EPAL Translation of the

The Freedom of Information and Protection of Privacy Act

Calvin Powers, IBM
Steve Adler, IBM
Bruce Wishart, IBM

[version 1.1] – March 11, 2004

Document Change History

Version Number	Date	Author / Editor	Description of Change
1.0	Feb 5, 204	Calvin Powers, Editor	Initial Draft
1.1	March 11, 2004	Steven Adler, Editor	Final

1 Introduction

This white paper describes the process in which the privacy protection principles outlined in Ontario's Freedom of Information and Protection of Privacy Act [FIPPA] were translated into the Enterprise Privacy Authorization Language [EPAL].

This project to translate the FIPPA law into EPAL is not an attempt to replace the discretion and good judgment needed when making decisions that balance privacy protection against other needs. Its intent is to create a technical template that reflects the current decision making processes used in judging privacy issues and helping to identify those parts of the overall process that can be automated.

1.1 Acknowledgements

The authors would like to thank the following people from the Information and Privacy Commission/Ontario:

- Ann Cavoukian - Commissioner
- Ken Anderson - Assistant Privacy Commissioner
- Brian Beamish - Director, Policy and Compliance
- Mary O'Donoghue - Senior Counsel and Manager of Legal Services
- Mike Gurski - Senior Policy and Technology Advisor
- Sara Azargive, Articling Student, IPC
- Colin Bhattacharjee - Project Analyst, IPC
- Judith Goldstein, Legal Counsel , IPC

Comments and questions about this workshop can be sent to:

- Steve Adler, IBM, adler1@us.ibm.com
- Colin Bhattacharjee, IPC, Colin.Bhattacharjee@ipc.on.ca
- Calvin Powers, IBM, cspowers@us.ibm.com

1.2 Disclaimer

The goal of this workshop was to test the expressiveness of EPAL against a set of “real world” scenarios. The resulting EPAL policies generated from this workshop should be viewed as illustrations of EPAL’s capabilities and not viewed as interpretations of the Ontario Freedom of Information and Protection of Privacy Act (FIPPA).

You are responsible for insuring your compliance with the legal requirements imposed by the Ontario Freedom of Information and Protection of Privacy Act. It is your responsibility to obtain advice of competent legal counsel as to the applicability and interpretation of FIPPA. IBM does not provide legal advice or represent or warrant that its products, services, or documentation will guarantee or insure compliance with any law, regulation, or requirement.

2 Overview of FIPPA

Ontario’s *Freedom of Information and Protection of Privacy Act* (the FIPPA) took effect in 1988. It applies to all Ontario government ministries and most provincial agencies, boards and commissions, as well as to colleges of applied arts and technology and district health councils.

Freedom of information refers to public access to general records about what government does, ranging from administration and operations to legislation and policy. The underlying objective is open government – to hold elected and appointed officials accountable to the people they serve.

Privacy protection refers to the safeguarding of personal information – that is, data about identifiable individuals – held by government organizations. FIPPA and its accompanying regulations establish rules about how government organizations may collect, retain, use, disclose and dispose of personal information. In addition, individuals have the right to examine their own personal information and correct it if necessary.

The premise of FIPPA is that government is the custodian, not the owner, of the information it possesses. The true owner of general government information is the public collectively. And the true owner of personal information is the individual to whom the information relates.

FIPPA establishes an independent agency – the Office of the Information and Privacy Commissioner or the IPC – to review government decisions on access to information as well as government data protection practices. To ensure impartiality, the Commissioner is appointed by and accountable to the Legislative Assembly, not the government of the day. (IPC 1995 Annual Report).

3 Overview EPAL

The Enterprise Privacy Authorization Language (EPAL) [EPAL] was designed to enable Chief Privacy Officers (CPO), other policy makers, and an organization's internal Information Technology (IT) staff to translate their privacy policies into an XML based computer language. The resulting coded translation of human policy into Information Technology policy allows complex description of the internal data handling practices needed for enforcing the privacy policy.

EPAL describes data handling practices in a way that's independent of any particular technology, application, or data access protocol. Once the necessary data handling practices have been described in EPAL, they can be deployed, or embedded, in a wide variety of IT applications, databases, middleware, and infrastructure.

3.1 Introduction To Privacy Policies

In the IT world, traditional access control policies define access control rules using a set of three factors, the identity of the data user, the resource being accessed, and the action being performed on the resource. For example:

"Members of the doctor group can read protected health information."

Here, the data user is anyone who is in the doctor authorization group, the resource is protected health information, and the action is read.

Privacy policies and privacy legislation extend the traditional access control rules with the following dimensions:

- Purpose
- Data subject
- Obligations

3.1.1 Purpose

“Purpose” in a privacy policy refers to the allowed usage of data. No longer is it simply a matter of determining *who* is accessing the data, but their *usage* of the data must be justified in terms of what the governing privacy policy *allows*. For example:

“Doctors may read protected health information for medical treatment and diagnosis.”

This policy rule associates the purpose “medical treatment and diagnosis” with the rule. So if a doctor is attempting to access protected health information as a part of any activity other than treatment and diagnosis, the access should not be allowed.

Because of this, privacy policies are sometimes referred to as purpose based access control policies.

3.1.2 Data Subject

“Data subjects” are the individuals that the personal data describes. In a privacy policy, the data subject is as important to the access control decision as the data user, and in some situations, even more important. A wide variety of information about the data subject, called “data subject context”, can be included in privacy policies. Some of this information is relatively static information, such as “state of residence” or “legal guardian.” Sometimes the information is dynamic, but not controlled by the data subject, such as “current age”. Sometimes this data subject context is dynamic and chosen by the data subject, such as “opt in” choices that the data subject makes.

Typically, data subject context is expressed as conditions on policy rules:

“Doctor’s may read protected health information for medical treatment and diagnosis if the patient has nominated the doctor as his or her primary care physician.”

Here, “patient” is the data subject, i.e., the person that the protected health information is about and the “primary care physician” is a choice that the patient makes, which can be changed over time.

As another example:

"Medical researchers may read protected health information for medical research projects if the patient explicitly authorizes the release and is either a legal adult or has obtained an opt-in from their legal guardian."

In this case, the data subject is the patient, and there are three instances of data subject context information that need to be known in order to make an access control decision based on the rule, the consumer's opt-in choice (the explicit authorization), the consumer's current age, and the identity of the consumer's legal guardian.

Because of their focus on the data subject, privacy policies are sometimes referred to as data subject-centered access control policies.

3.1.3 Obligations

In many privacy policies, the access control decisions are not simply a matter of making an "allow" or "deny" decision. In many privacy policies, granting or denying access incurs an obligation on the data user to take additional actions.

For example,

"Medical researchers may read protected health information for medical research projects if the patient explicitly authorizes the release and is either a legal adult or has obtained an opt-in from their legal guardian. When protected health information is released to the medical researcher, the patient must be notified within 90 days and the protected health information must be deleted by the researcher within one year."

In this example, the patient notification and deletion clauses are obligations that the medical researcher must fulfill if protected health information is accessed according to this rule.

3.2 EPAL Design Goals

EPAL is a purpose based, data subject centric mark up language designed to make it easy to translate human readable privacy laws and privacy policies into a machine interpretable description of data handling practices that can be enforced as part of a data access authorization decision.

EPAL has been designed to:

- Link Access Control to natural text policies
- Create precise, fine grained description of the policy
- Enable complex, context driven conditions on policy rules
- Create portable, reusable policies
- Allow for sector/legislation specific policy vocabularies
- Enable policy negotiation

3.2.1 Linkage to Natural Text Policies

EPAL separates privacy policies into two components. The first component is the policy vocabulary. The vocabulary represents the concepts and classifications found in the natural language policy or law that needs to be implemented.

An EPAL vocabulary definition consists of the following:

- Categories of user making access requests
  (doctors, sales staff, claim adjuster, law enforcement, emergency room worker, etc.)
- Categories of data
  (protected health information, order history, political party affiliation)
- Actions being performed on the data
  (creation, read, update, delete, etc)
- Business purpose associated with the access request
  (medical research, order fulfillment, serving warrant,)
- Data subject context and conditions
  (opted in to marketing newsletter, primary care physician, is legal adult, etc)
- Obligations incurred on access
  (data subject must be notified within 30 days, data must be deleted after 7 years, etc.)

The second component of an EPAL policy is the rule component, which expresses the terms and conditions of the policy using the concepts found from the vocabulary.

When a policy author is implementing a specific law or policy, he or she will extract the vocabulary concepts from the human text and define them in an EPAL policy vocabulary. Then the policy author will express the rules and restrictions in the law or policy in an EPAL policy rule set.

3.2.2 Creating Fine-Grained Descriptions of Practices

EPAL Policy elements can be organized into hierarchies. This enables the policy author to create broad categories of rules and then refine these rules with exception rules.

For example, a hospital policy might define a broad category of “protected health information” and define a set of rules for who can access protected health information for which business purposes. Because most data in the hospital falls into this category, a small number of policy rules can cover most authorization decisions.

But the hospital policy may define special exception conditions for psychiatric notes. In EPAL, “psychiatric notes” can be defined as a sub-category of protected health information. Psychiatric Notes would then inherit all of the rules that apply to protected health information. But additional rules can be authored that apply only to psychiatric notes which add to or override the rules governing protected health information.

These hierarchical relationships allow the policy author to create rules that are as broad or as detailed as necessary to express the policy.

3.2.3 Context Driven Conditions

Privacy policy rules often attach conditions to access rules, which must be true in order for the rule to be valid.

For example, the Child Online Privacy and Protection Act (COPPA) of the United States indicates that contact information may be collected from people under the age of 13 only if their legal guardian authorizes (opts in) within 30 days.

EPAL uses an implementation neutral condition language to enable policy authors to express the complex conditions that today’s privacy policies require.

3.2.4 Creating Portable Policies

EPAL policies are abstract conceptual documents that are designed to translate the terms and conditions of a natural language policy into something that can be interpreted by an automated enforcement system.

An EPAL aware enforcement mechanism can then map the characteristics of a specific IT system into the concepts represented by the EPAL policy vocabulary and then make access enforcement decisions based on the rules described in the EPAL rule set.

This enables the same EPAL policy to be ported and deployed on multiple IT systems, in a “write once, deploy everywhere” fashion. This ensures that the same policy rules are consistently being enforced across the enterprise’s IT infrastructure.

3.2.5 Policy Defined Vocabularies

Because EPAL allows the policy author to define the vocabulary of the rules, EPAL policies are not restricted to any particular industry sector or any particular law.

Some EPAL policies may be custom tailored for “business to consumer” (B2C) scenarios, while others may be “business to business” (B2B) oriented. Some EPAL policies may be designed for typical best practices in the health care field, while other EPAL policies may be designed for the car rental industry. Some EPAL policies may be specific to HIPAA rules, while other EPAL policies may be specific to COPPA.

3.2.6 Enabling Policy Negotiation

Because EPAL creates a clear separation between the vocabulary definition and the policy rule definition, policy vocabularies can be shared between multiple organizations that have separate policies.

For example, the car rental industry may standardize a policy vocabulary for privacy policies in their industry. This vocabulary would contain the concepts that are common across all car rental companies. For example, it might contain vocabulary elements for reservation agent, maintenance worker, customer, credit card info, car reservation, customer profile, car make, car model, etc.

Each company in the industry can then author its own privacy policy using the industry standard vocabulary. In B2C scenarios, this enables client applications to compare one company’s policy to another’s policy and compare the policies against the client’s preferences. In B2B scenarios, it would allow two companies to compare and negotiate terms of privacy policies before they exchange customer personal data between the two companies.

3.3 *How To Create an EPAL Policy*

There are two components to an EPAL policy, the policy vocabulary and the policy rules.

The policy vocabulary represents the concepts from the natural language text policy that needs to be followed. The policy rules express the data handling practices that are either allowed or disallowed by the natural language text policy.

3.3.1 Extracting Vocabulary from Natural Language Text

An EPAL policy author uses the natural language text policy to develop the conceptual vocabulary elements of the policy.

The EPAL vocabulary elements are grouped into the following categories of vocabulary elements:

- User categories
  The final recipients of the personal information. Sometimes the user category is represented by the identity that actually makes the data access request. But sometimes the data access request is made by an intermediary and given to someone else. For the purposes of auditing, the important aspect of the privacy policy is who the final recipient or user of the data is.

- Data categories
  these are policy defined categories of information. Generally, privacy policies do not explicitly list specific elements of data that are or are not covered by the policy. Instead, they define broad categories of information.

  For example, a privacy protection policy in the health care industry would typically not list x-rays, prescriptions, cholesterol test results, etc. in their privacy policy because it would be impossible to ensure that the list is complete. Instead, the policy would create a broad category, perhaps called “protected health information” and associate that term with a definition that serves as guidance for judging whether any given element of data falls into the category or not.

- Purpose categories
  The purpose categories in a policy represent the *allowed* and *disallowed* uses of data. Typically these are described in terms of the business processes or organizational services and functions that are performed by the enterprise.

For example, a hospital may have a policy that allows health care providers to access the health records of a patient's immediate blood relatives *for the purposes of diagnosing a patient's condition.* Diagnosis is one of the core activities of health care provider's in a hospital, so the data handling practices that are allowed as part of that activity should be described.

- Action categories
  Action categories are low-level operations on data that are allowed as part of performing one of the purposes. Typically, but not always, these low level actions are expressed in terms of "create, read, update" types of operations.

  Building on the example above, the health care provider may be allowed to *read* the medical histories of a patients blood relatives for the purpose of diagnosis, but may not be allowed to *update or delete* those medical histories.

- Obligations
  Obligations are activities that must be fulfilled as a result of accessing or using personal information. Data subject notification activities, data retention requirements, and data disposal requirements are examples of typical obligations.

- Conditions
  Conditions represent context under which a data handling practice can or cannot be performed.

  For example, a policy might require that e-mail addresses can only be used for marketing purposes if the owner of the e-mail address is older than 13 years old. In this case, "older than 13 years" is a condition that might have to be evaluated in order to determine if a particular data access request should or should not be allowed.

3.3.2 Expressing Rules in Semi-Structured English

The EPAL policies have a "default ruling" which can be either:

- Allow: The data access request should be allowed
- Deny: The data access request should be denied
- Not-Applicable: The data access request is not applicable to this policy

The default ruling is applied if none of the rules in the policy apply to a particular data access request.

Each EPAL rule can be expressed in a “semi-structured English syntax”

A [user category] should be [allowed or denied] the ability to perform [action] on [data category] for [purpose] under [conditions] yielding an obligation to [obligation].

For example:

A [Borderless Books Employee In Marketing] should be [allowed] the ability to perform [read] operations on [book purchase histories] for [Book of The Month Club Activities] under [the condition that customer authorizes the activity] yielding an obligation to [dispose of book purchase histories after 3 years].

3.3.3 Translating the policy into EPAL syntax

Once the vocabulary elements from the natural language text policy have been identified and categorized and the vocabulary elements have been used to create semi-structured representations of the policy requirements, it’s a straight forward process to convert these into EPAL syntax as defined by the EPAL schema definitions.

4 FIPPA Vocabulary

This section documents the EPAL vocabulary elements that were extracted from FIPPA by the workshop participants.

4.1 User Categories

4.1.1 Requester

A requester is a person who has requested access to a government-held record under the access scheme in Part II of FIPPA.

The term “requester” does not appear anywhere in FIPPA. However, section 10(1), which is in Part II, gives “every person” a right of access to a record or part of a record subject to certain exceptions.

Section 42(a) permits an institution to disclose personal information in accordance with Part II of FIPPA.

4.1.2 Affected party

An affected party is a person whose interests may be affected by the disclosure of his or her personal information.

In the context of privacy, section 28(1)(b) states that before a head grants a request for access to a record that is personal information that the head has reason to believe might constitute an unjustified invasion of personal privacy for the purposes of clause 21(1)(f), the head shall give written notice in accordance with subsection (2) to the person to whom the information relates.

4.1.3 Data subject

The data subject is the person to whom the personal information relates.

The term “data subject” does not appear in FIPPA. However, section 42(b) permits an institution to disclose personal information where the person to whom the information relates has identified that information in particular and consented to its disclosure.

4.1.4 Officer or employee of the institution

An officer or employee of the institution is a public servant.

Section 42(d) permits an institution to disclose personal information where disclosure is made to an officer or employee of the institution who needs the record in the performance of his or her duties and where disclosure is necessary and proper in the discharge of the institution's functions.

4.1.5 Law enforcement institution

A law enforcement institution refers to a police service or any body that falls within the definition in section 2(1).

Section 2(1) defines “law enforcement” as (a) policing, (b) investigations or inspections that lead or could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed in those proceedings, and (c) the conduct of proceedings referred to in clause (b).

Section 42(f) permits an institution to disclose personal information where disclosure is by a law enforcement institution, (i) to a law enforcement agency in a foreign country under an arrangement, a written agreement or treaty or legislative authority, or (ii) to another law enforcement agency in Canada.

Section 42(g) permits an institution to disclose personal information where disclosure is to an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result.

4.1.6 Law Enforcement Agency

In FIPPA, a law enforcement institution is a part of the Ontario government that engages in law enforcement activities. A law enforcement agency is an organization outside of the Ontario government, either at the Federal level or in a foreign country that also engages in law enforcement activities.

4.1.7 Next of kin or friend

The next of kin may be a family member of an injured, ill or deceased person. A friend is a close associate to a person.

Section 42(i) permits an institution to disclose personal information where disclosure is in compassionate circumstances, to facilitate contact with the next of kin or a friend of an individual who is injured, ill or deceased.

4.1.8 Member of the Legislative Assembly

A member of the Legislative Assembly is an elected member of Ontario’s provincial parliament.

Section 42(j) permits an institution to disclose personal information where disclosure is to a member of the Legislative Assembly who has been authorized by a constituent to whom the information relates to make an inquiry on the constituent's behalf or, where the constituent is incapacitated, has been authorized by the next of kin or legal representative of the constituent.

4.1.9 Bargaining agent

A bargaining agent is a person or entity that represents and acts for others, usually in collective bargaining negotiations between unions and management.

Section 42(k) permits an institution to disclose personal information where disclosure is to a member of the bargaining agent who has been authorized by an employee to whom the information relates to make an inquiry on the employee's behalf or, where the employee is incapacitated, has been authorized by the next-of-kin or legal representative of the employee.

4.1.10 Responsible minister

The responsible minister is a member of cabinet who is the minister responsible for the purposes of the FIPPA..

Section 2(1) defines “responsible minister" as the minister of the Crown who is designated by order of the Lieutenant Governor in Council under section 3.

Section 42(l) permits an institution to disclose personal information where disclosure is to the responsible minister.

4.1.11 Information and Privacy Commissioner

The Information and Privacy Commissioner (IPC) is the person responsible for overseeing enforcement of FIPPA in Ontario.

Section 2(1) defines "Information and Privacy Commissioner" and "Commissioner" as the Commissioner appointed under subsection 4(1).

Section 42(m) permits an institution to disclose personal information where disclosure is to the Information and Privacy Commissioner.

4.1.12 Government of Canada

The Government of Canada refers to the federal government.

Section 42(n) permits an institution to disclose personal information where disclosure is to the Government of Canada in order to facilitate the auditing of shared cost programs.

4.1.13 Head of an Institution

Defined in section 2(1):

"head", in respect of an institution, means,

(0.a) in the case of the Assembly, the Speaker;

(a) in the case of a ministry, the minister of the Crown who presides over the ministry, and

(b) in the case of any other institution, the person designated as head of that institution in the regulations;

4.2 Data Categories

4.2.1 General records

These records contain information relating to the activities of government, ranging from administration and operations to legislation and policy. They do not include personal information.

4.2.2 Personal Information

These records contain personal information, which defined in section 2(1) as recorded information about an identifiable individual, including:

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

(b) information relating to the education or the medical, psychiatric, psychological, 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, telephone number, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they relate to another individual,

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

(g) the views or opinions of another individual about the individual, and

(h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

Note that section 46(2) expands this definition to also include: (2) A record retained under subsection 46(1) forms part of the personal information to which it is attached or linked.

4.2.3 Identifiable Personal Information

Identifiable information is a sub-category of personal information and is defined in section 44 as personal information that is “intended to be retrieved by the individual's name or by an identifying number, symbol or other particular assigned to the individual.”

4.3 Actions

4.3.1 Collection

The rules governing the collection of personal information are found in sections 37-39.

4.3.2 Use

The rules governing the use of personal information are found in sections 41 and 43.

4.3.3 Disclosure

The rules governing the disclosure of personal information are found in sections 42 and 43.

4.3.4 Create A Record of Use or Disclosure

From 46(1):

(1) A head shall attach or link to personal information in a personal information bank,

(a) a record of any use of that personal information for a purpose other than a purpose described in clause 45(d); and

(b) a record of any disclosure of that personal information to a person other than a person described in clause 45(e).

4.4 Purposes

4.4.1 Complying with an access request

If an institution receives a request for access to personal information, it must follow the access rules in Part II of FIPPA.

Section 42(a) permits an institution to disclose personal information in accordance with Part II of FIPPA.

4.4.2 Performing government business

An institution may use or disclose personal information for the purpose of performing government business.

Section 41(b) permits an institution to use personal information for the purpose for which it was obtained or compiled or for a consistent purpose.

Section 42(c) permits an institution to disclose personal information for the purpose for which it was obtained or compiled or for a consistent purpose.

Section 42(d) permits an institution to disclose personal information where disclosure is made to an officer or employee of the institution who needs the record in the performance of his or her duties and where disclosure is necessary and proper in the discharge of the institution's functions.

Section 42(e) permits an institution to disclose personal information for the purpose of complying with an Act of the Legislature or an Act of Parliament or a treaty, agreement or arrangement thereunder.

4.4.3 Law enforcement

An institution may disclose personal information for the purposes of law enforcement.

Section 42(f) permits an institution to disclose personal information where disclosure is by a law enforcement institution, (i) to a law enforcement agency in a foreign country under an arrangement, a written agreement or treaty or legislative authority, or (ii) to another law enforcement agency in Canada.

Section 42(g) permits an institution to disclose personal information where disclosure is to an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result.

4.4.4 Affecting health and safety

An institution may disclose personal information for the purpose of affecting (or protecting) an individual’s health and safety.

Section 42(h) permits an institution to disclose personal information in compelling circumstances affecting the health or safety of an individual if upon disclosure notification thereof is mailed to the last known address of the individual to whom the information relates.

4.4.5 Contacting a party

An institution may disclose personal information for the purpose of contacting a party in compassionate circumstances.

Section 42(h) permits an institution to disclose personal information in compassionate circumstances, to facilitate contact with the next of kin or a friend of an individual who is injured, ill or deceased.

4.4.6 Facilitating ministerial responsibility

The responsible minister may require personal information for the purpose of fulfilling his or her duties. Section 42(l) permits an institution to disclose personal information to the responsible minister.

4.4.7 Dealing with access appeals and privacy complaints

The IPC requires access to records containing personal information in order to mediate and adjudicate access appeals and conduct privacy investigations.

Section 42(m) permits an institution to disclose personal information where disclosure is to the Information and Privacy Commissioner.

4.4.8 Facilitating the auditing of shared cost programs

The federal government may require access to personal information held by the Ontario government in order to audit shared cost programs.

Section 42(n) permits an institution to disclose personal information where disclosure is to the Government of Canada in order to facilitate the auditing of shared cost programs.

4.4.9 Creation of a Personal Information Bank

Section 44 defines the following reason for using personal information: “shall cause to be included in a personal information bank”

4.4.10 Publishing an Index of Personal Information Banks

From section 45: “The responsible minister shall publish at least once each year an index of all personal information banks . . “

4.4.11 Notifying the Responsible Minister In Order To Update Index

From 46(3): “the head shall, (a) forthwith notify the responsible minister of the use or disclosure; and (b) ensure that the use is included in the index.

4.4.12 Respond To A Correction Request

From section 47(2): “(a) request correction of the personal information where the individual believes there is an error or omission therein; (b) require that a statement of disagreement be attached to the information reflecting any correction that was requested but not made”

4.5 Obligations

4.5.1 Retention

Section 40(1) requires that personal information that has been used by an institution be retained after use by the institution for the period prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the personal information.

Section 5(1) of Regulation 460 requires that personal information used by an institution be retained for at least one year after use unless the individual to whom the information relates consents to its earlier disposal.

4.5.2 Disposal

The rules governing the disposal of personal information are found in section 40(4) and Regulation 459.

Section 6(1) of Regulation 459 requires every head of an institution to ensure that the institution maintains a disposal record setting out what personal information has been destroyed or transferred to the Archives and the date of that destruction or transfer.

Section 6(2) requires that the head ensure that the disposal record maintained under subsection (1) does not contain personal information.

4.5.3 Collection – Providing proper notice to the data subject

Section 39(2) states that where personal information is collected on behalf of an institution, the head shall, unless notice is waived by the responsible minister, inform the individual to whom the information relates of,

(a) the legal authority for the collection;

(b) the principal purpose or purposes for which the personal information is intended to be used; and

(c) the title, business address and business telephone number of a public official who can answer the individual's questions about the collection.

4.5.4 Disclosure – Providing proper notice to the data subject

Section 42(h) permits an institution to disclose personal information in compelling circumstances affecting the health or safety of an individual if upon disclosure notification thereof is mailed to the last known address of the individual to whom the information relate.

4.5.5 Notification of Correction Request

Section 47(2)(c) requires that in cases where an information correction has been requested, that recipients or users of the data in question must be notified.

4.5.6 Proper Manner of Disclosure For Access Requests

Section 48(3) sets requirements on how data may be disclosed in cases where the individual has requested access to his or her information:

"(3) Subject to the regulations, where an individual is to be given access to personal information requested under subsection (1), the head shall, (a) permit the individual to examine the personal information; or (b) provide the individual with a copy thereof."

Section 48(4) creates additional obligations on the form of the information provided to the requestor:

"Where access to personal information is to be given, the head shall ensure that the personal information is provided to the individual in a comprehensible form and in a manner which indicates the general terms and conditions under which the personal information is stored and used."

5 FIPPA Conditions and Rules

5.1 Conditions

Note on condition definitions. In EPAL, a formal condition language is used to articulate the exact semantics of the conditions in a way that could be implemented in a wide variety of IT systems and to make the exact meaning of the condition more clear.

Due to the limited time period for the workshop, the formal expression of the condition semantics was omitted.

5.1.1 Maintained for purpose of making public

This condition is taken directly from section 37, which exempts personal information from the requirements of Part III if the purpose of the collection is for making or creating a record that is available to the general public.

For example, databases used to check for current owners of land and property are considered public information because it’s used to check for liens, etc., so the collection of data to keep these databases up to date and accurate is not covered by Part III.

EPAL Syntax:

```
- <condition id="maintained-for-purpose-of-making-public">
     <long-description>maintained for the purpose of creating a
        record that is available to the general public. 1987, c. 25,
        s. 37. Further interpretation of the law has added the
        further requirement that the data be currently held by the
        same institution that originally collected it.</long-
        description>

     <evaluates-container refid="x" />

     <xacml:Condition FunctionId="" />

  </condition>
```

5.1.2 Proper Purpose of Collection

An institution is not allowed to collect personal information unless one of three conditions is met.

Section 38(2) states that no person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

EPAL Syntax:

```
- <condition id="condition-for-proper-collection">
    <long-description>(2) No person shall collect personal
      information on behalf of an institution unless the
      collection is expressly authorized by statute, used for the
      purposes of law enforcement or necessary to the proper
      administration of a lawfully authorized activity.</long-
      description>

    <evaluates-container refid="x" />

    <xacml:Condition FunctionId="" />

  </condition>
```

5.1.3 Proper Manner of Collection

An institution must collect personal information directly from an individual. It may only collect information from a source other than individual (i.e., indirectly) if specific conditions are met.

Section 39(1) requires that personal information only be collected by an institution directly from the individual to whom the information relates unless,

(a) the individual authorizes another manner of collection;

(b) the personal information may be disclosed to the institution concerned under section 42 or under section 32 of the Municipal Freedom of Information and Protection of Privacy Act;

(c) the Commissioner has authorized the manner of collection under clause 59(c);

(d) the information is in a report from a reporting agency in accordance with the Consumer Reporting Act;

(e) the information is collected for the purpose of determining suitability for an honour or award to recognize outstanding achievement or distinguished service;

(f) the information is collected for the purpose of the conduct of a proceeding or a possible proceeding before a court or tribunal;

(g) the information is collected for the purpose of law enforcement; or

(h) another manner of collection is authorized by or under a statute.

EPAL Syntax:

```
<condition id="proper-manner-of-collection">
    <long-description>39. (1) Personal information shall only be
      collected by an institution directly from the individual to
      whom the information relates unless, (a) the individual
      authorizes another manner of collection; (b) the personal
      information may be disclosed to the institution concerned
      under section 42 or under section 32 of the Municipal
      Freedom of Information and Protection of Privacy Act; (c)
      the Commissioner has authorized the manner of collection
      under clause 59(c); (d) the information is in a report from
      a reporting agency in accordance with the Consumer
      Reporting Act; (e) the information is collected for the
      purpose of determining suitability for an honour or award
      to recognize outstanding achievement or distinguished
      service; (f) the information is collected for the purpose of
      the conduct of a proceeding or a possible proceeding
      before a court or tribunal; (g) the information is collected
      for the purpose of law enforcement; or (h) another
      manner of collection is authorized by or under a
      statute.</long-description>

    <evaluates-container refid="x" />

    <xacml:Condition FunctionId="" />
    </condition>
```

5.1.4 Proper Notice To Individual

Where information is collected, notice must be given to the data subject.

EPAL Syntax:

```
  <condition id="proper-notice-to-individual">
      <long-description>s. 39(2) (2) Where personal information is
         collected on behalf of an institution, the head shall, unless
         notice is waived by the responsible minister, inform the
         individual to whom the information relates of, (a) the
         legal authority for the collection; (b) the principal purpose
         or purposes for which the personal information is
         intended to be used; and (c) the title, business address
         and business telephone number of a public official who
         can answer the individual's questions about the
         collection.</long-description>

      <evaluates-container refid="x" />

      <xacml:Condition FunctionId="" />

    </condition>
```

5.1.5 Proper Exceptions to Notice Obligation

EPAL Syntax:

```
  <condition id="proper-exceptions-to-notice-obligation">
      <long-description>s. 39(3) (3) Subsection (2) does not apply
         where the head may refuse to disclose the personal
         information under subsection 14 (1) or (2) (law
         enforcement), section 14.1 (Remedies for Organized
         Crime and Other Unlawful Activities Act, 2001) or section
         14.2 (Prohibiting Profiting from Recounting Crimes Act,
         2002). or unless notice is waived by the responsible
         minister as described in 39(2)</long-description>
```

```
        <evaluates-container refid="x" />

        <xacml:Condition FunctionId="" />

    </condition>
```

5.1.6 Disclosure on Consent

This condition comes directly from section 41 (a), an institution must not use or disclose personal information unless the data subject has identified that particular information and agreed to its use or disclosure.

EPAL Syntax:

```
  - <condition id="disclosure-on-consent">
        <long-description>(a) where the person to whom the
           information relates has identified that information in
           particular and consented to its disclosure;</long-
           description>

        <evaluates-container refid="x" />

        <xacml:Condition FunctionId="" />

    </condition>
```

5.1.7 Disclosure Purpose Same Or Consistent With Collection Purpose

This condition comes directly from the text of section 41 (b)

EPAL Syntax:

```
  <condition id="disclosure-purpose-same-or-consistent-with-
        collection-purpose">
        <long-description>for the purpose for which it was obtained
           or compiled or for a consistent purpose;</long-description>

        <evaluates-container refid="x" />
        <xacml:Condition FunctionId="" />

    </condition>
```

5.1.8 Complying With An Act

This condition comes directly from the text of section 42(e)

EPAL Syntax:

```
  - <condition id="complying-with-an-Act">
        <long-description>(e) for the purpose of complying with an
           Act of the Legislature or an Act of Parliament or a treaty,
           agreement or arrangement thereunder;</long-description>

        <evaluates-container refid="x" />

        <xacml:Condition FunctionId="" />

    </condition>
```

5.1.9 Disclosure By Law Enforcement Institution

Disclosure of personal information by an institution for law enforcement purposes is conditional on correctly identifying the recipient agency as a “law enforcement” institution.

EPAL Syntax:

```
  <condition id="disclosure-by-law-enforcement-institution">
        <long-description>See section 2 for definition of “law
           enforcement”  and 42(f) and (g) for rules governing
           disclosure. </long-description>

        <evaluates-container refid="x" />

        <xacml:Condition FunctionId="" />

    </condition>
```

5.1.10 Under An Arrangement

This condition covers disclosure of personal information by an institution for the purpose of complying with an Act of the Legislature or an Act of Parliament or a treaty, agreement or arrangement thereunder, in conditional on the institution correctly interpreting the Act, treaty, agreement or arrangement.

EPAL Syntax:

```
<condition id="under-an-arrangement">
    <long-description>42 f l l under an arrangement, a written
      agreement or treaty or legislative authority,</long-
      description>

    <evaluates-container refid="x" />

    <xacml:Condition FunctionId="" />

  </condition>
```

5.1.11 To Aid An Investigation

Section 42(g) defines a condition that allows for permits an institution to disclose personal information where disclosure is to an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result.

EPAL:

```
- <condition id="to-aid-an-investigation">
    <long-description>(g) where disclosure is to an institution or
      a law enforcement agency in Canada to aid an
      investigation undertaken with a view to a law
      enforcement proceeding or from which a law enforcement
      proceeding is likely to result;</long-description>

    <evaluates-container refid="x" />

    <xacml:Condition FunctionId="" />
```

```
      </condition>
```

5.1.12 Authorized By A Constituent

Section 42(j) defines the conditions under which data can be disclosed to a member of the legislative assembly.

EPAL syntax:

```
   <condition id="authorized-by-a-constituent-next-of-kin-or-legal-
        representative">

        <long-description>Section 42(j) permits an institution to
           disclose personal information where disclosure is to a
           member of the Legislative Assembly who has been
           authorized by a constituent to whom the information
           relates to make an inquiry on the constituent's behalf or,
           where the constituent is incapacitated, has been
           authorized by the next of kin or legal representative of
           the constituent. So there needs to be a condition that
           tests the relationship between the member of the
           legislative assembly and the data subject.</long-
           description>

        <evaluates-container refid="x" />

        <xacml:Condition FunctionId="" />

  </condition>
```

5.1.13 Authorized by Employee

The conditions under which an institution may disclose personal information to an employees’ bargaining agent are defined in 42(k).

EPAL Syntax:

```
   - <condition id="authorized-by-employee-next-of-kin-or-legal-
        representative">
```

```
    <long-description>Section 42(k) permits an institution to
      disclose personal information where disclosure is to a
      member of the bargaining agent who has been authorized
      by an employee to whom the information relates to make
      an inquiry on the employee's behalf or, where the
      employee is incapacitated, has been authorized by the
      next-of-kin or legal representative of the
      employee.</long-description>

    <evaluates-container refid="x" />

    <xacml:Condition FunctionId="" />

  </condition>
```

5.1.14 For the Purpose For Which Data Was Obtained

Section 41(b) allows for data usage by an institution for the purposes that it was originally obtained or compiled or for a consistent purpose.

EPAL Syntax:

```
- <condition id="for-the-purpose-for-which-it-was-obtained-or-
    compiled-or-for-a-consistent-purpose">
    <long-description>41(b) and see 43 for definition of
      consistent purpose</long-description>

    <evaluates-container refid="x" />

    <xacml:Condition FunctionId="" />

  </condition>
```

5.1.15 For A Purpose For Which the Data May Be Disclosed To An Institution

This condition links the purpose of receiving data via disclosure to the purpose of the usage.

EPAL Syntax:

```
- <condition id="for-a-purpose-for-which-the-information-may-be-
    disclosed-to-the-institution">
    <long-description>41(c) for a purpose for which the
      information may be disclosed to the institution under
      section 42 or under section 32 of the Municipal Freedom
      of Information and Protection of Privacy Act. Notes:
      Should be covered under all section of 42 of this Act
      except f,j,k, m, n In the MFIPPA, all clauses would apply
      except f, k, and l.</long-description>

    <evaluates-container refid="x" />

    <xacml:Condition FunctionId="" />

  </condition
```

5.1.16 Standard of Accuracy

In some cases, data may not be used by the institution if it can’t show that it has adequate controls in place to ensure the accuracy of the data.

It’s tempting to express this concept as an obligation, but obligations are something that happens *after* the data is used or disclosed. But this is a condition that you would want to test *before* the data is disclosed.

EPAL Syntax:

```
- <condition id="standard-of-accuracy">
    <long-description>The head of an institution shall take
      reasonable steps to ensure that personal information,
      except that collected for law enforcement purposes
```

```
            (40(3)), is not used unless it is accurate and up to date.
            1987, c. 25, s. 40(1, 2).</long-description>

        <evaluates-container refid="x" />

        <xacml:Condition FunctionId="" />

    </condition>
```

5.1.17 No section 49 Exemptions are being exercised

Section 49 gives the head of the institution some discretion in when an individual has a right to access their information:

A head may refuse to disclose to the individual to whom the information relates personal information,

(a) where section 12, 13, 14, 14.1, 14.2, 15, 16, 17, 18, 19, 20 or 22 would apply to the disclosure of that personal information;

(b) where the disclosure would constitute an unjustified invasion of another individual's personal privacy;

(c) that is evaluative or opinion material compiled solely for the purpose of determining suitability, eligibility or qualifications for employment or for the awarding of government contracts and other benefits where the disclosure would reveal the identity of a source who furnished information to the institution in circumstances where it may reasonably have been assumed that the identity of the source would be held in confidence;

(d) that is medical information where the disclosure could reasonably be expected to prejudice the mental or physical health of the individual;

(e) that is a correctional record where the disclosure could reasonably be expected to reveal information supplied in confidence; or

(f) that is a research or statistical record.

5.1.18 Consistent Purpose Test on Direct Collection

This condition expresses the tests from section 43. In cases where the data is collected directly from the individual, the uses or disclosure of data are further qualified by a test that “the individual might reasonably have expected such a use or disclosure.”

5.1.19 Within One Year of Last Index

Section 45 states: “The responsible minister shall publish at least once each year an index of all personal information banks.”

5.1.20 Inconsistent with section 45 d and e

Section 46(1):

(1) A head shall attach or link to personal information in a personal information bank,

(a) a record of any use of that personal information for a purpose other than a purpose described in clause 45(d); and

(b) a record of any disclosure of that personal information to a person other than a person described in clause 45(e).

5.1.21 Recipient Is Data Subject

Sections 47 to 49 address situations in which an individual as requesting access to data about himself, so these rules must be qualified with a condition that ensures that the data recipient matches the data subject of the request.

5.1.22 Access Request Criteria Met

Sections 47(1) and 48(1) spell out criteria which the individual must satisfy in order for the access request to processed by the institution.

Section 47(1) states:

47. (1) Every individual has a right of access to,

(a) any personal information about the individual contained in a personal information bank in the custody or under the control of an institution; and

(b) any other personal information about the individual in the custody or under the control of an institution with respect to which the individual is able to provide sufficiently specific information to render it reasonably retrievable by the institution.

Section 48 states:

48. (1) An individual seeking access to personal information about the individual shall,

(a) make a request in writing to the institution that the individual believes has custody or control of the personal information;

(b) identify the personal information bank or otherwise identify the location of the personal information; and

(c) at the time of making the request, pay the fee prescribed by the regulations for that purpose.

5.2 Rules

As mentioned before, the rules from the natural language text must be reformed into a standard, semi-structured statement in the form of:

A [user category] should be [allowed or denied] the ability to perform [action] on [data category] for [purpose] under [conditions] yielding an obligation to [obligation].

5.2.1 Rule for Section 37

Natural Language Text:

This Part does not apply to personal information that is maintained for the purpose of creating a record that is available to the general public. 1987, c. 25, s. 37.

Semi-Structured Text

Any institutional user should be allowed the ability to disclose, collect or use personal information for any-purpose if the data is maintained for the purpose of making public.

EPAL Syntax:

```
 - <rule id="S37" ruling="allow">
      <user-category refid="any-user" />

      <data-category refid="personal-information" />

      <purpose refid="any-purpose" />

      <action refid="disclosure" />

      <action refid="use" />

      <action refid="collect" />

      <condition refid="maintained-for-purpose-of-making-public"
        />

   </rule>
```

5.2.2 Rule for Section 38 – Without Notice

Sections 37-39 of the Act cover the conditions for collecting personal information. This rule covers situations in which section 39 exempts the institution from providing notice of the collection.

Semi-Structured Text

An institution is allowed to collect personal information if the conditions for proper collection are met, the data was collected in a proper manner, and the conditions for exceptions to notice obligation are met.

EPAL Syntax:

```
 - <rule id="s38-2-no-notice" ruling="allow">
      <user-category refid="institution" />
```

```
    <data-category refid="personal-information" />

    <purpose refid="any-purpose" />

    <action refid="collection" />

    <condition refid="condition-for-proper-collection" />

    <condition refid="proper-manner-of-collection" />

    <condition refid="proper-exceptions-to-notice-obligation" />

  </rule>
```

5.2.3 Rule for Section 38 – With Notice

Sections 37-39 of the Act cover the conditions for collecting personal information. This rule covers situations in which the institution is obligated to provide notice of the collection

Semi-Structured Text

An institution is allowed to collect personal information if the conditions for proper collection are met, the data is collected in a proper manner, an proper notice has been given to the individual.

EPAL Syntax:

```
- <rule id="s38-2" ruling="allow">
    <user-category refid="institution" />

    <data-category refid="personal-information" />

    <purpose refid="any-purpose" />

    <action refid="collection" />

    <condition refid="condition-for-proper-collection" />
    <condition refid="proper-manner-of-collection" />

    <condition refid="proper-notice-to-individual" />

  </rule>
```

5.2.4 Rule for 41(a)

Natural Language Text:

41. An institution shall not use personal information in its custody or under its control except,

(a) where the person to whom the information relates has identified that information in particular and consented to its use;

Semi-Structured Text

An institution is allowed to use personal information for any-purpose if the individual has identified the data and consented to its disclosure, the institution has taken reasonable steps to ensure that the personal information is accurate yielding an obligation to ensure that proper retention policies are followed.

EPAL Syntax:

```
- <rule id="s41-a" ruling="allow">
    <user-category refid="institution" />

    <data-category refid="personal-information" />

    <purpose refid="any-purpose" />

    <action refid="use" />

    <condition refid="disclosure-on-consent" />

    <condition refid="standard-of-accuracy" />
```

```
        <obligation refid="retention-of-personal-information" />

      </rule>
```

5.2.5 Rule for 41(b)

Natural Language Text:

41. An institution shall not use personal information in its custody or under its control except, . . . (b) for the purpose for which it was obtained or compiled or for a consistent purpose; or

Semi-Structured Text

An institution is allowed to use personal information if the data is being used or a purpose for which it was obtained or compiled or for a consistent purpose and the institution has taken reasonable steps to ensure that the personal information is accurate yielding an obligation to ensure that proper retention policies are followed.

EPAL Syntax:

```
   - <rule id="s41-b" ruling="allow">
        <user-category refid="institution" />

        <data-category refid="personal-information" />

        <purpose refid="any-purpose" />

        <action refid="use" />

        <condition refid="for-the-purpose-for-which-it-was-obtained-
          or-compiled-or-for-a-consistent-purpose" />

        <condition refid="standard-of-accuracy" />

        <obligation refid="retention-of-personal-information" />

     </rule>
```

5.2.6 Rule for 41 (c)

Natural Language Text:

41. An institution shall not use personal information in its custody or under its control except, (c) for a purpose for which the information may be disclosed to the institution under section 42 or under section 32 of the Municipal Freedom of Information and Protection of Privacy Act.

Semi-Structured Text

An institution is allowed to use personal information if the data is being used or a purpose for a purpose for which the information may be disclosed to the institution and the institution has taken reasonable steps to ensure that the personal information is accurate yielding an obligation to ensure that proper retention policies are followed.

EPAL Syntax:

```
- <rule id="s41-c" ruling="allow">
    <user-category refid="institution" />

    <data-category refid="personal-information" />

    <purpose refid="any-purpose" />

    <action refid="use" />

    <condition refid="for-a-purpose-for-which-the-information-
      may-be-disclosed-to-the-institution" />

    <condition refid="standard-of-accuracy" />

    <obligation refid="retention-of-personal-information" />

  </rule>
```

5.2.7 Rule for 42(b)

Natural Language Text:

42. An institution shall not disclose personal information in its custody or under its control except, . . . (b) where the person to whom the information relates has identified that information in particular and consented to its disclosure;

Note: here the institution is making the disclosure, but the final recipient can be anyone. The user-category here is “any-user.”

Semi-Structured Text

Any person can have personal information disclosed to them by the institution for any purpose if the person to whom the information relates has identified that information in particular and consented to its disclosure.

EPAL Syntax:

```
- <rule id="s42-b" ruling="allow">
    <user-category refid="any-user" />

    <data-category refid="personal-information" />

    <purpose refid="any-purpose" />

    <action refid="disclosure" />

    <condition refid="disclosure-on-consent" />

  </rule>
```

5.2.8 Rule for 42(c)

Natural Language Text:

42. An institution shall not disclose personal information in its custody or under its control except, . . . (c) for the purpose for which it was obtained or compiled or for a consistent purpose;

Note: here the institution is making the disclosure, but the final recipient can be anyone. The user-category here is “any-user.”

Semi-Structured Text

Any person can have personal information disclosed to them by the institution for any purpose if the purpose for the disclosure is the purpose for which it was obtained or compiled, or for a consistent purpose.

EPAL Syntax:

```
 - <rule id="s42-c" ruling="allow">
      <user-category refid="any-user" />

      <data-category refid="personal-information" />

      <purpose refid="any-purpose" />

      <action refid="disclosure" />

      <condition refid="for-the-purpose-for-which-it-was-obtained-
         or-compiled-or-for-a-consistent-purpose" />

   </rule>
```

5.2.9 Rule for 42(e)

Natural Language Text:

42. An institution shall not disclose personal information in its custody or under its control except, . . . (e) for the purpose of complying with an Act of the Legislature or an Act of Parliament or a treaty, agreement or arrangement thereunder;

Note: here the institution is making the disclosure, but the final recipient can be anyone. The user-category here is “any-user.”

Semi-Structured Text

Any person can have personal information disclosed to them from an institution for any purpose if the disclosure is for the purpose of complying with an Act of the Legislature or an Act of Parliament or a treaty, agreement or arrangement thereunder.

EPAL Syntax:

```
- <rule id="s42-e" ruling="allow">
    <user-category refid="any-user" />

    <data-category refid="personal-information" />

    <purpose refid="any-purpose" />

    <action refid="disclosure" />

    <condition refid="complying-with-an-Act" />

  </rule>
```

5.2.10 Rule for 42(f) i

Natural Language Text:

An institution shall not disclose personal information in its custody or under its control except, . . .(f) where disclosure is by a law enforcement institution, (i) to a law enforcement agency in a foreign country under an arrangement, a written agreement or treaty or legislative authority

Semi-Structured Text

A foreign law enforcement agency can have personal information disclosed to it from a law enforcement institution if the purpose of the disclosure is made under an arrangement, a written agreement or treaty or legislative authority

EPAL Syntax:

```
- <rule id="s42-f-i" ruling="allow">
    <user-category refid="foreign-law-enforcement-agency" />

    <data-category refid="personal-information" />

    <purpose refid="any-purpose" />

    <action refid="disclosure" />
```

```
        <condition refid="disclosure-by-law-enforcement-institution"
          />

        <condition refid="under-an-arrangement" />

      </rule>
```

5.2.11 Rule for 42(f) ii

Natural Language Text:

An institution shall not disclose personal information in its custody or under its control except, . . .(f) where disclosure is by a law enforcement institution, (ii) to another law enforcement agency in Canada;

Semi-Structured Text

A Canadian law enforcement agency is allowed to have personal information disclosed to it by an institution for any purpose if the institution that is disclosing the personal information is a law enforcement institution.

EPAL Syntax:

```
    - <rule id="s42-f-ii" ruling="allow">
        <user-category refid="canadian-law-enforcement-agency" />

        <data-category refid="personal-information" />

        <purpose refid="any-purpose" />

        <action refid="disclosure" />

        <condition refid="disclosure-by-law-enforcement-institution"
          />

      </rule>
```

5.2.12 Rule for 42(g)

Natural Language Text:

An institution shall not disclose personal information in its custody or under its control except, . . . (g) where disclosure is to an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result;

Semi-Structured Text

A Canadian law enforcement agency or institution is allowed to have personal information disclosed to it for any-purpose if the disclosure is to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result;

EPAL Syntax:

```
- <rule id="s42-g" ruling="allow">
      <user-category refid="canadian-law-enforcement-agency" />

      <user-category refid="institution" />

      <data-category refid="personal-information" />

      <purpose refid="any-purpose" />

      <action refid="disclosure" />

      <condition refid="to-aid-an-investigation" />

  </rule>
```

5.2.13 Rule for 42(h)

Natural Language Text:

An institution shall not disclose personal information in its custody or under its control except, . . (h) in compelling circumstances affecting the health or safety of an individual if upon disclosure notification thereof is mailed to the last known address of the individual to whom the information relates;

Semi-Structured Text

Any user is allowed to receive personal information from an institution for the purpose of affecting the health and safety of an individual to whom the information relates if upon disclosure notification thereof is mailed to the last known address of the individual to whom the information relates.

EPAL Syntax:

```
 - <rule id="s42-h" ruling="allow">
     <user-category refid="any-user" />

     <data-category refid="personal-information" />

     <purpose refid="affecting-health-and-safety" />

     <action refid="disclosure" />

     <obligation refid="institution-provides-proper-notice-to-the-
        data-subject-for-disclosure" />

   </rule>
```

5.2.14 Rule for 42(i)

Natural Language Text:

An institution shall not disclose personal information in its custody or under its control except, . . . (i) in compassionate circumstances, to facilitate contact with the next of kin or a friend of an individual who is injured, ill or deceased;

Semi-Structured Text

Any person is allowed to have personal information disclosed to them by an institution for the purposes of facilitating contact if the recipient of the disclosure is next of kin or a friend, the disclosure is under compassionate circumstances, and the individual is injured, ill, or deceased.

EPAL Syntax:

```
- <rule id="DisclosureForCompassionateCircumstances" ruling="allow">
```

```
<short-description>Disclosure For Compassionate Circumstances</short-
   description>

<long-description>(i) in compassionate circumstances, to facilitate contact with
   the next of kin or a friend of an individual who is injured, ill or
   deceased;</long-description>

<user-category refid="NextOfKin" />

<data-category refid="PersonalInformation" />

<purpose refid="CompassionateCircumstances" />

<action refid="Disclosure" />

   </rule>
```

5.2.15 Rule for 42(j)

Natural Language Text:

An institution shall not disclose personal information in its custody or under its control except, . . . (j) to a member of the Legislative Assembly who has been authorized by a constituent to whom the information relates to make an inquiry on the constituent's behalf or, where the constituent is incapacitated, has been authorized by the next of kin or legal representative of the constituent;

Semi-Structured Text

Members of the legislative assembly are allowed to have personal information disclosed to them by an institution for the purposes of making an inquiry on the a constituent’s behalf, if the recipient of the disclosure has been authorized by a constituent, next of kin, or legal representative.

EPAL Syntax:

```
- <rule id="s42-j" ruling="allow">
     <user-category refid="member-of-the-legislative-assembly" />

     <data-category refid="personal-information" />
```

```
      <purpose refid="make-an-inquiry-on-constituents-behalf" />

      <action refid="disclosure" />

      <condition refid="authorized-by-a-constituent-next-of-kin-or-
        legal-representative" />

  </rule
```

5.2.16 Rule for 42(k)

Natural Language Text:

An institution shall not disclose personal information in its custody or under its control except, . . . (k) to a member of the bargaining agent who has been authorized by an employee to whom the information relates to make an inquiry on the employee's behalf or, where the employee is incapacitated, has been authorized by the next-of-kin or legal representative of the employee;

Semi-Structured Text

Bargaining agencies are allowed to have personal information disclosed to them by an institution for the purposes of making an inquiry on the an employee’s behalf, if the recipient of the disclosure has been authorized by the employee, next of kin, or legal representative.

EPAL Syntax:

```
- <rule id="s42-k" ruling="allow">
      <user-category refid="bargaining-agent" />

      <data-category refid="personal-information" />

      <purpose refid="make-an-inquiry-on-employee-behalf" />

      <action refid="disclosure" />

      <condition refid="authorized-by-employee-next-of-kin-or-
        legal-representative" />
```

```
    </rule>
```

5.2.17 Rule for 42(l)

Natural Language Text:

An institution shall not disclose personal information in its custody or under its control except, . . . (l) to the responsible minister;

Semi-Structured Text

The responsible minister is allowed to have personal information disclosed to him or her by an institution for any purpose.

EPAL Syntax:

```
  - <rule id="s42-l" ruling="allow">
      <user-category refid="responsible-minister" />

      <data-category refid="personal-information" />

      <purpose refid="any-purpose" />

      <action refid="disclosure" />

    </rule>
```

5.2.18 Rule for 42(m)

Natural Language Text:

An institution shall not disclose personal information in its custody or under its control except, . . . (m) to the Information and Privacy Commissioner;

Semi-Structured Text

The Privacy Commissioner is allowed to have personal information disclosed to him or her by an institution for any purpose.

EPAL Syntax:

```
- <rule id="s42-m" ruling="allow">
     <user-category refid="information-and-privacy-commissioner"
        />

     <data-category refid="personal-information" />

     <purpose refid="any-purpose" />

     <action refid="disclosure" />

  </rule>
```

5.2.19 Rule for 42(n)

Natural Language Text:

An institution shall not disclose personal information in its custody or under its control except, . . . (n) to the Government of Canada in order to facilitate the auditing of shared cost programs.

Semi-Structured Text

The Government of Canada is allowed to have personal information disclosed to it by an institution for the purpose of facilitating the auditing of shared cost programs.

EPAL Syntax:

```
- <rule id="s42-n" ruling="allow">
     <user-category refid="government-of-canada" />

     <data-category refid="personal-information" />

     <purpose refid="facilitating-the-auditing-of-shared-cost-
        programs" />

     <action refid="disclosure" />

  </rule>
```

5.2.20 Rule for section 44

Natural Language Text:

44. A head shall cause to be included in a personal information bank all personal information under the control of the institution that is organized or intended to be retrieved by the individual's name or by an identifying number, symbol or other particular assigned to the individual.

Semi-structured Text:

The head of an institution may perform any action on identifiable personal information for the purpose of creating a personal information bank.

EPAL Rule:

```
      <rule id="s44">
            <user-category refid="head-of-institution" ></user-
category>
            <data-category refid="identifiable-personal-information" />
            <purpose refid="creation-of-personal-information-bank" />
            <action refid="Use" />
      </rule>
```

5.2.21 Rule for section 45

Natural Language:

45. The responsible minister shall publish at least once each year an index of all personal information banks setting forth, in respect of each personal information bank,

(a) its name and location;

(b) the legal authority for its establishment;

(c) the types of personal information maintained in it;

(d) how the personal information is used on a regular basis;

(e) to whom the personal information is disclosed on a regular basis;

(f) the categories of individuals about whom personal information is maintained; and

(g) the policies and practices applicable to the retention and disposal of the personal information.

Semi-structured text:

The responsible minister may use general records for the purpose of publishing an index of personal information banks providing that it has been within 1 year of the last index.

EPAL Rule:

```
      <rule id="s45">
            <user-category refid="responsible-minister" />
            <data-category refid="general-records" />
            <purpose refid="publish-index-of-personal-information-
banks" />
            <action refid="Use" ></action>
            <condition refid="within-1-year-of-last-index" />
      </rule>
```

5.2.22 Rule for section 46(1)

Natural Language Text:

46. (1) A head shall attach or link to personal information in a personal information bank,

(a) a record of any use of that personal information for a purpose other than a purpose described in clause 45(d); and

(b) a record of any disclosure of that personal information to a person other than a person described in clause 45(e).

Semi-structured text:

The head of an institution may create a record of use or disclosure of personal information for any purpose if the use or disclosure is inconsistent with the criteria in 45(d) and 45(e).

EPAL Syntax:

```
      <rule id="s46-1">
            <user-category refid="head-of-institution" />
            <data-category refid="identifiable-personal-information" />
            <action refid="record-use-or-disclosure" />
            <condition refid="inconsistent-with-section-45-d-and-e" />
      </rule>
```

5.2.23 Rule for section 46(3)

Natural Language Text:

(3) Where the personal information in a personal information bank under the control of an institution is used or disclosed for a use consistent with the purpose for which the information was obtained or compiled by the institution but the use is not one of the uses included under clauses 45(d) and (e), the head shall,

(a) forthwith notify the responsible minister of the use or disclosure; and

(b) ensure that the use is included in the index.

Semi-structured Text:

The head of an institution may use general records for the purpose of notifying the responsible minister in order to update the personal information index if the use or disclosure is unusual but consistent with the purposes for which it was collected.

EPAL syntax:

```
      <rule id="s46-3">
            <user-category refid="head-of-institution" />
            <data-category refid="general-records" ></data-category>
            <purpose refid="notify-responsible-minister-to-update-
index" />
            <action refid="Use" />
            <condition refid="inconsistent-with-section-45-d-and-e" />
      </rule>
```

5.2.24 Rule for section 47(1)

Natural Language Text

47. (1) Every individual has a right of access to,

(a) any personal information about the individual contained in a personal information bank in the custody or under the control of an institution; and

(b) any other personal information about the individual in the custody or under the control of an institution with respect to which the individual is able to provide sufficiently specific information to render it reasonably retrievable by the institution.

Semi-structured Text:

An institution may disclose identifiable personal information for any purpose if the data is about the recipient, the access request criteria are met, and the head of the institution does not exercise any exemptions allowed in section 49. If data is disclosed, it must be disclosed according to the criteria for proper manner of disclosure.

5.2.25 Rule for 47-2

Natural Language Text

(2) Every individual who is given access under subsection (1) to personal information is entitled to,

(a) request correction of the personal information where the individual believes there is an error or omission therein;

(b) require that a statement of disagreement be attached to the information reflecting any correction that was requested but not made; and

(c) require that any person or body to whom the personal information has been disclosed within the year before the time a correction is requested or a statement of disagreement is required be notified of the correction or statement of disagreement.

Semi-structured Text:

An institution may use personal information to respond to a correction request and if so it must notify recipients and users of the information within the past year of the correction response.

EPAL Statement:

```
      <rule id="s47-2">
            <user-category refid="institution" />
            <data-category refid="personal-information" />
            <purpose refid="respond-to-correction-request" ></purpose>
            <action refid="Use" />
            <obligation refid="notification-of-correction-
request"></obligation>
```

```
    </rule>
```

6 Test Disclosure Scenario

At the FIPPA workshop, the following scenario was used to validate the FIPPA policy rules:

6.1 Scenario Description

Ministry X has implemented a Clean Driving program. The purpose of the program is to detect and reduce smog-related emissions from cars, trucks and buses. Light duty vehicles (cars, small vans, sport utility vehicles, and light trucks) must bring their vehicle into a Clean Driving facility (i.e. garage) to pass an emissions test every two years in order to obtain a new license plate sticker.

Ministry X maintains a database that includes:

- Gas emission results of every vehicle tested in the program
- Vehicle identification number for each vehicle tested in the program
- License plate number for each vehicle tested in the program
- Name, address and phone number of each vehicle owner
- Vehicle inspection certification numbers. These are unique numbers assigned to individual vehicle owners in the context of the emissions testing process.
- Garage identifiers, which is a four-digit number assigned to a Clean Driving facility

6.2 Request 1

Ministry X has received a freedom of information request from a member of the public, who wants access to the entire database.

This is request is covered by Part II of the Act, which was outside of the scope of the workshop, but the workshop participants briefly outlined how the procedures defined in Part II would apply to the request.

Section 24 defines how and under what circumstances a Freedom Of Information request can be made.

Section 25 discusses the procedures for forwarding a request to the correct institution.

Section 26 describes how the institution that deals with the request, shall within 30 of receiving the request, give written notice to the requestor that they are going to give the data or not.

Section 27 gives conditions for extending the deadlines for responding to the request.

Section 21 defines how personal information should be handled with respect to Freedom Of Information requests.

Overall, none of the sections in Part III of the Act are incorporated into the procedures for Freedom of Information requests outlined in Part II.

6.3 Request 2

Ministry X has also received an informal request from a private-sector company, which wants to negotiate an agreement to purchase the database on an annual basis.

The ministry is going to need to judge this disclosure under part III of the Act, in order to ensure that it won't be subject to the privacy complaints after the disclosure.

First step, examine all the requested elements and determine which are personal information. In this scenario, the elements that are likely fall under the Act's definition of personal information are:

- License plate number for each vehicle tested in the program
- Name, address and phone number of each vehicle owner
- Vehicle inspection certification numbers. These are unique numbers assigned to individual vehicle owners in the context of the emissions testing process.

In EPAL, it's possible to define multiple categories of personal information, which have different rules applied to each category. But in Part III of the Act, there is effectively only one category of data, called "personal information." So in this case, all of the personal information elements are treated the same way, so only one decision has to be made.

In cases where the data elements that are being requested fall into different policy defined data categories, each element would have to be judged independently.

6.3.1 Evaluating the Request

The first decision that the ministry would have to make is whether or not the request falls into the section 37 rules.

For purposes, of the scenario, we assumed that the ministry in question is not collecting the data for the purpose of making or creating a record that is available to the general public.

This corresponds to the “s37” EPAL rule. When this rule is evaluated in an EPAL engine, it would ask the following questions:

- Does the requestor fall into the “any-user” category? (yes)
- Does the requested information fall into the category of “personal information” (yes)
- Does the request fall into the “any purpose” category? (yes)
- Is the requested action a “disclosure”? (yes)
- Is the condition “for the purpose of making creating a record that is available to the general public” true? (no)

Based on the above questions, this rule would not be used to generate a ruling for the request.

The next step that the ministry would likely follow in the process is to evaluate the request against section 42, which further defines allowable disclosures.

Section 42, says that disclosures should not be allowed, except under specific exceptions. The ministry would look through 42 exceptions and would probably conclude that none of the exceptions apply to this scenario.

Because none of the exceptions to denying the disclosure apply, the ministry would conclude that the request should be denied. (Or, at least, none of the elements that are categorized as personal information should be released.)

An EPAL engine, would first, consider rules “s38-2-no-notice” and “s38-2” because these are next in the policy file. These rules cover section 38 and 39 of The Act which covers the collection of data and the corresponding notices associated with data collection. However, in both of these rules, the EPAL engine will ask if the action is a “collection” of data. In this case, the action is not a collection, but a disclosure, so the EPAL engine would not apply these rules to the decision.

Next, an EPAL engine would evaluate the three “s41” rules in the policy because they are next in the list of rules. One of the questions that the EPAL engine would ask when evaluating this scenario is “Does this request fall into the action definition of ‘use’?” In this case, the action is a disclosure, not a usage, so these three rules would not apply to the request.

The EPAL engine would then start through all of the 19 section 42 rules that are in the policy.

The EPAL engine would not apply rule s42-b, because the condition “disclosure on consent” would not be true.

The EPAL engine would not apply rule s42-c, because the condition “for-the-purpose-for-which-it-was-obtained-or-compiled-or-for-a-consistent-purpose” would not be true.

The EPAL engine would not apply rule s42-e, because the condition “complying-with-an-Act” would not be true.

The EPAL engine would not apply rule s42-f-I, because the recipient of the data would not fall into the category of “foreign-law-enforcement-agency.”

The EPAL engine would not apply rule, “s42-f-ii,” because the recipient of the data would not fall into the category of “canadian-law-enforcement-agency.”

The EPAL engine would not apply rule “s42-g”, also because the recipient of the data would not fall into the category of “canadian-law-enforcement-agency.”

The EPAL engine would not apply rule “s42-h” because the purpose of the request does not match the definition of “affecting-health-and-safety.”

The EPAL engine would not apply rule “s42-i,” because the purpose of the request does not match the definition of “to-facilitate-contact-with-the-next-of-kin-or-a-friend.”

The EPAL engine would not apply rule “s42-j,” because the recipient of the data does not fall into the category of “member-of-the-legislative-assembly.”

The EPAL engine would not apply rule "s42-k," because the recipient of the data does not fall into the category "bargaining-agent."

The EPAL engine would not apply rule "s42-l," because the recipient of the data does not fall into the category "responsible minister."

The EPAL engine would not apply rule "s42-m," because the recipient of the data does not fall into the category of "information and privacy commissioner."

Finally, the EPAL engine would not apply rule "s42-n," because the recipient of the data does not fall into the category of "government-of-canada."

At this point, the EPAL engine has looked at all of the rules in its policy and found no rules that apply to this scenario. This is similar to the ministry making a decision that none of the exceptions in section 42 apply to the request.

Because none of the rules in the EPAL policy apply to the request, the policy's default ruling is applied. Because the presumption of Part II is that requests should be denied unless specifically allowed, the default ruling for the EPAL policy is "deny." So the EPAL engine would return a "deny" as the ruling for the request in this scenario.

7 Conclusion

Based on the evaluation of the test scenario, the EPAL policy for part II of FIPPA generated the same ruling that the hypothetical ministry is likely to have made. And in general, the process and the types of questions that the EPAL engine would have asked are the same sorts of questions that the ministry would have asked as well.

So our conclusion is that the EPAL policy rules for FIPPA that were developed in the workshop generally reflect the same process that the ministry would have to go through in evaluating a disclosure request.

While developing the EPAL vocabulary and policy for FIPPA, several areas of improvement for the EPAL specification were identified. These are documented in "Appendix: Lessons Learned for EPAL" below.

8 Next Steps

The next steps for this joint project is to take the EPAL policy that has been developed in the workshop to an existing ministry and compare these rules against data to day use, collection, and disclosure procedures that the ministry has in place.

There will be two parts of this work. First, we will need to refine the vocabulary generated in the workshop to extend with ministry specific concepts. For example, we'll need to identify ministry specific purposes for using and collecting data, we'll need to enumerate the specific types of data that ministry collects and holds and relate it to the "personal data category" of the current EPAL vocabulary.

The second part of this work will be to use the refined vocabulary and the FIPPA policy and test it against some existing procedures and disclosure requests that the ministry has to handle so see if the process the EPAL policy would suggest matches reasonably closely to the decision making processes in the ministry.

9 References

[IPC Report] – Information and Privacy Commisioner/Ontario, 1995 Annual Report, p. 5,

http://www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=13337&N_ID=1&PT_ID=11137&U_ID=0

[FIPPA] The full text of the Ontario Freedom of Information and Protection of Privacy Act can be found at:
http://www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=11607&U_ID=0&N_ID=1

[EPAL] The latest specification for the Enterprise Privacy Authorization Language can be found at:

http://www.zurich.ibm.com/security/enterprise-privacy/epal/

10 Appendix: Lessons Learned for EPAL

From discussions about the Act and the workshop exercises, several issues were identified with the EPAL 1.1 specification that should be considered for future revisions of the specification.

10.1 Disclosures Are Often Workflows

In most scenarios where personal data is being used or disclosed in a government environment, the evaluation of the request is done before the data access request is even made. The reason for this is that the conditions that need to be checked, i.e., the questions about the request that have to be answered, require human evaluation and discretion.

While this has no direct bearing on the EPAL language specification, it is relevant to designing EPAL based products.

10.2 Categories Are Sometimes Conditional

In the current EPAL specification, user categories, data categories, action categories and purpose categories are just labels that are applied to characteristics of a data access request.

However, sometimes the policy being implemented creates conditional definitions for these concepts. For example, the FIPPA Act defines personal information only to people who are currently living or who have been dead for more than 30 years. So there is a condition that has to be checked at the time the data access request is made in order to determine if the data being requested falls into the category of “personal information.”

These conditions could be expressed as conditions attached to rules, however, management of these conditions would become cumbersome because they would apply to all rules that involve the affected vocabulary element.

One possibility would be to allow conditions to be attached to vocabulary elements. However, this would significantly change the semantics of the EPAL engine.

10.3 Both Access Entity and Recipient Entity Are Relevant

Currently, the EPAL syntax only identifies a category for “data user.” But in several parts of the act, both the entity that does the disclosure *and* the entity that is the recipient need to be know.

Section 42 (f) (i) is a good example. In this part of the Act, the entity making the disclosure must be a law enforcement institution and the recipient of the data must be a foreign law enforcement agency.

The EPAL syntax could be expanded to include a "recipient" element to the rules in parallel with the "data-user" element of the rules. However, a more general solution might be to allow for the policy itself to define the elements of the rules. This would give EPAL broader applicability for data handling practices beyond just privacy policies.

10.4 Support Needed for Non-Standard Functions

Because the goal of EPAL is to mirror the concepts found in natural language text, there is sometimes the need for operations on data that can't be expressed in formal mathematical notation.

For example, the FIPPA Act refers to concepts such as "a purpose consistent with" the purpose for which the data was originally collected. There is not logical or mathematical operation for "is consistent with."

So the EPAL syntax needs to provide ways for defining new operations that can be used to capture these semantics in the policy and EPAL engines that are developed need to provide ways for customers to supply implementations of these new operations.

Building on the example above, the policy needs to provide for the ability to define a function that takes two purpose labels and evaluate whether or not they are "consistent" purposes. The implementation of this function that is plugged into the EPAL engine would likely consult a table of purpose associations that have been established by precedent and case law as being "consistent" with each other.

This is a good example of EPAL policies being used to standardize the parts of the decision making process to activities that can be standardized, while consulting with decision makers in cases where human evaluation is needed.

10.5 Context Attributes Need to Be Multi-Valued

When data is collected from an individual, there may be multiple purposes associated with a "purpose for collection" field on a record. All of these need to be considered when future uses of the data are evaluated as to whether they are for the same or a "consistent" purpose. Therefore the EPAL syntax for container attributes needs to provide for the possibility that there may be multiple values for an attribute and there needs to be suitable operations for using multi-values attributes. ("set" functions, "bag" functions, etc.)

11 Appendix: Complete FIPPA Vocabulary

```
  <?xml version="1.0" encoding="UTF-8" ?>
- <epal-vocabulary xmlns="http://www.research.ibm.com/privacy/epal"
    xmlns:xacml="urn:oasis:names:tc:xacml:1.0:policy"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.research.ibm.com/privacy/epal
    C:\work\ipc\schema\epal.xsd">

  - <vocabulary-information id="foippa-v1">

      <version-info start-date="2003-10-07T00:00:00" revision-
        number="1" last-modified="2003-10-07T00:00:00" />

    </vocabulary-information>

  - <user-category id="requester">

      <short-description>A requester is a person who has requested
        access to a government-held record under the access
        scheme in Part II of FIPPA.</short-description>

      <long-description>A requester is a person who has requested
        access to a government-held record under the access
        scheme in Part II of FIPPA. The term “requester” does not
        appear anywhere in FIPPA. However, section 10(1), which
        is in Part II, gives “every person” a right of access to a
        record or part of a record subject to certain exceptions.
        Section 42(a) permits an institution to disclose personal
        information in accordance with Part II of FIPPA.</long-
        description>

    </user-category>

  - <user-category id="affected-party">

      <short-description>An affected party is a person whose
        interests may be affected by the disclosure of his or her
        personal information.</short-description>

      <long-description>An affected party is a person whose
        interests may be affected by the disclosure of his or her
```

```
          personal information. In the context of privacy, section
          28(1)(b) states that before a head grants a request for
          access to a record that is personal information that the
          head has reason to believe might constitute an unjustified
          invasion of personal privacy for the purposes of clause
          21(1)(f), the head shall give written notice in accordance
          with subsection (2) to the person to whom the
          information relates.</long-description>

    </user-category>

  - <user-category id="data-subject">

       <short-description>The data subject is the person to whom
          the personal information relates.</short-description>

       <long-description>The data subject is the person to whom the
          personal information relates. The term “data subject”
          does not appear in FIPPA. However, section 42(b) permits
          an institution to disclose personal information where the
          person to whom the information relates has identified
          that information in particular and consented to its
          disclosure.</long-description>

    </user-category>

  - <user-category id="public-servant">

       <short-description>An officer or employee of the institution is
          a public servant.</short-description>

       <long-description>Section 42(d) permits an institution to
          disclose personal information where disclosure is made to
          an officer or employee of the institution who needs the
          record in the performance of his or her duties and where
          disclosure is necessary and proper in the discharge of the
          institution's functions.</long-description>

    </user-category>

  - <user-category id="law-enforcement-institution">
```

```
    <short-description>A law enforcement institution refers to a
      police service or any body that falls within the definition
      in section 2(1).</short-description>

    <long-description>Section 2(1) defines “ law enforcement” as
      (a) policing, (b) investigations or inspections that lead or
      could lead to proceedings in a court or tribunal if a
      penalty or sanction could be imposed in those
      proceedings, and (c) the conduct of proceedings referred
      to in clause (b). Section 42(f) permits an institution to
      disclose personal information where disclosure is by a law
      enforcement institution, (i) to a law enforcement agency
      in a foreign country under an arrangement, a written
      agreement or treaty or legislative authority, or (ii) to
      another law enforcement agency in Canada. Section 42(g)
      permits an institution to disclose personal information
      where disclosure is to an institution or a law enforcement
      agency in Canada to aid an investigation undertaken with
      a view to a law enforcement proceeding or from which a
      law enforcement proceeding is likely to result.</long-
      description>

  </user-category>

- <user-category id="Next-of-kin-or-friend">

    <short-description>The next of kin may be a family member of
      an injured, ill or deceased person. A friend is a close
      associate to a person.</short-description>

    <long-description>Section 42(i) permits an institution to
      disclose personal information where disclosure is in
      compassionate circumstances, to facilitate contact with
      the next of kin or a friend of an individual who is injured,
      ill or deceased.</long-description>

  </user-category>

- <user-category id="member-of-the-legislative-assembly">

    <short-description>A member of the Legislative Assembly is
      an elected member of Ontario’s provincial
      parliament.</short-description>
    <long-description>Section 42(j) permits an institution to
       disclose personal information where disclosure is to a
       member of the Legislative Assembly who has been
       authorized by a constituent to whom the information
       relates to make an inquiry on the constituent's behalf or,
       where the constituent is incapacitated, has been
       authorized by the next of kin or legal representative of
       the constituent.</long-description>

  </user-category>

- <user-category id="bargaining-agent">

    <short-description>A bargaining agent is a person or entity
       that represents and acts for others, usually in collective
       bargaining negotiations between unions and
       management.</short-description>

    <long-description>Section 42(k) permits an institution to
       disclose personal information where disclosure is to a
       member of the bargaining agent who has been authorized
       by an employee to whom the information relates to make
       an inquiry on the employee's behalf or, where the
       employee is incapacitated, has been authorized by the
       next-of-kin or legal representative of the
       employee.</long-description>

  </user-category>

- <user-category id="responsible-minister">

    <short-description>The responsible minister is a member of
       cabinet who is responsible for the purposes of the
       Freedom of Information and Protection of Privacy
       Act.</short-description>

    <long-description>Section 2(1) defines “responsible minister"
       as the minister of the Crown who is designated by order
       of the Lieutenant Governor in Council under section 3.
       Section 42(l) permits an institution to disclose personal
       information where disclosure is to the responsible
       minister.</long-description>
  </user-category>
- <user-category id="information-and-privacy-commissioner">
    <short-description>The Information and Privacy
      Commissioner (IPC) is the person responsible for
      overseeing enforcement of FIPPA in Ontario.</short-
      description>
    <long-description>Section 2(1) defines "Information and
      Privacy Commissioner" and "Commissioner" as the
      Commissioner appointed under subsection 4(1). Section
      42(m) permits an institution to disclose personal
      information where disclosure is to the Information and
      Privacy Commissioner.</long-description>
  </user-category>
- <user-category id="government-of-canada">
    <short-description>The Government of Canada refers to the
      federal government.</short-description>
    <long-description>Section 42(n) permits an institution to
      disclose personal information where disclosure is to the
      Government of Canada in order to facilitate the auditing of
      shared cost programs.</long-description>
  </user-category>
  <user-category id="any-user" />
- <user-category id="canadian-law-enforcement-agency">
    <short-description>law enforcement agency that is not an
      institution in terms of Ontario Gov't</short-description>
    <long-description>see definition in section 2</long-description>
  </user-category>
  <user-category id="foreign-law-enforcement-agency" />
```

```
- <user-category id="institution">
    <long-description>2(1) "institution" means, (0.a) the
      Assembly; (a) a ministry of the Government of Ontario,
      and (b) any agency, board, commission, corporation or
      other body designated as an institution in the
      regulations;</long-description>
  </user-category>
- <data-category id="general-records">
    <short-description>These records contain information relating
      to the activities of government, ranging from
      administration and operations to legislation and policy.
      They do not include personal information.</short-
      description>
    <long-description />
  </data-category>
- <data-category id="personal-information">
    <short-description>These records contain personal
      information,</short-description>
    <long-description>These records contain personal
      information, which defined in section 2(1) as recorded
      information about an identifiable individual, including: (a)
      information relating to the race, national or ethnic origin,
      colour, religion, age, sex, sexual orientation or marital or
      family status of the individual, (b) information relating to
      the education or the medical, psychiatric, psychological,
      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, telephone number, fingerprints or blood type
      of the individual, (e) the personal opinions or views of the
      individual except where they relate to another individual,
      (f) correspondence sent to an institution by the individual
      that is implicitly or explicitly of a private or confidential
```

```
          nature, and replies to that correspondence that would
          reveal the contents of the original correspondence, (g)
          the views or opinions of another individual about the
          individual, and (h) the individual's name where it appears
          with other personal information relating to the individual
          or where the disclosure of the name would reveal other
          personal information about the individual. This category
          also includes orally collected information as defined in 38.
          (1) .</long-description>

    </data-category>

  - <purpose id="complying-with-an-access-request">

      <short-description>If an institution receives a request for
          access to personal information, it must follow the access
          rules in Part II of FIPPA. Section 42(a) permits an
          institution to disclose personal information in accordance
          with Part II of FIPPA.</short-description>

      <long-description />

    </purpose>

  - <purpose id="performing-government-business">

      <short-description>An institution may use or disclose personal
          information for the purpose of performing government
          business.</short-description>

      <long-description>Section 41(b) permits an institution to use
          personal information for the purpose for which it was
          obtained or compiled or for a consistent purpose. Section
          42(c) permits an institution to disclose personal
          information for the purpose for which it was obtained or
          compiled or for a consistent purpose. Section 42(d)
          permits an institution to disclose personal information
          where disclosure is made to an officer or employee of the
          institution who needs the record in the performance of his
          or her duties and where disclosure is necessary and
          proper in the discharge of the institution's functions.
          Section 42(e) permits an institution to disclose personal
          information for the purpose of complying with an Act of
      the Legislature or an Act of Parliament or a treaty,
      agreement or arrangement thereunder.</long-description>

  </purpose>

- <purpose id="law-enforcement">

    <long-description>An institution may disclose personal
      information for the purposes of law enforcement. Section
      42(f) permits an institution to disclose personal
      information where disclosure is by a law enforcement
      institution, (i) to a law enforcement agency in a foreign
      country under an arrangement, a written agreement or
      treaty or legislative authority, or (ii) to another law
      enforcement agency in Canada. Section 42(g) permits an
      institution to disclose personal information where
      disclosure is to an institution or a law enforcement
      agency in Canada to aid an investigation undertaken with
      a view to a law enforcement proceeding or from which a
      law enforcement proceeding is likely to result.</long-description>

  </purpose>

- <purpose id="affecting-health-and-safety">

    <long-description>An institution may disclose personal
      information for the purpose of protecting an individual’s
      health and safety. Section 42(h) permits an institution to
      disclose personal information in compelling circumstances
      affecting the health or safety of an individual if upon
      disclosure notification thereof is mailed to the last known
      address of the individual to whom the information
      relates.</long-description>

  </purpose>

- <purpose id="contacting-a-party-for-compassionate-
    circumstances">

    <short-description>An institution may disclose personal
      information for the purpose of contacting a party in
      compassionate circumstances.</short-description>
    <long-description>Section 42(h) permits an institution to
       disclose personal information in compassionate
       circumstances, to facilitate contact with the next of kin or
       a friend of an individual who is injured, ill or
       deceased.</long-description>
  </purpose>
- <purpose id="dealing-with-access-appeals-and-privacy-
    complaints">
    <long-description>The IPC requires access to records
       containing personal information in order to mediate and
       adjudicate access appeals and conduct privacy
       investigations. Section 42(m) permits an institution to
       disclose personal information where disclosure is to the
       Information and Privacy Commissioner.</long-description>
  </purpose>
- <purpose id="facilitating-ministerial-responsibility">
    <long-description>Government ministers are ultimately
       accountable and responsible for what happens in their
       institutions and may require personal information for the
       purpose of fulfilling their duties. Section 42(l) permits an
       institution to disclose personal information to the
       responsible minister.</long-description>
  </purpose>
  <purpose id="make-an-inquiry-on-constituent’s-behalf" />
- <purpose id="facilitating-the-auditing-of-shared-cost-programs">
    <long-description>The responsible minister is a member of
       cabinet who is responsible for the purposes of the
       Freedom of Information and Protection of Privacy Act.
       Section 42(l) permits an institution to disclose personal
       information to the responsible minister.</long-description>
  </purpose>
  <purpose id="make-an-inquiry-on-employee-behalf" />
- <action id="collection">
    <short-description>The rules governing the collection of
      personal information are found in sections sections 38(2)
      and 39.</short-description>
    <long-description />
  </action>
- <action id="Use">
    <short-description>The rules governing the use of personal
      information are found in sections 41 and 43.</short-
      description>
  </action>
- <action id="disclosure">
    <short-description>The rules governing the disclosure of
      personal information are found in sections 42 and
      43.</short-description>
  </action>
- <action id="retention">
    <short-description>The rules governing the retention of
      personal information are found in section 40.</short-
      description>
  </action>
- <action id="disposal">
    <short-description>The rules governing the disposal of
      personal information are found in section 40(4) and
      Regulation 459.</short-description>
  </action>
- <obligation id="providing-proper-notice-to-the-data-subject-for-collection">
    <short-description />
    <long-description>Section 39(2) states that where personal information is collected on behalf of an institution, the head shall, unless notice is waived by the responsible minister, inform the individual to whom the information relates of, (a) the legal authority for the collection; (b) the principal purpose or purposes for which the personal information is intended to be used; and (c) the title, business address and business telephone number of a public official who can answer the individual's questions about the collection.</long-description>
    <parameter id="p1" simpleType="http://www.w3.org/2001/XMLSchema#boolean" />
  </obligation>
- <obligation id="institution-provides-proper-notice-to-the-data-subject-for-disclosure">
    <short-description />
    <long-description>Section 42(h) permits an institution to disclose personal information in compelling circumstances affecting the health or safety of an individual if upon disclosure notification thereof is mailed to the last known address of the individual to whom the information relates.</long-description>
    <parameter id="p2" simpleType="http://www.w3.org/2001/XMLSchema#boolean" />
  </obligation>
- <obligation id="Providing-data-subject-access-to-own-data">
```

```
    <long-description>Retention – Providing the data subject with
      an opportunity to access his/her own personal
      information Section 40(1) requires that personal
      information that has been used by an institution be
      retained after use by the institution for the period
      prescribed by regulation in order to ensure that the
      individual to whom it relates has a reasonable opportunity
      to obtain access to the personal information. Section 5(1)
      of Regulation 460 requires that personal information used
      by an institution be retained for at least one year after
      use unless the individual to whom the information relates
      consents to its earlier disposal.</long-description>

    <parameter id="p3"
      simpleType="http://www.w3.org/2001/XMLSchema#bool
      ean" />

  </obligation>

- <obligation id="Maintaining-a-disposal-record">

    <long-description>Section 6(1) of Regulation 459 requires
      every head of an institution to ensure that the institution
      maintains a disposal record setting out what personal
      information has been destroyed or transferred to the
      Archives and the date of that destruction or
      transfer.</long-description>

    <parameter id="p4"
      simpleType="http://www.w3.org/2001/XMLSchema#bool
      ean" />

  </obligation>

- <obligation id="Keeping-personal-information-out-of-the-
    disposal-record">

    <long-description>Section 6(2) requires that the head ensure
      that the disposal record maintained under subsection (1)
      does not contain personal information.</long-description>
    <parameter id="p5"
      simpleType="http://www.w3.org/2001/XMLSchema#bool
      ean" />

  </obligation>

- <obligation id="retention-of-personal-information">



    <parameter id="p6"
      simpleType="http://www.w3.org/2001/XMLSchema#bool
      ean" />

  </obligation>

- <obligation id="disposal">

    <long-description>(4) A head shall dispose of personal
      information under the control of the institution in
      accordance with the regulations. 1989, c. 64, s. 3(15).
      See regulation 459 section 2, 3, 4, and 5</long-description>

    <parameter id="p7"
      simpleType="http://www.w3.org/2001/XMLSchema#bool
      ean" />

  </obligation>

</epal-vocabulary>
```

12 Appendix: Complete FIPPA Policy

```
  <?xml version="1.0" encoding="UTF-8" ?>
- <epal-policy xmlns="http://www.research.ibm.com/privacy/epal"
    xmlns:xacml="urn:oasis:names:tc:xacml:1.0:policy"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.research.ibm.com/privacy/epal
    C:\work\ipc\schema\epal.xsd" default-ruling="deny">

  - <policy-information id="fippa-policy">
```

```
    <version-info start-date="2003-10-10T00:00:00" revision-
      number="1" last-modified="2003-10-10T00:00:00" />
  </policy-information>
  <epal-vocabulary-ref id="fippa-vocab" location="" />
- <condition id="maintained-for-purpose-of-making-public">
    <long-description>Further interpretation of the law has added
      the requirement that the institution intending to rely on
      this provision be the one that is maintaining the personal
      information for the purpose of creating a record that is
      available to the general public.</long-description>
    <evaluates-container refid="x" />
  - <!--
    -->
    <xacml:Condition FunctionId="" />
  </condition>
- <condition id="condition-for-proper-collection">
    <long-description>(2) No person shall collect personal
      information on behalf of an institution unless the
      collection is expressly authorized by statute, used for the
      purposes of law enforcement or necessary to the proper
      administration of a lawfully authorized activity.</long-
      description>
    <evaluates-container refid="x" />
    <xacml:Condition FunctionId="" />
  </condition>
- <condition id="proper-manner-of-collection">
```

```
      <long-description>39. (1) Personal information shall only be
         collected by an institution directly from the individual to
         whom the information relates unless, (a) the individual
         authorizes another manner of collection; (b) the personal
         information may be disclosed to the institution concerned
         under section 42 or under section 32 of the Municipal
         Freedom of Information and Protection of Privacy Act; (c)
         the Commissioner has authorized the manner of collection
         under clause 59(c); (d) the information is in a report from
         a reporting agency in accordance with the Consumer
         Reporting Act; (e) the information is collected for the
         purpose of determining suitability for an honour or award
         to recognize outstanding achievement or distinguished
         service; (f) the information is collected for the purpose of
         the conduct of a proceeding or a possible proceeding
         before a court or tribunal; (g) the information is collected
         for the purpose of law enforcement; or (h) another
         manner of collection is authorized by or under a
         statute.</long-description>

      <evaluates-container refid="x" />

      <xacml:Condition FunctionId="" />

   </condition>

 - <condition id="proper-notice-to-individual">

      <long-description>s. 39(2) (2) Where personal information is
         collected on behalf of an institution, the head shall, unless
         notice is waived by the responsible minister, inform the
         individual to whom the information relates of, (a) the
         legal authority for the collection; (b) the principal purpose
         or purposes for which the personal information is
         intended to be used; and (c) the title, business address
         and business telephone number of a public official who
         can answer the individual's questions about the
         collection.</long-description>

      <evaluates-container refid="x" />

      <xacml:Condition FunctionId="" />
```

```
    </condition>
  - <condition id="proper-exceptions-to-notice-obligation">
      <long-description>s. 39(3) (3) Subsection (2) does not apply
         where the head may refuse to disclose the personal
         information under subsection 14 (1) or (2) (law
         enforcement), section 14.1 (Remedies for Organized
         Crime and Other Unlawful Activities Act, 2001) or section
         14.2 (Prohibiting Profiting from Recounting Crimes Act,
         2002). or unless notice is waived by the responsible
         minister as described in 39(2)</long-description>
      <evaluates-container refid="x" />
      <xacml:Condition FunctionId="" />
    </condition>
  - <condition id="disclosure-on-consent">
      <long-description>(b) where the person to whom the
         information relates has identified that information in
         particular and consented to its disclosure;</long-
         description>
      <evaluates-container refid="x" />
      <xacml:Condition FunctionId="" />
    </condition>
  - <condition id="disclosure-purpose-same-or-consistent-with-
      collection-purpose">
      <long-description>for the purpose for which it was obtained
         or compiled or for a consistent purpose;</long-description>
      <evaluates-container refid="x" />
      <xacml:Condition FunctionId="" />
  </condition>
- <condition id="complying-with-an-Act">
    <long-description>(e) for the purpose of complying with an
      Act of the Legislature or an Act of Parliament or a treaty,
      agreement or arrangement thereunder;</long-description>
    <evaluates-container refid="x" />
    <xacml:Condition FunctionId="" />
  </condition>
- <condition id="disclosure-by-law-enforcement-institution">
    <long-description>See section 2 for definition</long-
      description>
    <evaluates-container refid="x" />
    <xacml:Condition FunctionId="" />
  </condition>
- <condition id="under-an-arrangement">
    <long-description>s. 42(f)(i) permits a law enforcement
      institution to disclose personal informaton to a law
      enforcement agency in a foreign country under an
      arrangement, a written agreement or treaty or legislative
      authority.</long-description>
    <evaluates-container refid="x" />
    <xacml:Condition FunctionId="" />
  </condition>
- <condition id="to-aid-an-investigation">
```

```
      <long-description>(g) where disclosure is to an institution or
         a law enforcement agency in Canada to aid an
         investigation undertaken with a view to a law
         enforcement proceeding or from which a law enforcement
         proceeding is likely to result;</long-description>

      <evaluates-container refid="x" />

      <xacml:Condition FunctionId="" />

   </condition>

 - <condition id="individual-is-injured-ill-or-deceased">

      <long-description>Section 42(h) permits an institution to
         disclose personal information in compassionate
         circumstances, to facilitate contact with the next of kin or
         a friend of an individual who is injured, ill or deceased. So
         there needs to be a condition to determine that the data
         subject is injured, ill, or deceased.</long-description>

      <evaluates-container refid="x" />

      <xacml:Condition FunctionId="" />

   </condition>

 - <condition id="compassionate-circumstances">

      <long-description>Section 42(h) permits an institution to
         disclose personal information in compassionate
         circumstances, to facilitate contact with the next of kin or
         a friend of an individual who is injured, ill or deceased. So
         there needs to be a condition to determine that the
         circumstances of the disclosure would qualify as
         compassionate circumstances.</long-description>

      <evaluates-container refid="x" />

      <xacml:Condition FunctionId="" />

   </condition>
```

```
- <condition id="authorized-by-a-constituent-next-of-kin-or-legal-
    representative">
    <long-description>Section 42(j) permits an institution to
      disclose personal information where disclosure is to a
      member of the Legislative Assembly who has been
      authorized by a constituent to whom the information
      relates to make an inquiry on the constituent's behalf or,
      where the constituent is incapacitated, has been
      authorized by the next of kin or legal representative of
      the constituent. So there needs to be a condition that
      tests the relationship between the member of the
      legislative assembly and the data subject. So there needs
      to be a condition that tests whether an employee is
      represented by a bargaining agent or whether an
      employee is incapacitated.</long-description>
    <evaluates-container refid="x" />
    <xacml:Condition FunctionId="" />
  </condition>
- <condition id="authorized-by-employee-next-of-kin-or-legal-
    representative">
    <long-description>Section 42(k) permits an institution to
      disclose personal information where disclosure is to a
      member of the bargaining agent who has been authorized
      by an employee to whom the information relates to make
      an inquiry on the employee's behalf or, where the
      employee is incapacitated, has been authorized by the
      next-of-kin or legal representative of the
      employee.</long-description>
    <evaluates-container refid="x" />
    <xacml:Condition FunctionId="" />
  </condition>
- <condition id="for-the-purpose-for-which-it-was-obtained-or-
    compiled-or-for-a-consistent-purpose">
```

```
     <long-description>41(b) and see 43 for definition of
        consistent purpose</long-description>

     <evaluates-container refid="x" />

     <xacml:Condition FunctionId="" />

  </condition>

- <condition id="for-a-purpose-for-which-the-information-may-be-
     disclosed-to-the-institution">

     <long-description>41(c) for a purpose for which the
        information may be disclosed to the institution under
        section 42 or under section 32 of the Municipal Freedom
        of Information and Protection of Privacy Act. Notes:
        Should be covered under all section of 42 of this Act
        except f,j,k, m, n In the MFIPPA, all clauses would apply
        except f, k, and l.</long-description>

     <evaluates-container refid="x" />

     <xacml:Condition FunctionId="" />

  </condition>

- <condition id="standard-of-accuracy">

     <long-description>The head of an institution shall take
        reasonable steps to ensure that personal information,
        except that collected for law enforcement purposes
        (40(3)), is not used unless it is accurate and up to date.
        1987, c. 25, s. 40(1, 2).</long-description>

     <evaluates-container refid="x" />

     <xacml:Condition FunctionId="" />

  </condition>

- <condition id="recipient-of-disclosure-must-be-friend-or-next-of-
     kin-to-data-subject">
```

```
      <evaluates-container refid="x" />
      <xacml:Condition FunctionId="" />
    </condition>
  - <rule id="S37" ruling="allow">
      <user-category refid="any-user" />
      <data-category refid="personal-information" />
      <purpose refid="any-purpose" />
      <action refid="disclosure" />
      <action refid="use" />
      <action refid="collect" />
      <condition refid="maintained-for-purpose-of-making-public"
        />
    </rule>
  - <rule id="s38-2-no-notice" ruling="allow">
      <user-category refid="institution" />
      <data-category refid="personal-information" />
      <purpose refid="any-purpose" />
      <action refid="collection" />
      <condition refid="condition-for-proper-collection" />
      <condition refid="proper-manner-of-collection" />
      <condition refid="proper-exceptions-to-notice-obligation" />
  </rule>
- <rule id="s38-2" ruling="allow">
    <user-category refid="institution" />
    <data-category refid="personal-information" />
    <purpose refid="any-purpose" />
    <action refid="collection" />
    <condition refid="condition-for-proper-collection" />
    <condition refid="proper-manner-of-collection" />
    <condition refid="proper-notice-to-individual" />
  </rule>
- <rule id="s41-a" ruling="allow">
    <user-category refid="institution" />
    <data-category refid="personal-information" />
    <purpose refid="any-purpose" />
    <action refid="use" />
    <condition refid="disclosure-on-consent" />
    <condition refid="standard-of-accuracy" />
    <obligation refid="retention-of-personal-information" />
  </rule>
- <rule id="s41-b" ruling="allow">
    <user-category refid="institution" />
```

```
      <data-category refid="personal-information" />
      <purpose refid="any-purpose" />
      <action refid="use" />
      <condition refid="for-the-purpose-for-which-it-was-obtained-
        or-compiled-or-for-a-consistent-purpose" />
      <condition refid="standard-of-accuracy" />
      <obligation refid="retention-of-personal-information" />
    </rule>
  - <rule id="s41-c" ruling="allow">
      <user-category refid="institution" />
      <data-category refid="personal-information" />
      <purpose refid="any-purpose" />
      <action refid="use" />
      <condition refid="for-a-purpose-for-which-the-information-
        may-be-disclosed-to-the-institution" />
      <condition refid="standard-of-accuracy" />
      <obligation refid="retention-of-personal-information" />
    </rule>
  - <rule id="s42-b" ruling="allow">
      <user-category refid="any-user" />
      <data-category refid="personal-information" />
      <purpose refid="any-purpose" />
      <action refid="disclosure" />
      <condition refid="disclosure-on-consent" />
    </rule>
  - <rule id="s42-c" ruling="allow">
      <user-category refid="any-user" />
      <data-category refid="personal-information" />
      <purpose refid="any-purpose" />
      <action refid="disclosure" />
      <condition refid="for-the-purpose-for-which-it-was-obtained-or-compiled-or-for-a-consistent-purpose" />
    </rule>
  - <rule id="s42-e" ruling="allow">
      <user-category refid="any-user" />
      <data-category refid="personal-information" />
      <purpose refid="any-purpose" />
      <action refid="disclosure" />
      <condition refid="complying-with-an-Act" />
    </rule>
  - <rule id="s42-f-i" ruling="allow">
      <user-category refid="foreign-law-enforcement-agency" />
      <data-category refid="personal-information" />
      <purpose refid="any-purpose" />
      <action refid="disclosure" />
      <condition refid="disclosure-by-law-enforcement-institution"
        />
      <condition refid="under-an-arrangement" />
    </rule>
  - <rule id="s42-f-ii" ruling="allow">
      <user-category refid="canadian-law-enforcement-agency" />
      <data-category refid="personal-information" />
      <purpose refid="any-purpose" />
      <action refid="disclosure" />
      <condition refid="disclosure-by-law-enforcement-institution"
        />
    </rule>
  - <rule id="s42-g" ruling="allow">
      <user-category refid="canadian-law-enforcement-agency" />
      <user-category refid="institution" />
      <data-category refid="personal-information" />
      <action refid="disclosure" />
      <condition refid="to-aid-an-investigation" />
    </rule>
  - <rule id="s42-h" ruling="allow">
```

```
      <user-category refid="any-user" />
      <data-category refid="personal-information" />
      <purpose refid="affecting-health-and-safety" />
      <action refid="disclosure" />
      <obligation refid="institution-provides-proper-notice-to-the-
        data-subject-for-disclosure" />
    </rule>
  - <rule id="s42-i" ruling="allow">
      <user-category refid="any-user" />
      <data-category refid="personal-information" />
      <purpose refid="to-facilitate-contact-with-the-next-of-kin-or-
        a-friend" />
      <action refid="disclosure" />
      <condition refid="recipient-of-disclosure-must-be-friend-or-
        next-of-kin-to-data-subject" />
      <condition refid="compassionate-circumstances" />
      <condition refid="individual-is-injured-ill-or-deceased" />
    </rule>
  - <rule id="s42-j" ruling="allow">
      <user-category refid="member-of-the-legislative-assembly" />
      <data-category refid="personal-information" />
      <purpose refid="make-an-inquiry-on-constituents-behalf" />
```

```
        <action refid="disclosure" />
        <condition refid="authorized-by-a-constituent-next-of-kin-or-
          legal-representative" />
      </rule>
    - <rule id="s42-k" ruling="allow">
        <user-category refid="bargaining-agent" />
        <data-category refid="personal-information" />
        <purpose refid="make-an-inquiry-on-employee-behalf" />
        <action refid="disclosure" />
        <condition refid="authorized-by-employee-next-of-kin-or-
          legal-representative" />
      </rule>
    - <rule id="s42-l" ruling="allow">
        <user-category refid="responsible-minister" />
        <data-category refid="personal-information" />
        <purpose refid="any-purpose" />
        <action refid="disclosure" />
      </rule>
    - <rule id="s42-m" ruling="allow">
        <user-category refid="information-and-privacy-commissioner"
          />
        <data-category refid="personal-information" />
        <purpose refid="any-purpose" />
        <action refid="disclosure" />
      </rule>
    - <rule id="s42-n" ruling="allow">
        <user-category refid="government-of-canada" />
        <data-category refid="personal-information" />
        <purpose refid="facilitating-the-auditing-of-shared-cost-
          programs" />
        <action refid="disclosure" />
      </rule>
    </epal-policy>
```

13 End of Document