

Overview of the FOIPP Act and the Request Process



FOIPP Analyst Training

Victoria, BC

June 5 & 6, 2007

Who We Are

The IM/IT Privacy & Legislation Branch's (PLB) is part of the Office of the Government Chief Information Officer. PLB is responsible for the *Freedom of Information and Protection of Privacy Act*, the *Personal Information Protection Act*, the *Electronic Transactions Act*, and the *Document Disposal Act* and all related policy, standards and directives for the first three pieces of legislation.

PLB provides:

- leadership, support and services to ministries and other public bodies to assist them in complying with their privacy and access obligations.
- central agency comment and direction on privacy and access matters in contracts, legislative, program and systems development initiatives.
- Cross Government Request Coordination; Education and Training
- Manages Privacy impact assessments/Information Sharing Agreements and Privacy Breaches.

Today's Agenda

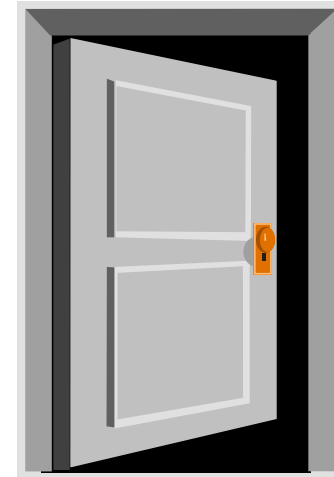
- Provide an overview of the FOIPP Act and the request process (custody/control, time extensions, fees);
- Conduct an in-depth review of exceptions and severing (mandatory exceptions, applying exceptions);
- Discuss privacy requirements and their implications (collection, use & disclosure of personal information, retention);
- Address recent amendments to the legislation and proposed changes, and
- Accomplish all of this in an interactive and informative way.

Purpose of the Act

- **Makes public bodies more accountable to the public** by
 - providing a right of access to records,
 - specifying limited exceptions to the right of access, and
 - providing for an independent review of decisions made under the Act.
- **Protects privacy** by
 - giving people a right of access to their own information,
 - a right to request correction, and
 - preventing the unauthorized collection, use, or disclosure of personal information by public bodies.

A Change of Culture

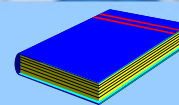
- Culture of openness
- Alters how organizations handle information
- Common sense (What if it were my information?)
- Not to replace current methods of access (except for personal information)
- Avenue of last resort



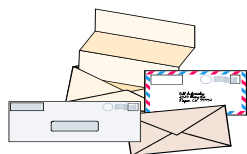
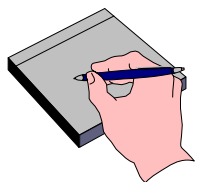
Coverage of the Act - Public Bodies

- Ministries of the Province, Crown Corporations, Agencies Boards, Commissions
- Local public bodies (local government bodies, health care bodies, municipal police and educational bodies)
- Governing bodies of professional organizations (e.g., teachers, doctors, nurses, lawyers, engineers)

Coverage of Act - Records

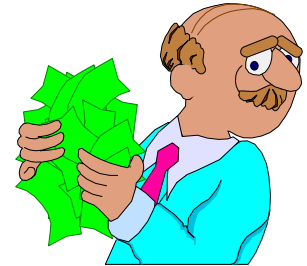


- All records in the custody or under the control of a public body
- **RECORD is any information recorded or stored by any means whether in hard copy or in electronic format**
 - Includes books, documents, maps, drawings, photographs, letters, e-mails, telephone records, black books, vouchers, papers, etc...
 - Includes contractor records
 - “Record” does not include research which must be done to answer a question



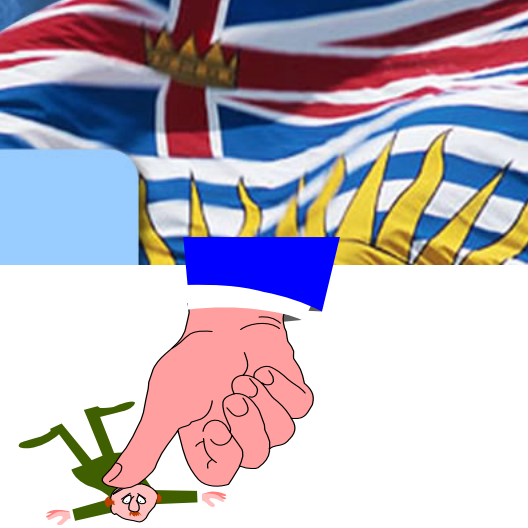
What Does Custody Mean?

- Custody means:
 - Physical possession of the record
 - May not be responsible for the actual content of the record
- What does custody entail?
 - Responsible for providing access to and security of the record
 - Managing, maintaining, preserving and disposing of the record



What Does Control Mean?

Authority to manage, restrict, regulate or administer the use or disclosure of a record



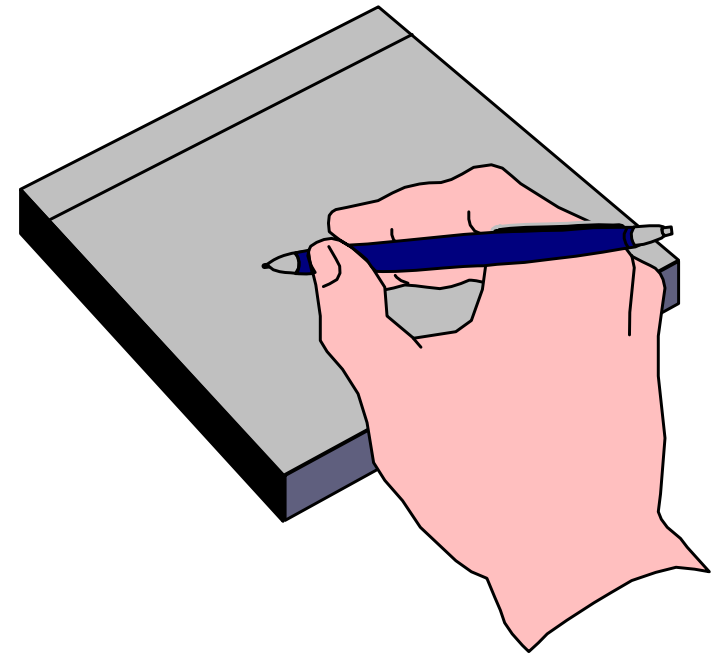
Indicators of Control:

The record

- was created by an employee of a public body,
- was created by a consultant for the public body,
- is specified in a contract,
- is subject to inspection, review or copying by the public body under contract.

The Request Process

- **Written request (s. 5)**
- **Must provide sufficient detail to identify record sought (s. 5)**
- **Proof of authority if acting for another person (s. 5)**
- **May ask for a copy or to examine record (s. 5)**
- **30 business days to respond (s. 7)**



Considerations

- Does a record exist?
- Does public body have custody or control?
- Transfer?

Transfers of Requests - Section 11

- **Can only transfer request to another “public body”**
- **Other bodies: consultations only**
- **No section 11 transfers within a public body**
- **Must complete transfer within 20 days and notify applicant**

Considerations

- Does a record exist?
- Does public body have custody or control?
- Transfer?
- Is there sufficient detail in order to identify record(s)?
- Do 3rd parties need to be notified?
- Time Extensions

Time Extensions - Section 10

- **Section 10: three reasons for time extensions**
 - Applicant does not provide enough detail
 - A large number of records is requested or must be searched and meeting deadline would unreasonably interfere with the operations of the public body
 - More time is needed to consult with a third party
- **Public bodies: take 30 days on own authority and notify applicant**
- **OIPC extensions: beyond 30 days**
 - **Required information:** *name of applicant, all relevant dates, exact new expiry date, reasons for extension (use wording in section 10)*

2006 Amendments to Section 10

- Provided the Information and Privacy Commissioner with authority to grant time extensions to public bodies when unexpected circumstances occur that prevent them from responding to access requests on time;
- Clarified that an applicant has the right to ask the Commissioner to review a time extension taken by a public body only when the public body has taken the time extension under its own authority. An applicant cannot ask the Commissioner to review a time extension that was granted by the Commissioner.

Considerations

- Does a record exist?
- Does public body have custody or control?
- Transfer?
- Is there sufficient detail in order to identify record(s)?
- Do 3rd parties need to be notified?
- Time Extensions
- **Fees & exceptions**

Fees

- Fees may be charged for locating, preparing, handling, and copying
- No fees may be charged for personal information
- No charge for first 3 hours of search
- No charge for time spent severing a record
- Applicants may request a fee waiver
- Fees prescribed by regulation



Duty to assist

- Positive duty in law to ensure that requests are responded to “openly, accurately and without delay”
- The requirement to create records--section 6
- If the decision is “no records exist”--make sure that is correct
- If there are no records, tell applicant:
 - other sources for the records
 - other available records that are similar to what the applicant has requested.



Section 43

The Commissioner may authorize a public body to disregard requests that:

- Would unreasonably interfere with the operations of the public body because of their **Repetitious** or **Systematic** nature

OR

- Are **Frivolous** or **Vexatious**



Top Five Tips for Responding to Requests

1. Communicate, Communicate, Communicate!
2. “What Does the Applicant Really Want?”
3. “Its not Personal – Its Business!”
4. Clarify Request – repeat if necessary.
5. Streamline Sign-off Process.

Exceptions and Severing



FOIPP Analyst Training

Victoria, BC

June 5 & 6, 2007

Right of Access

- The public has a right to “request” access to any record in the custody or control of a public body (s.4)
- BUT right of access limited by exceptions to disclosure (s.12 - 22)
- Must Sever

Applying Exceptions

- Two types of exceptions: Mandatory and Discretionary
- Exceptions are specific and limited
- “Disclosure should be the rule not the Exception”
- Think RELEASE, RELEASE, RELEASE, unless.....

Mandatory Exceptions

The head must not release requested information:

- Section 12: Cabinet confidences
- Section 21: Third party business information
- Section 22: Another person's personal information
- Section 22. 1: Related to abortion services



Cabinet Confidences s. 12(1)

- Prevents the harm to government that is presumed to occur if the substance of Cabinet deliberations is revealed.
- Does not apply to information in a record:
 - (a) that has been in existence for 15 yrs;
 - (b) of a decision of the Exe. Council or any of its committees on an appeal under an Act; or
 - (c) that presents background information/analysis to the Exe. Council for its consideration in making a decision that (i) has been made public, (ii) implemented, or (iii) after the passage of 5 yrs.

Third Party Business Information (s. 21)

Three part test and all 3 parts must be met:

- **Must reveal trade secrets or scientific, technical, commercial, financial or labour relations information of a third party**
- **that was supplied in confidence**
- **and disclosure must reasonably be expected to significantly harm the business interests of a third party.**

Third Party Business Information

- Which of the following records are likely to contain information which should be excepted under section 21 and
 - In which cases, should you notify the third party?
1. Record mentions the name of company which does contract work for the hospital.
 2. Record mentions name of company that does not have a contract with the hospital.
 3. Contract with third party business.
 4. Letter addressed the Mayor from a business.
 5. Consultant's report.
 6. Proposal from company that won competition.
 7. Proposal from an unsuccessful proponent.
 8. Evaluation results of proposals prepared by school board staff.

Personal Information (s. 22)

- Must refuse to disclose personal information to an applicant if the disclosure would be an unreasonable invasion of a third party's personal privacy.
- Means recorded information about an “identifiable” individual other than contact information

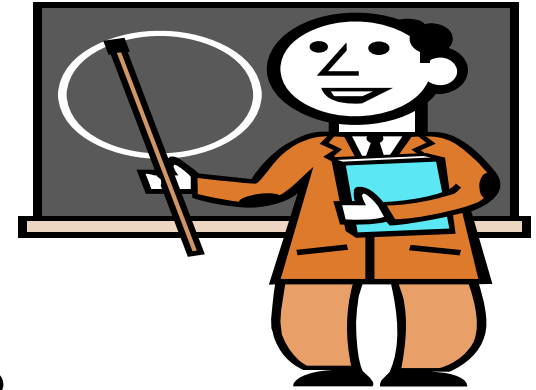
Examples of Personal Information

- name, address, telephone number
- race, national/ethnic origin, colour, religious or political beliefs or associations
- age, sex, sexual orientation, marital status
- identifying number or symbol
- fingerprints, blood type, DNA prints
- health care history
- educational, financial, criminal, employment history
- anyone else's opinions about individual and individual's personal views/opinions unless about someone else

Applying s. 22

Three parts to test:

1. Is it personal information?
2. Whose personal information is it?
3. Would disclosure be an unreasonable invasion of a third party's personal privacy?



*****Case Study*****

Is Disclosure an Unreasonable Invasion?

1. Covered by 22(4) - Not unreasonable - RELEASE
2. Covered by 22 (3) - Probably unreasonable but...
3. Must consider 22 (2) factors
 - if weigh in favour of disclosure - RELEASE
 - if weigh in favour of protection - DENY
4. 22(3) and 22(2) not exhaustive - consider all relevant circumstances.
5. If deny, does 22 (5) apply? If so, must create summary

Information Related to Abortion Services (s. 22.1)

- Must refuse to disclose information that relates to the provision of abortion services
- “Abortion Services” means Lawful medical services for termination of pregnancy

*****Severing Exercise # 1*****

Discretionary Exceptions

- The head of a public body may refuse to disclose requested information
- Two parts to applying exception:
 - does exception apply
 - exercise discretion

Exercising Discretion

- The purpose of the Legislation
- Balance of Interests (what is purpose of exception)
- Severing
- Historical practice
- Nature of the Record
- Will disclosure increase public confidence?
- Age of the Record
- Sympathetic or Compelling need
- Previous Orders
- Policy Advice: has decision already been made

Advice or Recommendations (s. 13)

May refuse to disclose advice or recommendations developed by or for a public body or a minister

- Purpose of section is to allow for open and frank discussions of policy issues within public bodies, preventing the harm which would occur if this process were subject to excessive scrutiny.
- Can not refuse to disclose information which has been in existence for 10 yrs or information which is listed under 13(2).
- Even if exception applies, consider disclosure if decision already made or if there is no perceived harm.

Solicitor Client Privilege – s. 14

Two branches:

Solicitor client communication privilege

Direct confidential communications between lawyer and client for the purpose of obtaining legal advice

- **privilege never ends**

Litigation privilege

Protects documents produced or obtained for existing or contemplated litigation

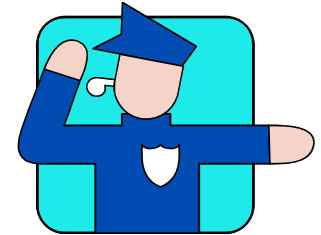
- ***dominant purpose* for producing or obtaining document must be to aid in the conduct of litigation**
- **litigation must have already commenced or be in “*reasonable prospect*” at the time document produced**
- **privilege ends when litigation concluded**

*Client has discretion to waive privilege

Does solicitor-client privilege apply to...

1. A legal bill
2. Correspondence between solicitor and client
3. An email update to solicitor on matter which he has been asked to provide advice
4. Email setting up meeting time with solicitor
5. A telephone message from solicitor
6. Letter to constituent copied to your solicitor
7. A letter from your counsel to opposing party's counsel
8. Minutes of an in-camera meeting which record solicitor's statements
9. A report prepared by in-house counsel acting in an administrative capacity
10. A report prepared by an employee, a copy of which is in litigation file

Disclosure Harmful to Law Enforcement – s. 15



- Not limited to policing
- Includes investigations or proceedings which could lead to a penalty or sanction being imposed
- Harms test
- Can withhold identities of confidential sources of law enforcement information (informants, witnesses etc...)

Intergovernmental Relations – s. 16

May refuse to disclose information that could reasonably be expected to harm intergovernmental relations or negotiations

1. Is the record less than 15 yrs old?
2. Would disclosure:
 - harm the conduct of relations between the provincial government and another government (federal, municipal, aboriginal or foreign)?
 - reveal information received in confidence by another government?
 - harm aboriginal self government or treaty negotiations?

Financial or Economic Interests – s. 17

May refuse to disclose information which could harm the financial or economic interests of a public body.

“The alleged harm must not be fanciful, imaginary or contrived but rather one which is based on reason. A reasonable person must conclude, based on the evidence, that an identified, or specific, harm to the financial or economic interests of the public body is likelier than not to flow from disclosure of the information”

Commissioner Loukidelis (Order 324/99)

2006 Amendment to Section 17

- Provided clarity to public bodies that information that may harm their negotiating position can be protected from release when responding to a request for access to records;
- This is an expansion of the already existing exception under section 17 for “information about negotiations” and is intended to protect future negotiations.

Harmful to Conservation - s. 18

May refuse to disclose information which could reasonably be expected to result in damage to, or interfere with, the conservation of anthropological sites, endangered species or other rare endangered living resources.

Examples:

- Locations of native burial sites
- Location of fossil sites or endangered species



May refuse to disclose information, including personal information about the applicant, if disclosure could reasonably be expected to:

- threaten anyone else's safety or mental or physical health, or interfere with public safety
- result in immediate and grave harm to the applicant's safety or mental or physical health.

May refuse to disclose information:

- **that is available for purchase by the public, or**
- **within 60 days is to be published or released to the public**



Overrides any other provision of the Act:

- Whether or not request for access made
- must release, without delay
- to the public, affected group or applicant
- information about a risk of significant harm to environment or public health or safety

*****Case Study # 2*****

Privacy



FOIPP Analyst Training

Victoria, BC

June 5 & 6, 2007

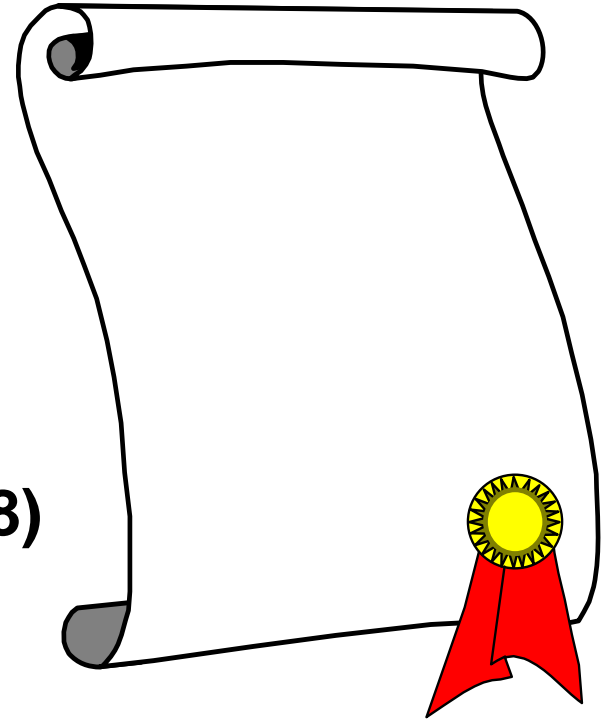
Code of Fair Information Practices

Places limits on:

- **collection, use and disclosure of personal information (s. 26, 27, 32, 33)**

Requires:

- **accuracy and completeness (s. 28)**
(Revisit student drawing)
- **reasonable security (s. 30)**
- **retention and disposal of records (s.31)**
- **access and correction (s.29)**



Collection of Personal Information



- **Key to protecting privacy**
- **The information in the record belongs to the individual it is about.**
- **Information should be collected directly from the individual whenever possible.**
- **Individual has right to know: what is being collected; why it is being collected; and how it will be used.**

Individual Privacy Rights

- Individual has right of access to and right to request correction of record (s. 29)
 - Assume what you write will be viewed by the individual
 - Only record what is necessary
 - Ensure language is clear and understandable
 - Avoid jargon, labels, pejorative statements – describe behaviour, be factual, objective
 - If an opinion is recorded, it should be documented as such

Management of Personal Information

- **Limit use to original purpose or *consistent purpose***
- **Set strict policies for security, retention and destruction**
- **Limit disclosure and data-sharing to need-to-know principle**



Reasonable Security

A public body must make reasonable security arrangements to protect personal information

- Should be appropriate and proportional to the sensitivity of the personal information
- Safeguards should include:
 - Physical measures (locked file cabinets, restricted access to offices)
 - Technological measures (user IDs, passwords, encryption)
 - And...

General Privacy Measures

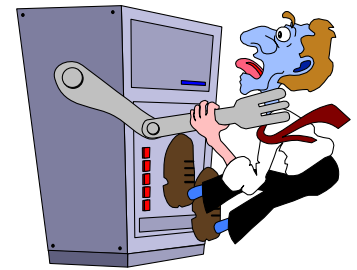
- **E-mail**
- **Fax**
- **Contractors**
- **Training**

Security Tips

- Security only as good as its weakest link (train staff, conduct periodic reviews)
- Consider internal security threats (limit access to “need to know”, audit trails)
- Protect personal information throughout its lifecycle (e.g., storing inactive records)

Retention

- **Must retain personal information for at least 1 year if it was used to make a decision that directly affects the individual and so the individual has a reasonable opportunity to access it**



Disclosure of Personal Information



- **Requirements of the Act (s.33, 33.1, 33.2)**
- **Consent**
- **Consistent Purpose**
- **Need to Know**
 - **limiting distribution**
 - **limiting content**

Disclosure for Research Purposes

- **Are permitted only if:**
 - **the research purpose cannot reasonably be accomplished unless the information is provided in personalized form or is approved by the Commissioner**
 - **any data matching does not harm individuals**
 - **information is not used for secondary purposes**
 - **all personal identifiers are destroyed ASAP**
 - **researcher signs a research agreement to comply with certain conditions (time limited, mutually beneficial)**

Disclosure of Personal Information



Case Study # 1

An individual calls your office claiming that he is a police officer and wants to know the home address of one of your employees?

What do you do?

Case Study # 2

A Ministry client, who is the subject of a number of fraud investigations, has behaved violently in the past when dealing with ministry staff. The investigation unit has annotated its file with a warning about this behaviour.

Can this information be shared with staff members in other departments so that they can take precautions when dealing with the individual?

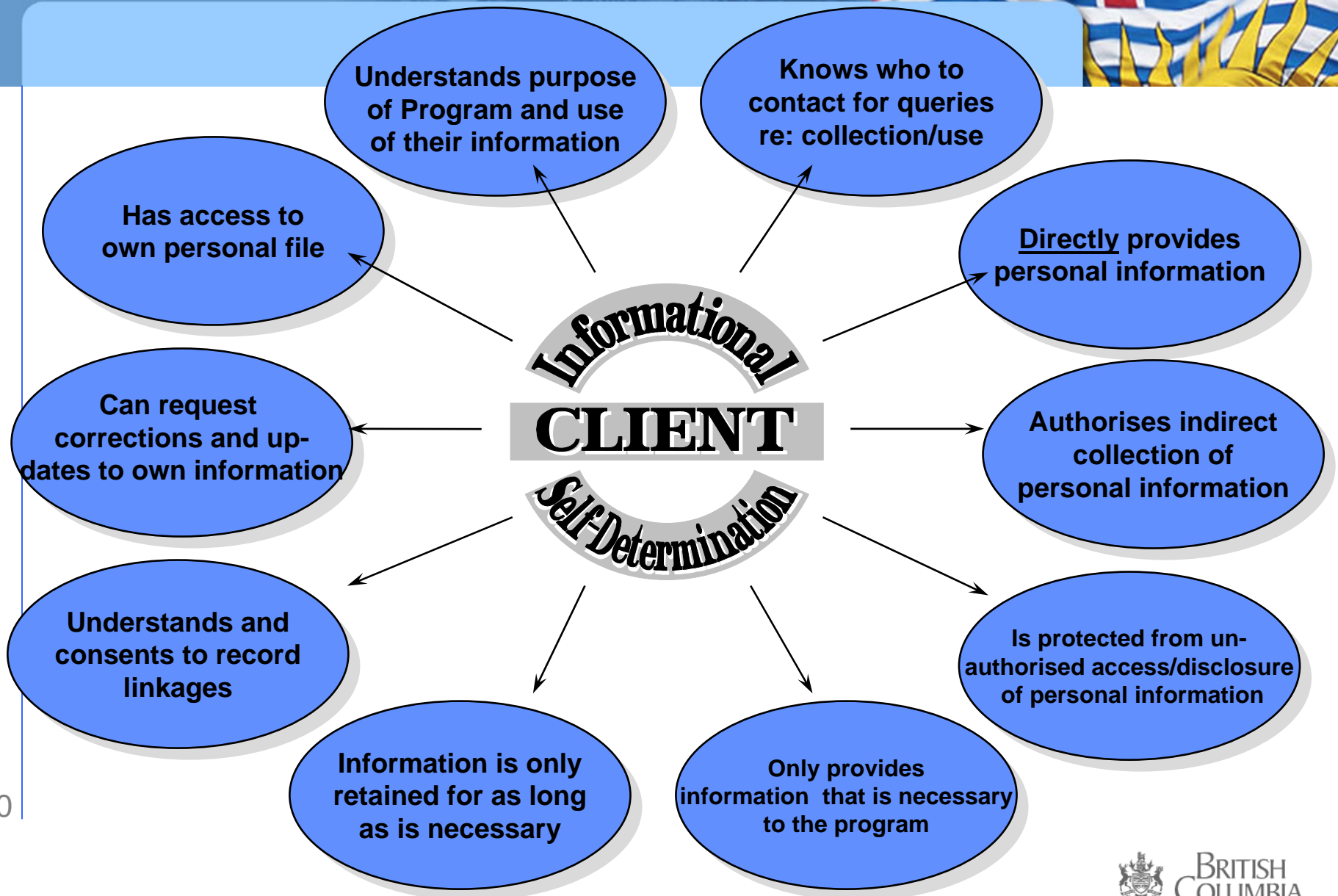
Case Study #3

Client: 23, schizophrenic. Is being released from hospital to live in a group home. Has violent outbursts. Will attend community resources. Parents visit frequently, provide care on weekends and holidays.

What information about client's history can be shared with or disclosed to:

- The client
- The group home
- Anger management counsellor
- Parents
- Local mental health centre
- Schizophrenia Advocacy centre
- The police

FAIR INFORMATION PRACTICES



Recent Amendments



Background on the *USA Patriot Act*

- ***USA Patriot Act* was a response to concerns about international crime and terrorism, heightened as a result of the events of September 2001.**
- **Amends powers already available to the FBI to obtain information about foreign intelligence for surveillance, interception and obstruction of terrorist activities.**
 - FBI must obtain orders from a special court: the Foreign Intelligence Surveillance Court.
- **Privacy concerns stem primarily from Section 215 which allow the FBI to conduct electronic surveillance, enter a facility covertly or access business records.**
 - The person who is the target of the order need not be a person suspected of criminal activity or of being a foreign agent.
 - A person served with a *USA Patriot Act* order is not permitted to disclose the fact of the order to anyone other than those persons necessary to produce the items sought.

The FOIPP Act – Pre-Amendments

- **The FOIPP Act authorized government to use contractors to provide services involving even sensitive personal information as long as reasonable security arrangements are in place to protect that information. For example:**
 - **Section 33 of the FOIPP Act authorized a public body to disclose personal information to a contractor that is necessary for a contractor to provide the contracted services.**
- **At the same time the Act required public bodies to implement appropriate privacy protection measures with respect to personal information in its custody or control.**

Proposed Changes to FOIPP Act

- Amended protection of privacy provisions in the FOIPP Act to prevent the disclosure of personal information outside of Canada
- Amended protection of privacy provisions in the FOIPP Act to prevent the storage of, and access to, personal information outside of Canada
- Extended requirements and restrictions posed by privacy protection provisions to service providers and employees
- Required the reporting of any requests received from jurisdictions external to Canada for unauthorized disclosure of personal information
- Included “whistle-blower protection” in legislation to protect individuals who report violations of the disclosure rules
- Created offences and penalties for violation of disclosure rules and failure to report
- Transitional provisions

2005 Amendments (1)

- Allowed information that is disclosed for the purposes of making payments to or from the government or a public body to be stored, or accessed from, outside of Canada.

As most credit card processors are located outside of Canada, this permits credit card payments to continue to be processed.

- Broadened the authority to disclose personal information inside or outside Canada to include personal information disclosed for the purpose of payments made to and from the government.

This amendment allows government and other public bodies to accept payments via all credit cards, including domestic cards, that require personal information to leave Canada and to accept cheques that are drawn on foreign banks.

2005 Amendments (2)

- Narrowed the disclosure of personal information outside of Canada for the purposes of debt collection to occasions where the individual resides or is located outside of Canada, or has assets outside of Canada.
- Added corporate debt provisions to ensure that personal information about directors and corporate officers can be disclosed in order to collect a corporate debt or to obtain information required to collect a corporate debt.
- Amended the disclosure provisions to permit personal information to be disclosed inside and outside of Canada if it is authorized or required by legislation to be made available to the public.
- Removed the prohibition against the Information and Privacy Commissioner serving more than one term of office.

2006 Amendments (1)

- Permitted limited and temporary trans-border access, storage and disclosure of personal information in special circumstances where it is necessary for system maintenance, trouble-shooting and data recovery.
- Permitted officers or employees of public bodies to access personal information while temporarily travelling outside Canada where that access is necessary for the performance of their duties.

The change also allowed a service provider of a public body that is authorized to access personal information to do so while temporarily travelling outside Canada where that access is normally necessary for the performance of duties in relation to the public body.

2006 Amendments (2)

- Clarified that disclosure of personal information under an “agreement” made under an enactment of British Columbia or Canada must be under a *written* agreement.
- Ensured transparency for the uses of personal health information contained in health information banks created under the *Health Act* by requiring the publication of summaries on an online public directory; and,
- Facilitated the removal from the coverage of the FOIPP Act public bodies that no longer exist or no longer meet the criteria for coverage.

Proposed 2007 Amendments (1)

- Ensure that the time period for transferring an access request commences only when a public body has sufficient detail to identify the records and the applicant's authority to request the records.
- Will permit school boards to disclose personal information to museums and archives for archival or historical purposes.
- Allow the Commissioner to require applicants to attempt to resolve complaints and requests for review with a public body before the Commissioner opens a file.

Proposed 2007 Amendments (2)

- Ensure that a matter is referred back to an applicant to resolve with a public body, the related time to resolve the issue does not count against the 90 days the Commissioner has to review the matter.
- Protect the Commissioner and his staff from testimonial compulsion.
- Enable the Commissioner to order a public body to perform its duty to sever excepted information and to disclose the remainder within a reasonable time specified by the order.

Proposed 2007 Amendments (3)

- Allow for the enforcement of the Commissioner's orders as orders of the Supreme Court of British Columbia.
- Will require employees and service providers of public bodies to notify the public bodies when they become aware of an unauthorized disclosure of personal information.
- Will permit public bodies to routinely disclose predetermined personal information that they can currently disclose in response to access requests.

Privacy Impact Assessment (PIA) Process

Do I need to complete a PIA?

- PIA needs to be completed for all new initiatives.
- If it is determined that there is no personal information being collected, used or disclosed, you should document that you have reviewed the initiative and have made this determination by completing section, Basic Information.
- The first question a public body needs to ask is “Is personal information being collected, used or disclosed in the initiative under assessment?”
- If the answer is yes, then the public body will need to do a PIA.

Information Sharing Agreements (ISA)

- What is an ISA?
- When should and ISA be used?
- Components of an ISA
- What are the benefits of an ISA?
- Six Steps to Building an ISA

Contact Information

IM/IT Privacy and Legislation Branch Contacts

Sharon Plater, Director	<u>Sharon.Plater@gov.bc.ca</u>	(250) 356-1369
Jason Eamer-Goult	<u>Jason.Eamer-Goult@gov.bc.ca</u>	(250) 387-6403
Nadine McGraw	<u>Nadine.McGraw@gov.bc.ca</u>	(250) 387-9812
Jeannette van den Bulk	<u>Jeannette.VanDenBulk@gov.bc.ca</u>	(250) 387-9809
Kash Basi	<u>Kash.Basi@gov.bc.ca</u>	(250) 387-7174
Ciaran Aiken	<u>Ciaran.Aiken@gov.bc.ca</u>	(250) 387-8595
Privacy Helpline	<u>CPIAADMIN@gov.bc.ca</u>	(250) 356-1851

Useful Links

- **IM/IT Privacy and Legislation:**
<http://www.lcs.gov.bc.ca/privacyaccess>
- **The Freedom of Information and Protection of Privacy Act:**
http://www.qp.gov.bc.ca/statreq/stat/F/96165_00.htm
- **Office of the Information and Privacy Commissioner for B.C.**
<http://www.oipc.bc.ca>
- **Core Policy Manual:**
http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm
- **Government-to-Government Personal Information Sharing Agreements - *Guidelines for Best Practice*:**
<http://www.iccs-isac.org/eng/privacy.html>