction with section 9 of the Privacy Act (see article .4.5) which requires retention of a record of any use or disclosure of personal information not accounted for in the Privacy Index and attachment of that record to the particular personal information used or disclosed.

.3.7.6 *Provinces, foreign states and international bodies*

Paragraph 8(2)(f) of the Privacy Act provides that personal information under the control of a government institution may be disclosed under an agreement or arrangement between the Government of Canada or an institution thereof and the government of a province; the government of a foreign state; an international organization of states or an international organization established by the governments of states; or any institution of any such government or organization, for the purpose of administering or enforcing any law or carrying out a lawful investigation.

This provision recognizes existing practices under which personal information is exchanged between federal police, security and other investigative bodies and their counterparts both domestically and internationally. Such disclosures aid the effective carrying out of law enforcement and investigative activities and are necessary to maintaining the flow of information to federal law enforcement agencies. The

paragraph also permits federal government institutions to provide information to provincial and foreign governments and international organizations for the purpose of administering a statute, as well as, enforcing one. Examples of this type of disclosure include the federal-provincial exchange of information related to social assistance and the international exchange of information required to administer veterans' benefits.

Disclosures under this provision are to take place in accordance with an agreement or arrangement. Many such agreements or arrangements have existed in the past. They have ranged in nature, however, from formal signed documents to oral commitments. Some formalization of existing procedures is now required. It is recommended that personal information should only be disclosed by the Government of Canada or a federal government institution to the governments of provinces, foreign states or international organizations in accordance with agreements signed by an appropriate government official. Such agreements should place the receiving government, organization or institution under an obligation not to use or disclose the personal information which is being transferred for any other purpose(s) than those stipulated in the agreement except with the written consent of the federal institution disclosing the information. *In order to ensure consistency of approach among federal government institutions, the terms of disclosure agreements shall meet the minimum requirements listed in document 5 in Appendix C.*

Written agreements are sometimes unacceptable to some foreign governments and international organizations when the exchange of information involves law enforcement, intelligence and security matters. This relatively limited area of activities should form the only exception to the general rule of disclosing personal information to other governments and international organizations by formal agreement. Therefore, when written agreements are unacceptable to a foreign government or international organization, and when the exchange of information is essential to law enforcement, intelligence and security activities, government institutions may disclose personal information under an informal arrangement.

All federal government institutions involved in the disclosure of personal information by agreement or arrangement shall indicate in the appropriate entries in the Privacy Index the various types of agencies with which the particular information in the entry is shared (e.g. provincial social assistance agencies, international law enforcement agencies etc.)

All institutions involved in disclosures of personal information to provincial and foreign governments or international organizations must, in accordance with subsection 9(1) and (2), make provision for the filing and retention of a copy of all records pertaining to any disclosure made under such agreements or arrangements which are not included in the appropriate statements in the Privacy Index (see article .4.5).

.3.7.7 *Members of Parliament*

Paragraph 8(2)(g) of the Privacy Act provides that personal information under the control of a government institution may be disclosed to a member of Parliament for the purpose of assisting the individual to whom the information relates in resolving a problem.

The term member of Parliament includes both members of the House of Commons and the Senate. This provision has been included to remove, in most instances, the necessity of a member having to prove to the satisfaction of a government institution that a person has asked for assistance. This could be difficult to do, for example, when the assistance of a member is in response to an oral request. In cases where the individual is incapable of requesting the member's assistance directly himself or herself, the request to a member may be made by an agent of the individual, who has been authorized to act on behalf of the individual.

In a limited number of instances, however, when the personal information is of an extremely sensitive nature (e.g. a medical record or immigration case record), the institution may ask the member to submit a formal request for the information in writing. Under similar circumstances, where the member is acting on behalf of an agent of an

individual, an institution may seek the member's assistance in obtaining proof that the agent is authorized to act on behalf of the individual in such matters.

Where information which may not be available to an individual under the exemptions of the Act is involved, the government institution may disclose more information in confidence to the member than would be available to the individual concerned if he or she made an application for access under subsection 12(1). Such disclosure may be made to assist the member in better understanding the circumstances concerning the individual and his or her problem. In such situations, the member must first agree not to disclose the information involved to the individual without the permission of the head of the government institution which controls the information.

.3.7.8 *Audit purposes*

Paragraph 8(2)(h) of the Privacy Act provides that personal information under the control of a government institution may be disclosed to officers or employees of the institution for internal audit purposes, or to the Office of the Comptroller General or any other person or body specified in regulations for audit purposes.

No persons or bodies were identified for inclusion in the Privacy Regulations. The Auditor General of Canada is not mentioned in this paragraph because disclosure to the Auditor General or a member of his or her office is specifically authorized under the Auditor General Act. Therefore, disclosure is permitted under paragraph 8(2)(b).

Audit purposes include the conducting of an independent review and appraisal of the management practices and controls and of the financial accountability of particular operations and programs. *Personal information disclosed pursuant to this provision shall be used only for audit purposes and not as part of any decision-making process concerning the individual to whom the information relates*.

.3.7.9 *Archival purposes*

Paragraph 8(2)(i) of the Privacy Act provides that personal information under the control of a government institution may be disclosed to the Public Archives of Canada for archival purposes.

Disclosure for archival purposes includes not only the actual transfer of personal information to the control of the Public Archives for archival and historical purposes, but also the examination by staff of the Public Archives of personal information within government institutions in order to determine whether or not that information qualifies as an archival record and to establish appropriate retention and disposal standards for that information.

Further disclosures of personal information by the Public Archives is provided for in subsection 8(3) of the Privacy Act. Refer to article .3.8 below.

.3.7.10 Research or statistical purposes

Paragraph 8(2)(j) of the Privacy Act provides that personal information under the control of a government institution may be disclosed to any person or body for research or statistical purposes provided that the head of the government institution:

> (a) is satisfied that the purpose for which the information is disclosed cannot reasonably be accomplished unless the information is provided in a form that would identify the individuals to whom it relates; and
>
> (b) obtains from the person or body a written undertaking that no subsequent disclosure of the information will be made in a form that could reasonably be expected to identify the individual to whom it relates.

The Research Application and Undertaking Form is discussed in Appendix C. Its purpose is to provide an avenue for continued research and statistical analysis involving personal data, especially in medicine

and the social sciences, while making researchers, statisticians and research or statistical bodies formally accountable for the protection of individual privacy when they are allowed access to such information.

When contemplating the use of this disclosure provision for older information, reference should also be made to subsection 8(3) of the Privacy Act (see article .3.8 below). This relates to disclosure by the Public Archives, under certain conditions, of personal information collected by it for historical and archival purposes for research or statistical purposes.

If a researcher or statistician, to whom information has been provided, wishes to release it in a personally identifiable form, he or she must obtain either the consent of the individual to whom the information relates or the permission of the head of the government institution controlling the information. In the latter instance, permission to disclose the information may be given on the basis of a public interest statement as provided sub-paragraph 8(2)(m)(i) (see sub-article .3.7.13 below).

When an institution discovers that personal information is being disclosed by a person or body through publication or any other method in contravention of a written undertaking, it shall immediately take steps to withdraw research privileges from that person or body and the institution's legal advisor shall be consulted in order to determine the proper steps to be taken to prevent further disclosure of the personal information concerned.

(In exercising discretion to disclose personal information under the research or statistical purposes provision, government institutions should take into account the sensitivity of the information involved and other factors set out in the invasion-of-privacy test included in sub-article .3.7.13.).

.3.7.11 *Native claims research*

Paragraph 8(2)(k) provides that personal information under the control of a government institution may be disclosed to any association of aboriginal people, Indian band, government institution or part

thereof, or to any person acting on behalf of any of these groups, for the purpose of researching or validating the claims, disputes or grievances of any of the aboriginal peoples of Canada.

This provision permits disclosure of personal information to researchers involved in the process of settling native claims. The term 'aboriginal people' is intended to have the same meaning as in the Canadian Charter of Rights. Such information is primarily contained in the records of the Department of Indian Affairs and Northern Development but is also found in other government institutions. Personal information may be disclosed to an individual acting on behalf of an association of aboriginal people, Indian band or government institution upon presentation of a letter by that individual from any such group accrediting him or her as undertaking work involved with researching or validating native claims on its behalf. Individuals accredited to undertake such research or validation but not employed by a government institution must also fill out the Research Application and Undertaking Form provided for in sub-article .3.7.10.

(In exercising discretion to disclose personal information under the native claim research provision, government institutions should take into account the sensitivity of the information involved and other factors set out in the invasion-of-privacy test included in sub-article .3.7.13.).

.3.7.12 *Payment of a benefit and collection of a debt*

Paragraph 8(2)(l) of the Privacy Act provides that personal information under the control of a government institution may be disclosed to any government institution for the purpose of locating an individual in order to collect a debt owing to Her Majesty in right of Canada by that individual or make a payment owing to that individual by Her Majesty in right of Canada.

This provision is included to facilitate the task of locating individuals for the purpose of Crown debts and paying money owing to individuals. Government institutions should release appropriate information to other institutions for the purpose of locating individuals

owing Crown debts, unless specifically prohibited from doing so. However, the provision does not permit the disclosure of information for the purpose of investigating the possibility that a Crown debt is owed. In the case of benefits due an individual the intention is to expedite the location of individuals entitled to income tax refunds or other government cheques. *For personal information to be disclosed for these reasons, the government institution requesting the information shall clearly specify the debt or benefit to the government institution which controls the information. On the other hand, the disclosing institution shall disclose only that personal information which can be useful in locating an individual*.

It should be noted that this provision does not override specific statutory prohibitions against the release of the information, such as are contained in the Income Tax Act.

.3.7.13 Public interest

Paragraph 8(2)(m) of the Privacy Act provides that personal information under the control of a government institution may be disclosed for any purpose where, in the opinion of the head of an institution, (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or (ii) disclosure would clearly benefit the individual to whom the information relates.

Sub-paragraph 8(2)(m)(i)

This provision is designed to deal with disclosure of personal information in situations which either cannot be readily foreseen or which are so specialized that they cannot be suitably covered in specific terms elsewhere in subsection 8(2) of the Privacy Act. It is emphasized that the provision does not imply any right of access to personal information by other government institutions or third parties. Rather, the provision only permits disclosure by the institution where, in the discretion of the head of that institution, the appropriate conditions, as set out in this policy, are met. Further, the provision is only a

supplement to and not a replacement for paragraphs (a) to (l) of subsection 8(2). In any case, it must be used by institutions with a good deal of restraint. *Information shall be disclosed under this provision only when it is apparent that there is a clear public interest in disclosure but no other release category under subsection 8(2) is applicable.*

Subsection 8(5) requires that the Privacy Commissioner be informed of disclosures made under this provision. The Privacy Commissioner may, subject to the admonition not to disclose information for which an exemption has been claimed, then, decide to inform or consult the individual concerned, or to initiate a complaint under subsections 29(1) and 29(3) or an investigation under section 37 of the Act.

In deciding whether or not to disclose information under this provision the head of an institution must balance the public interest in disclosure against the threat to an individual's privacy. This balancing must be based on a invasion-of-privacy test which weighs the expectations of the individual, the nature of the particular personal information involved and the possible consequences of disclosure for the individual against the public interest in disclosure, whether this is assessed in terms of the benefit to only a small number of people or to the public as a whole. There is no easy guide by which to determine whether or not a specific disclosure is in the public interest, especially since the criteria must cover unique, one-time cases, as well as what are termed 'class' disclosures (i.e. similar, regularly recurring and routine releases affecting a large number of individuals). There are obvious emergency situations where the circumstances are urgent and unambiguous, the public interest in disclosure is clear and the threat to privacy is very slight. There are situations, too, where, either because of the type of information involved or the passage of time, there is little, if any, threat to an individual's privacy. In most situations, however, the public interest in disclosure is less immediately apparent and a invasion-of-privacy test more crucial in deciding exactly which types of information may be released.

Basis of invasion-of-privacy test

There are three interrelated factors which must be taken into account in any invasion-of-privacy test. These are as follows.

(a) Expectations of the individual The conditions which governed the collection of the personal information and the expectations of the individual to whom it relates are important criteria in any test. Was the information compiled or obtained under guarantees which preclude some or all types of disclosures? Or, on the other hand, can the information be considered to have been unsolicited or given freely or voluntarily with little expectation of being maintained in total confidence? Has the individual himself or herself made a version of the information generally available to the public and thus waived the right to privacy in these circumstances?

(b) Sensitivity of the information It must be determined what type of information is involved in the request for a public interest disclosure. Is it of a highly sensitive personal nature or is it fairly innocuous information? Is the information very current and for that reason more sensitive or confidential, or has the passage of time reduced that sensitivity or confidentiality so that disclosure under specific circumstances would lead to no measurable injury to the individual's privacy?

(c) Probability of injury If the information is considered sensitive, can it be surmised that the particular disclosure carries with it the probability of causing measurable injury? Injury is to be interpreted as any harm or embarrassment which will have direct negative effects on an individual's career, reputation, financial position, safety, health or well-being. As well, a head of an institution must consider if a disclosure of personal information will make that information available for a decision-making process by a government institution beyond that for which it is being disclosed.

Institutions may also have other factors unique to their own situations which should also be added to a invasion-of-privacy test. These should be addressed in institutional guidelines drawn up in consultation with the Designated Minister. Arrangements for informing the Privacy Commissioner of 'class' public interest disclosures as well as particular disclosures should be made in consultation with the Privacy Commissioner.

Examples of situations in which there could be a public interest which outweighs the potential invasion of privacy in disclosure as outlined in paragraph 8(2)(m)(i) include:

(a) health or medical emergencies, accidents, natural disasters or hostile or terrorist acts where one or more individual's lives and well-being depend on disclosure;

(b) disclosure of information to carry out an order of the court (e.g enforcement of a custody order); and

(c) disclosure of information by an institution when it considers it in the public interest to release information relating to an individual either to substantiate a public statement by that individual or to correct such a statement. In these circumstances the individual involved must first have stated publicly much of the information being substantiated or corrected (e.g. a dispute over a social benefits claim).

Application to individuals who are deceased

Sub-paragraph 8(2)(m)(i) should be considered when disclosure of information relating to an individual dead less than twenty years is requested and administrative problems arise making it unfeasible to obtain consent from the executor or administrator of the individual's estate (see article .3.5). Very often there is a diminution of privacy concerns with the passage of time and such information can be disclosed. The head of an institution should weigh the sensitivity of the information

involved against the public interest in disclosure to determine if an unwarranted invasion of privacy would occur if the information was released. Important factors to consider when making a decision whether or not to disclose are whether:

(a) disclosure may cause definite financial injury to the immediate family of the deceased; or

(b) disclosure may endanger the physical well-being of the immediate family of the deceased; or

(c) the head of the institution has reason to believe that an immediate family member or ex-spouse does not want the information released;

(d) the information contains medical, psychological or social work case reports or data which it is reasonable to believe would prove harmful to familial relationships; or

(e) the deceased has expressed or implied any wishes with regard to the information.

Individuals failing to return a consent form

As stated in article .3.5.2, when an individual fails to indicate whether or not he or she consents to a particular use of disclosure, an institution shall consider this a refusal of consent. In some cases, however, where, in the opinion of the head of an institution, there is an overriding public interest or the administrative action would benefit the individual involved, the head of a government institution may consider the disclosure of personal information under the appropriate sub-paragraph in 8(2)(m). Such disclosures must only be undertaken in accordance with the requirements for public interest disclosures provided for in the Privacy Act, including notification of the Privacy Commissioner.

Sub-paragraph 8(2)(m)(ii)

This provision gives a discretion to the head of a government institution to ensure that personal information is not withheld from disclosure where an individual could clearly benefit from its release. The test in such circumstances is satisfied if the individual considers the release of the information of benefit to him or herself. Some examples of situations where personal information may be released on ground of 'benefit to the individual' are:

(a) disclosure to a doctor or hospital of an individual's blood type in an emergency when a transfusion is needed;

(b) disclosure to an airline of information to locate passengers' next of kin where an accident has occurred or to locate passengers when, for example, they have been exposed to food poisoning on a flight;

(c) disclosure of information to assist in the determination whether an individual is entitled to an honour, gift or reward or to a promotion or other professional advancement;

(d) disclosure of information that would verify that an individual is the owner of stolen or lost property;

(e) notification of next of kin in case of an accident or disaster; and

(f) disclosure of information about an individual to immediate family members or an authorized representative of the individual such as a lawyer, under compassionate circumstances (e.g. whether or not an individual has been arrested).

Notification of Privacy Commissioner

Subsection 8(5) of the Privacy Act provides that the head of a government institution must notify the Privacy Commissioner of any disclosure of personal information under paragraph 8(2)(m) either prior to the disclosure or, if this is not practicable, at the time of disclosure. The Privacy Commissioner has discretion to notify the individual to whom the information relates of the disclosure if this official deems such notification to be appropriate.

The provision acts as a check upon unreasonable use of paragraph 8(2)(m). When notified of an intention to disclose, the Privacy Commissioner may decide to intervene and recommend against disclosure.

Notification of an individual by the Privacy Commissioner is, however, subject to the requirements of section 64 of the Privacy Act. This provision places the Privacy Commissioner under a duty not to disclose any information that is exempt under either the Access to Information Act or Privacy Act or any information which could confirm the existence of personal information where the head of a government institution, in refusing to disclose the information, has not indicated whether it exists.

Particular disclosure

When personal information is disclosed under the public interest and individual benefit provisions on a unique, one-time basis, the institution must include in its notification to the Privacy Commissioner:

(a) the name and last known address of the individual involved;

(b) a description of the information being disclosed;

(c) the purpose of the disclosure and a statement as to why the public interest overrides privacy in this particular instance; and

(d) the name and signature of the person authorizing disclosure.

Class disclosures

Class disclosures are releases of personal information which are relatively routine in nature and occur regularly. Such disclosures are entirely dependent on the Privacy Commissioner agreeing to the approach being used. Government institutions must contact the Privacy Commissioner and make arrangements for class disclosures which meet the requirements of that office. Information relating to all class disclosures must be included as part of the appropriate information bank description in the Privacy Index and also transmitted to the Office of the Privacy Commissioner for notification purposes. This information pertaining to the arrangement made between the government institution and the Privacy Commissioner shall consist of:

(a) a detailed description of the type(s) of information involved in the class description;

(b) the purpose of disclosure and a statement as to how the public interest or individual benefit overrides privacy in the class release; and

(c) the name and signature of the person authorizing the disclosure.

Particulars of each arrangement concerning a class disclosure which have been transmitted to and accepted by the Office of the Privacy Commissioner satisfy the requirement of the Act for the head of a government institution to notify the Privacy Commissioner in advance of any disclosure of personal information under paragraph 8(2)(m). To

enable the Privacy Commissioner to monitor this type of disclosure more effectively, each government institution shall, no later than the termination of each financial year, report to the Privacy Commissioner the total number of disclosures per month pursuant to each arrangement for a class disclosure that has been authorized.

.3.8 *Disclosure by the Public Archives*

Subsection 8(3) of the Privacy Act provides that, subject to any other Act of Parliament, personal information under the control of the Public Archives that has been transferred to the Public Archives by a government institution for archival or historical purposes may be disclosed in accordance with the regulations to any person or body for research or statistical purposes.

Section 6 of the Privacy Regulations sets out the conditions for disclosure of archival or historical personal information for research or statistical purposes. Such information may be disclosed for these purposes where:

(a) the information is of such a nature that disclosure would not constitute an unwarranted invasion of the privacy of the individual to whom the information pertains;

(b) the disclosure is in accordance with paragraphs 8(2)(j) or (k) of the Act;

(c) one hundred and ten years have elapsed following the birth of the individual to whom the information pertains; or

(d) in cases where the information was obtained through the taking of a census or survey, ninety-two years have elapsed following the taking of the census or survey containing the information.

This provision permits the disclosure of personal information in certain circumstances for research of an historical nature. It is similar to paragraph 8(2)(j), disclosure for research or statistical purposes, but this latter clause was thought too restrictive in regard to further disclosure of personal information to allow historical research to be conducted at the Public Archives. The Public Archives is, therefore, permitted to make personal information which it has collected for archival or historical purposes available for research or statistical purposes under the specific conditions set out in the Privacy Regulations. It should be noted that:

(a) sub-section 8(3) does not create a right of access for third parties to personal information collected by the Public Archives for archival or historical purposes. Rather, it permits that institution discretion to disclose such information under particular conditions to serve specific research or statistical purposes; and

(b) while paragraphs 8(2)(j) and (k) of the Privacy Act are mentioned specifically in section 6 of the Privacy Regulations as providing for permissive disclosures by the Public Archives, all other provisions in section 8 of the Privacy Act apply equally to the Public Archives and it is governed by the policies prescribed in this Section of Chapter 410.

The provision is subject to any other Act of Parliament. This means that where a federal statute forbids the disclosure of personal information (e.g. the Income Tax Act), it cannot be disclosed by the Public Archives. The regulation prescribing the circumstances under which personal information of an archival or historical nature may be disclosed, is based on the differentiation between information which would and would not constitute an unwarranted invasion of privacy to the individual to whom it pertains. By way of example, sensitive medical, personnel and law enforcement records could contain information the disclosure of which could pose an unwarranted invasion of privacy. On

the other hand, a letter from a citizen to an employee of a government institution discussing a public issue probably would not qualify as information posing an unwarranted invasion of privacy.

Since the Public Archives assumes control over the personal information transferred to it for historical or archival purposes, discretion to differentiate between those types of personal information which would and would not constitute an unwarranted invasion of privacy is given to the head of that institution. *However, as a matter of government policy, the Public Archives shall:

(a) set out detailed guidelines based on section 6 of the Privacy Regulations to govern how all such differentiations are made;

(b) make such guidelines publicly available; and

(c) limit delegation of authority to approve such differentiations to senior officials within the Public Archives*.

These guidelines should take into account the principles of the invasion-of-privacy test set out in sub-article .3.7.13.

Further, the Public Archives shall, at time of transfer, consult with each government institution transferring personal information to its control for archival or historical purposes in order to obtain its advice, based on the guidelines prepared by the Archives, as to which personal information would, if disclosed, constitute an unwarranted invasion of privacy. The final decision as to whether or not to disclose particular personal information for archival or historical purposes, of course, lies with the Public Archives but it should take into account recommendations from the transferring institution.

In order to provide a control mechanism over disclosures of personal information for research or statistical purposes, subsection 8(3) is subject to review of the Privacy Commissioner in accordance with subsection 37(1) of the Act.

This section should be read in conjunction with sub-article .3.7.10 dealing with paragraph 8(2)(j), research or statistical purposes, and sub-article .3.7.11 dealing with paragraph 8(2)(k), native claims research.

.3.9 *Information publicly available*

Subsection 69(2) of the Privacy Act provides that the use and disclosure code in sections 7 and 8 of the Act does not apply to personal information which is publicly available.

This provision applies to information which has been published in any form or which constitutes or is part of a public record obtainable from another source. An example of the latter would be copies of trial records relating to an individual which are available from the court office. In such cases, it would not be sensible, for instance, to require an institution to obtain records directly from the court if they are more readily obtainable from another institution. The provision is included to prevent absurd situations where a government institution would be refusing to disclose information to another institution or other third party which is already in the public domain.

Such personal information remains accessible, however, to the individual to whom it relates under the Privacy Act.

.3.10 *Addresses and mailing lists*

An individual's home address falls within the definition of personal information in paragraph 3(d) of the Privacy Act. As a general rule, therefore, it is not to be disclosed for mailing list purposes by a government institution. Exceptions are limited to the following situations:

(a) the compilation of mailing lists for distribution to specified government institutions or third parties is the purpose for which the addresses of individuals were collected and the individuals concerned have been so advised by the government institution;

(b) the individuals on the mailing list have consented by voluntarily providing their addresses to facilitate their receipt of information about certain subjects and events;

(c) the transmitting of information contained in mailing lists is authorized by an Act of Parliament or a regulation as provided for in paragraph 8(2)(b) of the Privacy Act; and

(d) in exceptional circumstances only, disclosure of this type of information may be justified under paragraph 8(2)(a), consistent use, or subparagraph 8(2)(m)(ii), individual benefit, or one of the other provisions of subsection 8(2).

Part III

.4 Accounting for use and disclosure of personal information

.4.1 *General principles*

The Use and Disclosure Code dealt with in section .3 is based on the principle that the right of an individual to privacy includes the right to control the use which is made of information about him or herself and, when exceptions to this principle exist, to know what use can be made of the information. Section 9, paragraph 11(1)(iv) and subsection 11(2) of the Privacy Act ensure that all uses and disclosures of personal information in personal information banks are recorded, accounted for and, where appropriate, described in the personal information index (Privacy Index) so that an individual can determine what specific uses and disclosures of particular personal information have occurred.

.4.2 *Purpose*

The purpose of this section of Chapter 410 is to assist in the interpretation of those provisions of the Privacy Act relating to the publishing of primary, consistent and regular uses of personal information in personal information banks, the retention of use and disclosure records and the accounting for consistent uses not previously published; and to set out directives and guidelines concerning these provisions which are to be applied as a matter of government policy. Together, the statutory provisions and the policies based on them provide a framework to aid government institutions in accounting for the use and disclosure of personal information.

.4.3 *Statement of purposes*

Paragraph 11(1)(iv) of the Privacy Act provides that the Designated Minister shall cause to be published on a periodic basis not less frequently than once each year, as part of the Privacy Index, a statement of the purposes for which personal information in the bank was obtained or compiled and a statement of the uses consistent with such purposes for which the information is used and disclosed.

This requirement to publish a statement of uses and a statement of consistent uses is the essential basis of accounting for use and disclosures which underlies the Use and Disclosure Code set out in sections 7 and 8. These statements identify primary and consistent uses for the purposes of permitting uses and disclosures under paragraph 7(a) (see article .3.3 above) and 8(2)(a) (see sub-article .3.7.1 above). As well, they provide individuals with a way of determining the uses and disclosures which are made of information concerning themselves. *In order to ensure the completeness of this notification process, government institutions are required to provide to the Designated Minister comprehensive statements of all purposes for which personal information in each bank under their control was obtained or compiled and similar statements of consistent uses for which information in each bank is used or disclosed as part of the personal information bank identification and description process required by section 11 of the Act and to update these statements annually.*

.4.4 *Routine uses not included as primary or consistent uses*

Subsection 11(2) provides that the Designated Minister may set forth in the Privacy Index a statement of any of the uses and purposes not included in the statements made pursuant to sub-paragraph 11(1)(a)(iv), for which personal information contained in any of the personal information banks referred to in the Privacy Index is used or disclosed on a regular basis.

This provision permits government institutions to provide to the Designated Minister for publication in the Privacy Index statements of routine uses of personal information, which is neither a primary nor consistent use. These are permissible disclosures of the information under subsection 8(2) of the Act (see article .3.7 above) which take place on a regular basis. Examples of such routine uses are the provision of information in Unemployment Insurance Commission files to Members of Parliament (under paragraph 8(2)(g)) or the provision of family allowance information by National Health and Welfare to the Department of Indian Northern Affairs to carry out its programs (under paragraph 8(2)(b)).

Such statements of routine uses increase the knowledge of the individuals about the various uses and disclosures made of information concerning themselves. As well, this subsection enhances administrative efficiency. If no statement of a specific routine use is included in the Index then an institution is required, in accordance with subsection 9(1) of the Act (see article .4.5 below), to record each such use on an individual's file. The statement of routine uses eliminates this need to annotate an individual's file.

Government institutions shall, as part of the personal information bank identification and description process required by section 11 of the Act, provide to the Designated Minister a statement of routine uses made of information in each bank under their control and shall update these statements annually.

.4.5 *Retention of use and disclosure record*

Subsection 9(1) of the Privacy Act provides that a government institution shall retain a record of any use by the institution of personal information contained in a personal information bank or any use or purpose for which such information is disclosed by the institution where the use or purpose is not included in the statements of uses or purposes published in the Privacy Index pursuant to paragraph 11(1)(a)(iv) and subsection 11(2), and shall attach the record to the personal information.

Subsection 9(2) of the Act provides that such record of use or disclosure described in subsection 9(1) shall be deemed to form part of the personal information to which it is attached.

The purpose of these two subsections is to ensure that any use made of personal information which is not listed in the Privacy Index can be traced by the individual to whom the information relates. By requiring that a record of such uses and disclosures be attached to the personal information, it will be accessible along with the information when an access request is made, subject to any exemptions which may apply. This provision also assists the Office of the Privacy Commissioner in reviewing the use and disclosure of personal information.

In the case of a use or purpose for which personal information is disclosed but the use or purpose is not included in the description for the particular personal information banks, *a record shall consist (i) of the name and title of the person disclosing the information, (ii) the name of the institution, person, group of persons or organization receiving the information, (iii) notation of the use made of the information, and (iv) a copy of the information disclosed.*

As provided in section 4 of the Privacy Regulations (see Appendix B) these records must be retained for a minimum period of two years following the use or disclosure.

In the case of class disclosures reference must be made to the release arrangement agreed to by the Privacy Commissioner (see sub-article .3.7.13).

Investigative bodies

When a disclosure of personal information is made by a government institution to a federal investigative body under paragraph 8(2)(e) (see sub-article .3.7.5 above) subsections 9(1) and (2) still apply. A copy of the record of disclosure will be attached or maintained as part of the particular record disclosed and becomes part of the personal information concerning the individual that is under the control of the government institution. Such records of disclosure, if disclosed to the individual involved, could compromise an investigation which is in progress. *Therefore, institutions shall ensure that all records of disclosure are clearly marked as possibly qualifying for a section 22 exemption under the Act (the Model Form in Appendix C has this noted on it) and on those occasions when an individual requests access to personal information about him or herself to which is attached a record of disclosure to a federal investigative body, the government institution that has control of the information shall:

- consult with the investigative body which requested disclosure of the information before making a determination to exempt or disclose it in response to a request; and

- when exempting the information in response to an access request under section 22 of the Act, employ Model Letter E contained in Appendix D.

If the investigative body indicates that the record of disclosure does not qualify for exemption, it must be disclosed as part of the personal information requested. Of course, the record of disclosure of personal information to investigative bodies is available for examination by the Privacy Commissioner regardless of whether or not it is considered to qualify for exemption.

.4.6 *Consistent uses not previously accounted for*

Subsection 9(3) of the Privacy Act provides that where personal information in a personal information bank is used or disclosed for a use consistent with the purpose for which the information was obtained or compiled by an institution but the use is not included in the statement of consistent uses published in the Privacy Index pursuant to sub-paragraph 11(1)(a)(iv), the head of a government institution shall:

(a) forthwith notify the Privacy Commissioner of the use for which the information was used or disclosed; and

(b) ensure that the use is included in the next statement of consistent uses published in the Privacy Index.

This provision is included to deal with those exceptional circumstances where it may be necessary for institutions to use or disclose personal information for a purpose which, while consistent with the purpose for which it was obtained or compiled, could not be anticipated and is, therefore, not reflected in the Index. It permits use or disclosure for such a consistent use under paragraphs 7(a) and 8(2)(a) only where the Privacy Commissioner is immediately notified. Institutions are also required to submit an amendment of the personal

information bank description to the Designated Minister setting forth the new use. This amendment will be added to the statement of consistent uses for that bank and published in the next issue of the Privacy Index. The provision thus ensures that publication of all 'consistent uses' occurs in the same form but permits government institutions some flexibility when a legitimate new consistent use arises.

Part III

.5 *Right of access to personal information*

The Privacy Act provides individuals with a right of access to personal information about themselves. The Act also enables individuals to request corrections to be made to such information where there is an error or an omission or require that a notation be attached to that information reflecting any correction requested but not made.

.5.1 *Purpose*

This section provides assistance to government institutions in the interpretation of those provisions of the Privacy Act that deal with access to personal information under the Act and sets out directives and guidelines concerning these provisions which are to be applied as a matter of government policy. Government institutions should, where appropriate, develop and implement internal procedures, ensuring that these are consistent with the provisions of the Act and the content of this policy.

.5.2 *Informal access*

Provision of access to the type of personal information that has been generally available from government institutions to individuals about themselves is to be continued without formal processing under the Privacy Act. Examples include information in a claimant's UIC file, payroll deductions, vacation leave credits or personal information already published.

Where informal access cannot be given to the personal information requested, the applicant should be informed of his/her rights under the Privacy Act (see Model Letter A, Appendix D) and of the manner of exercising such rights through the use of the Access to Personal Information Request Form.

.5.3 *General requirements for processing formal requests*

.5.3.1 *Complete requests*

Subsection 12(1) of the Privacy Act provides the right of access to Canadian citizens or permanent residents, within the meaning of the Immigration Act, 1976, to personal information held about the individual by a government institution. Pursuant to subsection 12(3), the Governor in Council may, by order, extend the right of access to personal information to individuals not referred to above. This right has been extended to foreign prisoners incarcerated in Canada.

Section 13 of the Privacy Act and sections 8, 9 and 10 of the Privacy Regulations (see Appendix B) provide that an applicant has made a formal request for access to personal information when the application meets the following requirements:

- it is in writing, using the Access to Personal Information Request Form;
- it has been addressed to or received by an appropriate officer of the government institution listed in the Schedule to the Act that has control of the personal information in question; and
- it identifies each personal information bank that is the subject of the request or provides sufficiently specific information in respect of each class of personal information so as to render it reasonably retrievable by the government institution.

If the government institution believes that the application does not contain sufficient information on the location of the information to render it reasonably retrievable, it should contact the applicant to ask for more information before refusing to process the application. *If (subject to the foregoing), a request for access cannot be processed because it is incomplete, government institutions shall, within 10 days of receipt, inform the applicant of the steps required to complete his or her request and of his or her right to complain to the Privacy Commissioner if the applicant believes that sufficient information has already been provided to retrieve the information.*

The time available for government institutions to process requests to personal information is to be counted from the date of receipt of a complete request, as defined in this article.

As a matter of government policy, *government institutions should assist individuals seeking personal information under the Privacy Act, (e.g. handicapped individuals) who are unable to exercise their rights using regular procedures*.

.5.3.2 *Identification*

Before access is given to personal information, government institutions shall, pursuant to subsection 8(2) of the Regulations (see Appendix B), require adequate identification from the applicant, according to the identification requirements for individuals established by an institution for the relevant personal information bank. Where rigorous verification of identity is necessary, the applicant may be required to present himself/herself in person when access is given. If there is any doubt about the identity of the person, disclosure of personal information should not take place under any circumstances.

In accordance with Section 10 of the Regulations (see Appendix B), agents can be authorized by the applicant to exercise the right of access on his or her behalf. Where the rights of an applicant under the Act are exercised by a duly authorized representative, *government institutions shall require that the applicant's representative provide both adequate identification and written proof of authorization to act on behalf of the applicant before access is given*.

.5.3.3 *Documentation*

It is important that government institutions internally document essential control points at all stages of the access process, as such documentation may become necessary as evidence during the review process, especially review of institutional decisions undertaken by the Privacy Commissioner. A sample tracking document is provided in Appendix A of Part IV of this Chapter. This same form can be used to capture data

for the annual report to Parliament, pursuant to subsection 72(1) of the Act. *Government institutions shall record all administrative actions taken in processing requests under the Act where such actions are required by the Act or the Regulations.*

Exemption decisions must also be carefully documented. (*All reports, deliberations and decisions on invoking exemption provisions should be recorded and filed along with the information to which they pertain*). *Such documentation shall be subject to the controls on the retention and disposal of personal information set out in article .2.4 of this Part.*

.5.4 *Notices*

The Privacy Act sets out specific time limits for processing requests and conditions under which the applicant must be notified. Where the government institution fails to give access within the specified time limits, for the purposes of the Act, it is deemed to have refused access. Government institutions are encouraged to review the request with the applicant, especially when this would be helpful in interpreting the request, or aid the applicant in understanding any difficulties which may be encountered in processing the request (e.g. time extensions sought, the need for additional information etc.). Well-negotiated handling of requests may reduce the incidence of appeals.

The notification requirements prescribed by the Act are set out below. Model Letters for notices are provided in Appendix D.

The Act provides that government institutions shall, within thirty calendar days of receipt of a complete request, give a written notice to the applicant concerning the following:

(a) Excluded records: When the records containing personal information are excluded from access under the Privacy Act (for an explanation of excluded records, see section .6 of this Part).

(b) Method of access: When access is to be given, provide a copy of the personal information requested or by advising the applicant that arrangements can be made for viewing the information according to the conditions specified in section 9 of the Regulations (see Appendix B).

(c) Extension: When a government institution requires more time than the initial period of 30 days. The notice shall inform the applicant of the length of the extension and of his/her right to complain to the Privacy Commissioner about the extension. The circumstances under which the initial period of 30 days may be extended are the following, as set out in section 15 of the Privacy Act:

- if meeting the original time limit would unreasonably interfere with the operations of the government institution; or
- if the consultation necessary to comply with the request cannot reasonably be completed within 30 days. (Consultation in the context of this provision refers to consultation of the type undertaken with other government institution, foreign governments, medical practitioners etc. but not internal consultation.) It is important to note, however, that extension of time limits under the Privacy Act in these circumstances is permitted only for a maximum of another 30 days.

A form letter describing the required content of these notices is provided in Appendix D (see Model Letter G).

Time extension can also be sought for such a period of time as is reasonable, if additional time is necessary for translation purposes.

(d) Exemption: When access to the personal information requested or part thereof is refused. The notice should state the specific exemption which applies or that the personal information forms part of an exempt bank or that the personal information does not exist, or, where the government institution does not indicate whether the record exists, cite the specific

provision of the Privacy Act on which the refusal would be based or could reasonably be expected to be based if the information existed. It is to be noted that, pursuant to subsection 16(2), the government institution may but is not required to indicate whether or not the personal information exists. The notice should also inform the applicant of his/her right to appeal the decision to the Privacy Commissioner (see Model Letters D, E, and H in Appendix D).

.5.5 *Exemption application procedures*

.5.5.1 *Exemption review*

The underlying principle in applying most exemption criteria is the weighing or balancing of the right of access to personal information against the injury that could ensue from disclosure of that information. The bases of the factors governing exemptions are discussed in section .7 of this Part and this policy should be referred to when applying exemption criteria.

Under the coordination of its Privacy Coordinator, a *government institution shall review all personal information requested under the Privacy Act prior to disclosure in order to identify information that may technically qualify for exemption under the provisions of the Act*. In large institutions or institutions with regional offices, the review may take place under the coordination of a divisional or regional privacy coordinator. In some institutions personal information may be designated as part of an exempt bank. For policies regarding personal information contained in exempt banks see article .7.6.1.

.5.5.2 *Precedents*

In dealing with requests for information to which access has already been sought, government institutions should note that the decision to release or withhold a record may change because the injury involved is diminished or other new circumstances now apply.

Government institutions must assess each request on its own merits using precedents only as guidelines in making a determination either to disclose or exempt personal information. Documents classified under the government security classification system should receive more careful preliminary examination. However, the fact that a document is classified does not mean that it is exempt and each document must be judged in relation to the exemption provisions of the Act. At the review stage, the information should be screened for medical information and a decision made as to whether it may potentially qualify for an exemption under section 28 of the Act and thus should be referred to a duly qualified medical practitioner. Procedures concerning the disclosure of personal information relating to physical or mental health are contained in sections 13 and 14 of the Regulations (see Appendix B) and sub-article .7.6.11 of this Part.

.5.5.3 *Consultation*

Before making a determination to exempt or disclose certain information, it is the responsibility of the Privacy Coordinator to ensure that consultation with other government institutions takes place.

Consultation is mandatory whenever the personal information requested includes information received from or relating to the activities of another government institution from that processing the request as described in:

(a) section 19; information obtained 'in confidence' from other governments and international organizations (see sub-article .7.6.2);

(b) section 21; defence of Canada or any state allied or associated with Canada; international affairs and the detection, prevention and suppression of subversive or hostile activities (see sub-article .7.6.4);

(c) section 22; law enforcement and investigations (see sub-article .7.6.5);

(d) section 23; security clearances (see sub-article .7.6.6);

(e) section 25; the physical safety of individuals (see sub-article .7.6.8).

Consultation prior to determining whether or not to invoke any other exemptions is optional.

If the government institution consulted wishes to have an exemption invoked it should supply the government institution processing the request with a written explanation of why such an exemption is necessary. Even where consultation is mandatory, timely response to access requests is the responsibility of the institution processing the request. The point of consultation in the 'other' institution must either be the Privacy Coordinator or the official with the delegated authority to make a determination to exempt or disclose the particular information involved, which ever is most appropriate.

.5.5.4 *Exemption Decision*

The results of the review, the consultation report and, where necessary, the opinion of the institution's legal advisor form the basis for the final decision whether or not to actually invoke an exemption. This decision must be taken by the officer delegated authority by the head of the institution to claim the exemption.

Where another government institution has requested the exemption of certain information and there is to be a disclosure, it should be approved by the head of the institution processing the request.

Although the Privacy Act contains no specific provisions for the severing of documents containing personal information, this principle is built into the nature of the exemptions themselves, and therefore, when a decision has been reached to exempt particular records, a review should be undertaken to determine if exempt information can be severed from the record. The guidelines on severability are found in article .7.4 of this Part.

Pursuant to subsection 16(2), in notifying the applicant, the government institution may, but is not required to indicate whether the personal information exists. This provision was included to cover those situations, such as in the law enforcement area, where the denial or indication of the existence of the information could, in and of itself, expose the information for which exemption is being claimed. Use of this provision should be restricted to this type of exemption and only employed when necessary. In these cases, government institutions may, in the notification of refusal, use the wording suggested in Model Letter H in Appendix D.

The written notification of an exemption shall be signed by the appropriate officer within the government institution who has been delegated this responsibility or by the Privacy Coordinator on his or her behalf. Model letters of exemption notifications are provided in Appendix D.

.5.6 *Method of access*

Subsection 17(1) of the Privacy Act requires that where an individual is given access to personal information, the government institution shall, subject to Regulations, either permit the individual to examine the information or provide the individual with a copy thereof. Government institutions should, whenever possible, attempt to provide access through the method indicated by the applicant on the Access to Personal Information Request Form.

Pursuant to section 9 of the Regulations (see Appendix B), government institutions are required, where access to personal information is provided by means of examination, to ensure that the time arranged for examination is convenient not only for the institution but also for the individual and to provide reasonable facilities for the examination. Because of the sensitive nature of most personal information, the facilities provided for the examination of the information should be sufficiently private to allow undisturbed examination of the information while, at the same time, ensuring adequate security for it.

Government institutions should make every effort to ensure, where personal information is of a complex or technical nature, that an officer of the institution who understands the information is available to discuss with the applicant any questions that may arise. Special provision is made in Section 14 of the Regulations (see Appendix B) for dealing with certain types of sensitive medical information. An individual, under this provision, may be required by the head of a government institution, when given access to his or her physical or mental health information, to examine the information in person, in the presence of a duly qualified medical practitioner or psychologist, chosen by the head, who may explain or clarify the information to the individual.

.5.7 *Language of access*

Subsection 17(2) of the Act provides that if access to personal information is to be given, and the applicant requests that access be given in a particular official language, as declared in the Official Languages Act:

> (a) access shall be given in that language, if the personal information already exists in that language under the control of the government institution; and
>
> (b) where personal information does not exist in that language, the government institution that has control of the personal information shall cause it to be translated or interpreted for the individual if the translation or interpretation is considered to be necessary to enable the individual to understand the information.

Pursuant to paragraph 15(b), the initial time limit of 30 days for response may be extended by the government institution for a reasonable period of time that is necessary for translation purposes. In the case of lengthy records, interpretation (i.e. oral translation) should be considered as an alternative. Such an extension is subject to the notification procedures prescribed in article .5.4 of this Part.

Interpretation may be combined, in the case of technically complex information, with an explanation of the personal information by an expert, as prescribed by the directive in section .5.6 of this policy.

.5.8 *Corrections and notations*

.5.8.1 *Corrections*

Paragraph 12(2)(a) of the Act provides that every individual given access to personal information about him or herself that has been used, is being used or is available for use for an administrative purpose is entitled to request correction of such information where the individual believes it contains an error or omission.

Subsection 11(1) and (2) of the Privacy Regulations (see Appendix B) sets out the procedures to be followed by an individual in seeking a correction and by government institutions when responding to such requests.

When seeking a correction of information about him or herself, an individual is required to complete a Correction Request Form (see Model Form, Appendix D) for each personal information bank or class of personal information containing information which is considered by the individual to be in error or to contain an omission. Each completed form should be forwarded to the appropriate officer named for the particular bank(s).

In processing the Correction Request Form, institutions should also, where necessary, obtain from the individual making the request any documentary evidence needed to establish the validity of the correction.

The Act requires that the government institution, within 30 days of receiving a Correction Request Form, notify an individual, in writing, whether or not it will comply with the request for correction. As a matter of government policy, when an institution agrees to a request, it shall, forthwith, either:

(a) forward to the individual a copy of the relevant information duly corrected; or

(b) indicate in its notification to the individual that the requested correction has been made and that the individual may examine the information in person. Such examination of the information must be in accordance with the conditions set out in section 9 of the Privacy Regulations (see Appendix B).

When a government institution refuses to comply with a request for correction, the Regulations require that the individual be notified of the following:

(a) the reason for not correcting the information;

(b) the right of the individual to require a notation reflecting the correction requested (see sub-article .5.8.2 below) to be attached to the information in question;

(c) the right of the individual to bring a complaint before the Privacy Commissioner; and

(d) the address of the Privacy Commissioner.

Model Letter J included in Appendix D may be used for this purpose.

Accepting corrections

Different criteria should be used by institutions in determining whether or not to accept a correction request for:

(a) factual information such as age, occupation, family, etc.; and

(b) information consisting largely of opinions, such as evaluations, assessments, probabilities or beliefs.

Requests for corrections to factual information should usually be accepted, particularly when the individual originally supplied the information. However, in cases where changing the information has a direct financial or other impact on the individual (e.g. age, income or some other eligibility factor for a benefit), documentary proof to support the correction may be required. Such proof should ordinarily be the same as that required when the information was originally collected or obtained. Appropriate substitute documentation should be accepted, however, when original records have been lost, misplaced or are similarly not available.

Requests for correction of information consisting of opinion should ordinarily be accepted if the individual involved was the source of the original opinion. In most cases, however, opinion-type information will be derived from another source. In these instances, the original opinion should ordinarily remain as part of the personal information about an individual, unless there are reasons to suspect the reliability of the source who gave it. The individual should be informed that, while there is no reason to suspect that the record does not accurately reflect the opinion of the third party source, a notation can be attached to the information indicating the individual's views on the matter, as described in sub-article .5.8.2 of this Part.

.5.8.2 *Notations*

Paragraph 12(2)(b) of the Act provides that every individual given access to personal information about him or herself that has been used, is being used or is available for use for an administrative purpose is entitled to require that a notation be attached to that information reflecting any correction requested but not made.

Subsection 11(3) of the Privacy Regulations (see Appendix B) sets out the procedures to be followed by an individual requesting notation and by a government institution in responding to such a request.

When seeking a notation of personal information about him or herself, an individual is required to complete a Notation Request Form (see Model Form, Appendix D) for each personal information bank or class

of personal information containing information to be notated. Each completed form should be forwarded to the appropriate officer named for each bank containing the information involved. A government institution is required to process a request for notation within 30 days and shall notify the individual that the notation has been made (see Model Letter L, Appendix D). Failure to comply with a request for notation is subject to complaint to the Privacy Commissioner (see paragraph 29(1)(c).

.5.8.3 *Incorporation of corrections and notations*

In many cases, correction can be made by changing specific information within a record. In instances, however, where this is not possible (e.g. in the case of certain computer records), the accepted form of correction or notation is to be stored in such a way that it is normally retrieved with the original information (e.g. a flag indicator on a computer file or a notice attached to a paper file). *In all cases, corrections and notations must be stored so that they will be retrieved and used whenever the complete original personal information in question is used for an administrative purposes.*

.5.8.4 *Notification of correction or notation*

Paragraph 12(2)(c) of the Act provides that every individual who is given access to personal information about him or herself that has been used, is being used or is available for use for an administrative purpose is entitled to require that any person or body to whom such information has been disclosed for use for an administrative purpose within two years prior to the time a correction is requested or a notation required of that information under subsection 12(2):

- be notified of the correction or notation; and
- where the disclosure is to a government institution, the institution make the correction or notation on any copy of the information under its control.

This provision enables an individual who has either corrected or notated personal information about him or herself to ensure that such corrections or notations are passed on to any person or body which has received the information and is using it for an administrative purpose. Further, it requires government institutions which have received such information and are using it for an administrative purpose to ensure that the correction or notation is made or attached to every copy of the information under its control. *Government institutions receiving a request for correction of personal information or a notice of notation must clearly inform the individual to whom the information pertains of his or her right to have all persons or bodies to which the information has been disclosed notified of the correction or notation and acknowledge that a request for notification has been forwarded to the appropriate persons or bodies.* Model letters which may be used for these purposes are found in Appendix D. *Government institutions which receive notification of a requirement to correct or notate information disclosed to it for an administrative purpose shall inform the individual to whom the information pertains within 30 days of receiving the notification that the correction or notation has been made.*

Further, as matter of government policy, *government institutions shall also ensure that a copy of all accepted corrections or any notations are transmitted to all parts of the institution having copies of the information with instructions that the appropriate correction or notation be made.*