Privacy and Access in British Columbia

B.C.'s *Freedom of Information and Protection of Privacy Act (FOIPPA)*

Legislation, Privacy and Policy Branch of the Office of the Chief Information Officer (OCIO)

What we do:

- Responsible for FOIPPA, *Personal Information Protection Act* (PIPA), *Document Disposal Act* (DDA), and *Electronic Transactions Act* (ETA) and all policy, standards and directives that flow from them.
- Leading strategic privacy initiatives across government
- Establishing government policy, standards and guidelines on access and privacy issues
- Providing services, support and leadership to assist ministries and other public bodies in complying with FOIPPA
- Providing input and advice on legislative proposals and reviews
- Supporting information provision and privacy training

Information and Privacy Commissioner

- Information and Privacy Commissioner is an independent Officer of the Legislature
- Elizabeth Denham is B.C.'s Information and Privacy Commissioner
- The Office of the Information and Privacy Commissioner (OIPC):
  - conducts reviews and investigations to ensure compliance with FOIPPA
  - mediates FOI disputes
  - comments on FOI and privacy implications of proposed legislative schemes or public body programs

Information and Privacy Commissioner

The Sectional Index provides OIPC decisions and orders, arranged by relevant sections of FOIPPA.

FOIPPA is distinct from B.C. private sector and federal legislation

Freedom of Information and Protection of Privacy Act **(FOIPPA)**
public sector access and privacy legislation; applies to "public bodies" in B.C.

Personal Information Protection Act **(PIPA)**
private sector privacy legislation; applies to "organizations" (more than just businesses) in B.C.

Personal Information Protection and Electronic Documents Act (PIPEDA)
applies to federal works, undertakings or businesses (banks, airlines, and telecommunications companies) applies to the collection, use and disclosure of personal information in the course of a commercial activity and across borders.

Canada's ***Access to Information Act*** and ***Privacy Act***
are the federal equivalents to the BC FOIPPA (access and privacy obligations for federal government institutions and the federally regulated)

Structure of the Act - Overview

- Part 1: Introductory Provisions
- Part 2: Freedom of Information
- Part 3: Protection of Privacy
- Part 4: Office and Powers of Information and Privacy Commissioner
- Part 5: Reviews and Complaints
- Part 6: General Provisions
- Schedule 1: Definitions
- Schedules 2 and 3: List public bodies
- *Freedom of Information and Protection of Privacy Regulation*

Purposes of FOIPPA (s. 2)

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

- a right to request correction, and
- preventing the unauthorized collection, use, or disclosure of personal information by public bodies.

Coverage of FOIPPA

APPLIES TO:

all **records**
in the **custody** or under the **control**
of a **public body**

Coverage of FOIPPA – Public Bodies

Applies to the public sector in BC:

- 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 FOIPPA

FOIPPA does not necessarily cover....????

A) Ministry of Finance

B) Office of the Premier

C) Vancouver Island Health Authority

D) Canadian Bar Association

E) Municipality of Saanich

F) College of Physician and Surgeons

Coverage of FOIPPA

FOIPPA does not necessarily cover....????

A) Ministry of Finance

B) Office of the Premier

C) Vancouver Island Health Authority

D) Canadian Bar Association ✔

E) Municipality of Saanich

F) College of Physician and Surgeons

Coverage of FOIPPA

Section 3(1) states to what records FOIPPA does not apply.

Examples:

Court records – A draft decision prepared by a Provincial Court judge.

Material available for purchase – A report that the Queen's Printer prints and sells to the public.

Research information - A bibliography prepared by a research assistant at a university to enable a professor to determine what background material is relevant to a research proposal.

Unrelated Service Provider Records - Phone service provider's customer files.

What is a "Record"?

- A "record" is any information recorded or stored by any means whether in hard copy or in electronic format

- This includes books, documents, maps, drawings, photographs, letters, e-mails, telephone records, black books, vouchers, papers, etc...




What Does "Custody" Mean?

- Physical possession of the record
- May not be responsible for the actual content of the record
- Responsible for providing access to and security of the record
- Responsible for managing, maintaining, preserving and disposing of the record

What Does "Control" Mean?

Control means:

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

Indicators of control are that 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.

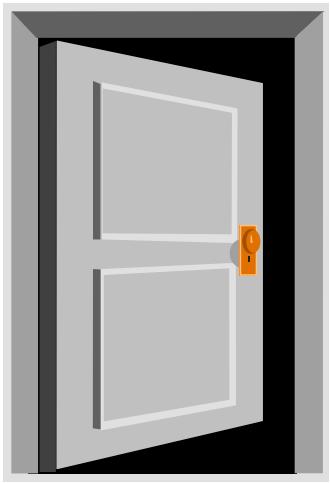
Access to Information a.k.a. Freedom of Information (FOI)

"the overarching purpose of access to information legislation, then, is to facilitate democracy. It does so in two related ways. It helps to ensure first, that citizens have the information required to participate meaningfully in the democratic process, and secondly, that politicians and bureaucrats remain accountable to the citizenry."

Justice Laforest, in a landmark Supreme Court of Canada decision in Dagg vs. Canada

A Culture of Openness

- Increased transparency
- Alters how public bodies handle information
- Common sense (What if it were my information?)
- Not to replace other existing methods of access
  (except for personal information)
- Avenue of last resort



Open Information & DataBC

Open Information: http://www.openinfo.gov.bc.ca

- The goal of this initiative is to enhance the current FOI process by making requested records available to the broader public. This new strategy on proactive disclosure and routine release does not impact the rights that every individual has to request records under FOIPPA.

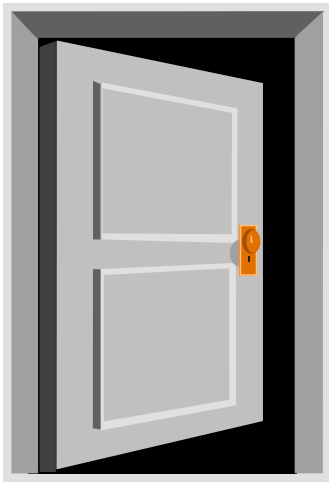
Open Information & DataBC

DataBC: http://www.data.gov.bc.ca

- DataBC made approximately 3,000 data sets public with plans to release more. Users of DataBC are encouraged to request information too. This allows users to create web portals to datasets like budget information, population demographics and elections data.

FOI Sweeping the World

- Over 70 countries around the world have implemented some form of such legislation
- Many countries have pending FOI legislation
- Sweden's Freedom of the Press Act (of 1766) is thought to be the oldest FOI legislation



Source: Wikipedia
search term: Freedom of Information

'Creative FOI'

Manchester rockers performed a song in front of dozens of the CCTV cameras that proliferate around Britain then made FOI requests for the tapes thereby saving the cost of video production. They then cut the tapes into their new video (not all of the footage is from surveillance cameras, but most is).

http://www.youtube.com/watch?v=W2iuZMEEs_A

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)
    - Includes the right to seek access to personal information whether in a case file, or elsewhere (e.g. email and memos)
- BUT right of access limited by exceptions to disclosure (s.12 – 22.1)
- AND subject to payment of fees as required (s.75)

Note: no fees if the request is for the applicant's own personal information

The Request Process (s. 5)

The applicant:

- Must make a written request
- Must provide sufficient detail to identify record sought
- May ask for a copy or to examine record
- Must provide proof of authority if acting for another person*
  - persons under 19 years of age
  - persons who have committees
  - deceased persons

* See also s. 3, 4, 5 of the FOIPP Regulation

What is Needed for an FOI Request?

Example

Applicant handwrites a letter to the public body, providing their name and address, and stating the following:

"Give me a copy of John Smith's Report dated June 2, 2013"

Applicant fails to use the public body's FOI request form or even cite FOIPPA?

What are the public body's obligations?

Example


Print Story - canada.com network - Windows Internet Explorer
http://www.canada.com/components/print.aspx?id=
Live Search
Print Story - canada.com network
Page
Tools
canada.com
WHERE PERSPECTIVES CONNECT
Wednesday » January 14 » 2009
canada, canadian search engine, free email, canada news
Oddball information requ
government
Ken Meaney
The Ottawa Citizen
Monday, October 22, 2007
One access to information request was written regarding dirty socks. Another wanted the location, make, model and number of every photocopier in the national capital region.
If it's out there, chances are someone's filed an access to information request about it. But some requests for information are more out there than others.
Anne Rooke laughs when asked if she keeps tabs on the wackier requests she gets.
Ms. Rooke, who is in charge of access to information at Correctional Service Canada, couldn't recall any, but she asked around for examples among her colleagues.
One told her about the dirty socks, which came with a $5 processing fee stuffed inside. "The requester wanted the name of the cleaning company responsible for cleaning trains. They had worn their socks on one of them and couldn't believe the trains were so dirty."
Done
Internet | Protected Mode: On
100%

Making FOI Requests for Others

Example

- Your public body interviews a 17 year old girl
- Her mother (who is separated from her spouse and has custody) makes an access request for the interview notes

Can the mother make the request on behalf of her daughter? Are the daughter's age and capabilities relevant?

Duty to Assist s. 6

- Positive duty in law to ensure that requests are responded to "openly, accurately and without delay"
- Includes a requirement to create records
- If the decision is that "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.

Timelines for Responding

- A public body has 30 business days to respond to a request (s. 7)
- A public body may extend the timeline for responding by 30 days, if (s. 10)
  - A large number of records has been requested or must be searched
  - There is not enough detail to enable the public body to identify the record
  - More time is needed to consult with a third party or other public body
  - The applicant has consented to the extension
- Further extensions for the above four reasons may be granted to the public body by the Office of the Information and Privacy Commissioner (OIPC)

Fair and Reasonable Extension – s.10(2)(b)

- Even if there are no volume, detail and consultation concerns:

The Commissioner can grant time extensions:

- if the Commissioner considers it fair and reasonable for the public body to take an extension (i.e. when unexpected circumstances occur that prevent them from responding to access requests on time)

Fees

- Fees may be charged for locating, preparing, handling, and copying records
- Cannot charge fees for:
  - Applicant's own personal information
  - First 3 hours of search for records
  - Time spent severing a record
- Written estimates must be provided (track time!)
- Applicants may request a fee waiver
- Fees prescribed by regulation

Third Party Notice

A public body:

- must give notice if it intends to give access and either s. 21 (harm to business interests) or s. 22 (harm to personal privacy) "might" apply
- may give notice if it does not intend to give access based on s. 21 or s. 22
  - Notice goes to third party and applicant
  - Timelines set out in sections 23 and 24
  - OIPC assists in resolution of access disputes

Disregarding Requests

- 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

Leicester City Council 'not ready' for zombie attack

A worried member of the public has forced Leicester City Council to admit it is unprepared for a zombie invasion.

The authority received a Freedom of Information request which said provisions to deal with an attack, often seen in horror films, were poor.

The "concerned citizen" said the possibility of such an event was one that councils should be aware of.

The FOI request said "councils across the kingdom" should be prepared for a potential zombie attack

"We've had a few wacky ones before but this one did make us laugh," said Lynn Wyeth, head of information governance.

The Freedom of Information Act allows a right of access to recorded information held by public authorities.

Ms Wyeth said she was unaware of any specific reference to a zombie attack in the council's emergency plan, however some elements of it could be applied if the situation arose.

Other submissions to the council have included requests for records of paranormal activity and haunted buildings within the city.

"To you it might seem frivolous and a waste of time... but to different people it actually means something," said Ms Wyeth.

"Everybody has their own interests and their own reasons for asking these questions."

Zombie letter in full

Dear Leicester City Council,

Can you please let us know what provisions you have in place in the event of a zombie invasion? Having watched several films it is clear that preparation for such an event is poor and one that councils throughout the kingdom must prepare for.

Please provide any information you may have.

Yours faithfully,

Concerned Citizen

Tips for responding to requests

1. Communicate, communicate, communicate!
2. What does the applicant really want?
3. Raise awareness of legislated timelines and other requirements in FOIPPA
4. It's not Personal – It's Business!
5. Consider a 'staged' release of records
6. Streamline sign-off process

Exceptions and Severing: Applying Exceptions to Disclosure

- Must release unless an exception applies
- Disclosure should be the rule, not the exception
- Two types of exceptions:
  - Mandatory and Discretionary

Mandatory Exceptions

The head must not release requested information:

- Section 12: Cabinet confidences
- Section 21: Third party business information
- Section 22: Disclosure harmful to personal privacy
- Section 22.1: Related to abortion services

Cabinet Confidences s. 12

- Prevents the harm to government that is presumed to occur if the substance of deliberations of Cabinet are revealed.
- All requests for Cabinet submissions and related records including any reference to a Cabinet matter, are reviewed by the Office of the Premier

Third Party Business Information s. 21

Three part test and all 3 parts must be met:

1. Must reveal trade secrets or scientific, technical, commercial, financial or labour relations information of a third party

2. that was supplied in confidence

3. and disclosure must reasonably be expected to significantly harm the business interests of a third party.

Personal Information s. 22

Three parts to test (applying s. 22):

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?

Discretionary Exceptions

- The head of a public body may refuse to disclose requested information.
- Two parts to applying a discretionary exception:
  - Does the 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 or Recommendations s. 13

- Intended to allow open and frank discussion of policy issues among and within public bodies, preventing harm which could occur if the deliberate process were subject to excessive scrutiny.
- Factual information presented in support of the advice- must be released unless another exception applies.
- Must be able to demonstrate that the public body exercised discretion in applying this exception.

Legal Advice – 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

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…)

Disclosure Harmful to Intergovernmental Relations or Negotiations – s. 16

- Information that would harm British Columbia's relationship with other governments including Aboriginal governments
- Information that is received in confidence from other governments or international bodies
- Harm the conduct of negotiations relating to aboriginal self government or treaties

Disclosure Harmful to Economic and Financial Interests of a Public Body – s. 17

- Information which could harm the economic, financial, competitive or negotiating interests of the British Columbia government or one of its public bodies
- Includes plans, negotiations, etc of a public body that has not yet been implemented or made public
- Can work in conjunction with s. 15, s. 16 and s. 21

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

Harm to Individual or Public Safety – s. 19

- 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
- Health professionals providing opinions regarding the reasonable expectation of harm
- Health professionals and family members helping the applicant understand the information in the record

Published or Released Within 60 Days – s. 20

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

Embarrassment is not an exception!

Public Interest Paramount – s. 25

Overrides any other provision of the Act:

- Whether or not request for access made
- Must release *information*, without delay
- To the public, affected group or applicant
- Information about a risk of significant harm to environment or health or safety of the public or a group of people; or other disclosure which is, for any other reason, clearly in the public interest.

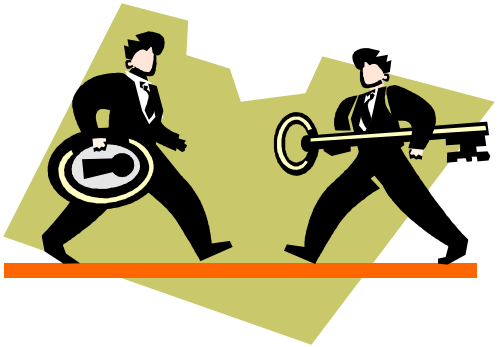
Public Interest Paramount – s. 25

Example – *significant risk of harm to the public*

- An employee observes an angry client expressing deep despair & hopelessness;
- The client blames others for their misfortunes, expresses ideas of "getting even" and has no known friends or family;
- The employee reviews the client's work, which is disturbing, self-aggrandizing and includes a picture depicting the client with what looked like an improvised explosives device;
- The employee's opinion is that the client is on the verge of a breakdown and is concerned that the client will harm themself or others;
- The employee recognizes the duty to respect the client's privacy but believes there is a significant risk.

Is the employee authorized to disclose the client's personal information?

To protect personal privacy by preventing the unauthorized collection, use, or disclosure of personal information by public bodies.



What is privacy?

- It is not defined in FOIPPA, PIPA or any legislation in Canada
- None of the statutes define "privacy" but aim to achieve it with rules for how personal information is to be collected, used and disclosed.
- Different types of privacy:
  - physical, spatial, informational

The foundation of privacy laws

Informational self determination

- an individual's personal information is their own
- to the extent possible, the individual controls how their personal information is collected, used and disclosed

This is reflected in a Code of Fair Information Practices…

Fair Information Practices: Informational Self-Determination

Code of Fair Information Practices

Places limits on:

- collection, use and disclosure of personal information (s. 26, 27, 32, 33, 33.1 and 33.2)

Requires:

- accuracy and completeness (s. 28)
- access (Part 2) and correction (s.29)
- reasonable security (s. 30)
- retention of records (s.31)

Information Management Guiding Principles

Right Information

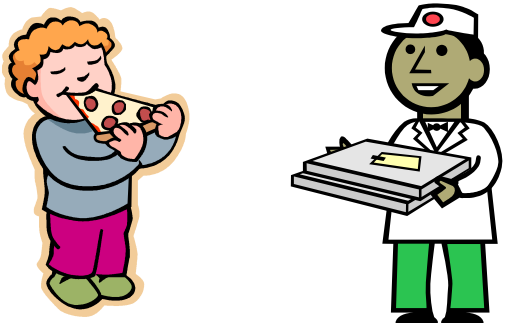
Right Person

Right Purpose

Right Time

Right Way

- Managed based on the "need to know" and least privilege principles
- Access only to the minimum amount of personal information required to perform employment duties
- Access permissions should be assigned consistently and kept up to date



Ordering Pizza in the 21st century…Created by the American Civil Liberties Union

Link:
http://www.aclu.org/pizza/index.html?orgid=EA071904&MX=1414&H=1

What is "Personal Information"?

"Personal information" means recorded information about an identifiable individual other than contact information"

(Schedule 1 definition in the FOIPPA)

Examples of your personal information:

- Your race, national/ethnic origin, skin colour
- Your religious or political beliefs or associations
- Your age, sex, sexual orientation, marital status
- Your fingerprints, blood type, DNA information, biometrics
- Your health care, educational, financial, criminal, employment history
- Your opinion unless it is your opinion about someone else

Collection of Personal Information (s. 26)

- Key to protecting privacy
- Personal information can only be collected if:
  - Authorized under an Act
  - For law enforcement
  - Related directly to and necessary for an operating program or activity
  - Consent in limited circumstances (set out in regulations)
  - Necessary for planning or evaluating a program or activity of the public body
  - The information is collected by observation at a public and voluntarily attended presentation, ceremony, performance, sports meet or similar event
  - Other authorities (domestic violence, provincial identity services)

How Personal Information is Collected (s. 27)

- Information must be collected directly from the individual, except in limited circumstances.
- Must notify the individual of the purpose, the legal authority, and who to contact with questions, except in limited circumstances.

Sample notification for collection:

This information is collected by [*name of public body*] under [*section*] of the [*name of enactment*] and will be used to [*purpose*]. Should you have any questions about the collection of this personal information please contact

[*Position Title*]

[*Address*]

[*Phone Number*]

Collection of Personal Information (s. 26)

Example

Your organization wants to offer a brand new service targeted to young people. A survey is created to ask questions about the preferences of young people, which includes: how they access services, how they prefer to pay for services and how healthy they are compared to their friends. Responses are sorted by name and Personal Education Number.

Is this an authorized collection of personal information?

When Information is NOT Collected (s. 27.1)

Personal information is not collected when a public body does nothing other than read it and

- delete
- destroy
- return or
- transfer the information

Collection of Personal Information

Example

A municipality collects pictures of infrastructure problems from citizens via the web. Common issues reported include potholes and burnt-out street lamps. Some pranksters submit inappropriate photos of their friends.

Are they authorized to collect all of this information? If not, what steps should they take now that the photos have been submitted?

Use of Personal Information (s. 32)

A public body may only use personal information:

- For the purpose for which it was obtained or compiled, or for a consistent purpose.
  - A consistent purpose (s. 34):
    - has a reasonable connection to the original purpose, and
    - Is necessary to perform the duties of, or for operating a legally authorized program, of the public body
- If the individual has consented to the use.
- For a purpose for which the personal information has been disclosed to it under the Act.

Use of Personal Information (s. 32)

Example

- Public body has already collected employee home addresses for tax purposes and now wants to use the information to send employees birthday cards.

OR

- Public body wants to use student email addresses to canvas students for suggestions to improve registration services.

Disclosure of Personal Information (ss. 33, 33.1, 33.2)

Disclosure only in limited circumstances

- Need an authority in order to disclose – do a PIA to figure out if you have authority

Inside versus outside Canada – important distinction

- 24 inside/outside Canada authorities
- 10 inside Canada only authorities

Disclose based on a need to know

- limit distribution
- limit content

Disclosure of Personal Information - Examples

Within Canada only:

- consistent purpose
- program planning or evaluation

On the web (outside of Canada):

- consent (written)
- public, voluntarily attended event (e.g. photos of ribbon cutting)
- social media engagement (e.g. via Facebook)
- under an enactment

Debt collection and enforcement:

- debt collection
- investigations (law enforcement)

Disclosure of Personal Information - Examples

Teachers Act - Written reasons and publication of reasons:

- s.66 (1) A panel must give written reasons for making one of the findings under section 63 [findings after hearing] …
- (2) Subject to subsection (4), the director of certification must make public the written reasons under subsection (1)
- (3) The publication under subsection (2) may be made by posting a notice on a publicly accessible website maintained by or on behalf of the ministry.

Disclosure of Personal Information (ss. 33, 33.1, 33.2)

Example

- A public body client has behaved violently in the past in dealing when dealing with staff.
- Staff has annotated its file with a warning about this behaviour.
- Can this information be shared with staff members in other departments/programs so that they can take precautions when dealing with the individual?

Disclosure of Personal Information (ss. 33, 33.1, 33.2)

Example

- Joe is employed by a public body
- Another public body contacts Joe's employer to get details on his earnings
- The public body says that it is granted the power by statute to demand this information from Joe's employer to assist in its settlement of a claim

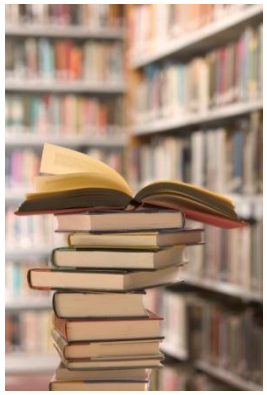
Should the public body give the information?

Disclosure of Personal Information (ss. 33, 33.1, 33.2)

Example

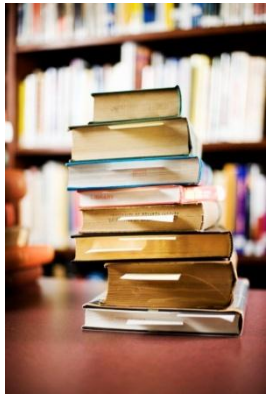
- An individual calls your office claiming that he is a police officer and wants to know the home address of one of your employees?

What do you do?



Disclosure for Research Purposes (s. 35)

Disclosure for Archival or Historical Purposes (s. 36)



Accuracy and Completeness (s. 28)

If...

- personal information is in the custody or under the control of a public body, and
- will be used by or on behalf of the public body to make a decision that directly affects the individual

... then the public body must make every reasonable effort to ensure that the personal information is accurate and complete.

The Right to Correction (s. 29)

- Individual has right to request correction of personal information
- Section 29 applies to factual errors or omissions in personal information, not to expressions of judgement
- The right to request correction is distinct from the public body's duty to annotate
- Section 29 does not function as an avenue for appeal

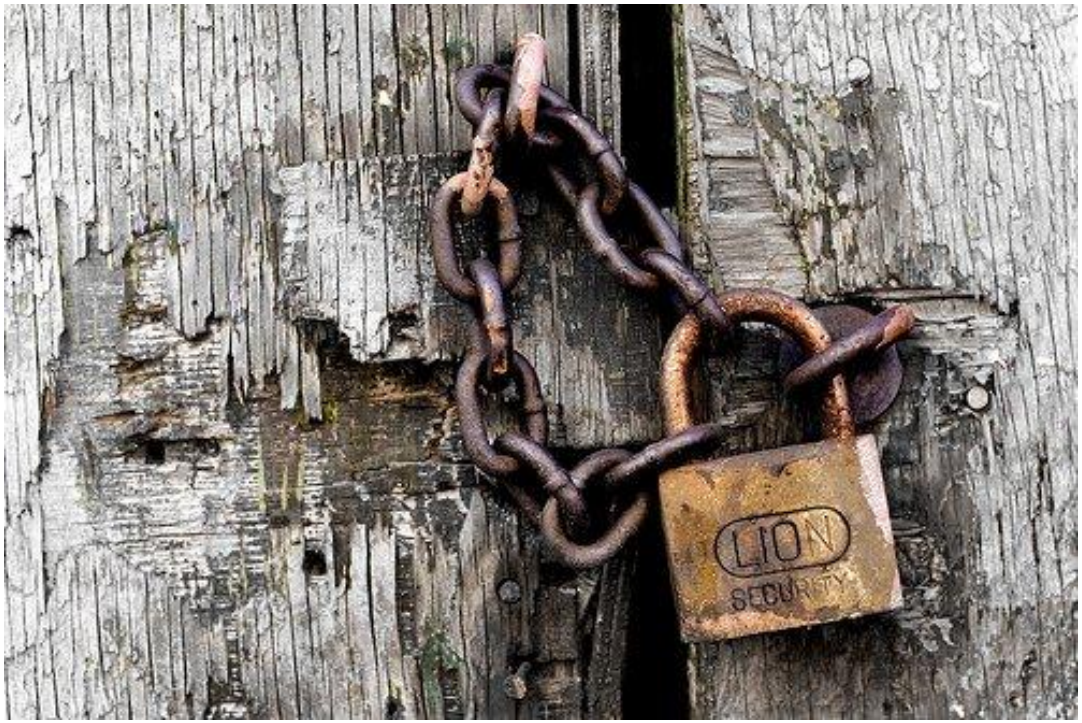
Retention (s. 31)

- Must retain personal information for at least 1 year after it is used to make a decision that directly affects the individual so that the individual has a reasonable opportunity to access it;
- This is the minimum standard – ensure that you also meet other applicable legal and policy requirements.

Example:

- Joe applies to public body for entrance into job training program
- Joe provides certain educational and financial information in support of the application
- Application is denied and Joe has no idea why
- One week later, Joe contacts the public body to follow up and wants to see the information written down about him (because he thinks an error has been made)
- The public body tells Joe it based its decision on the information it had in its file, and has since destroyed the file – and by the way, "feel free to apply next year".

Privacy and Security



FOIPPA: security measures

- A public body must make reasonable security arrangements to protect personal information (s. 30)
- Should be appropriate and proportional to the sensitivity of the personal information e.g. suspension information vs lunch order
- Storage & Access must be in Canada (s. 30.1)
- Safeguards should include:
  - Physical measures (e.g. locked file cabinets, restricted access to offices)
  - Technological measures (e.g. user IDs, passwords, encryption)
  - Have policies and procedures for keeping files secured

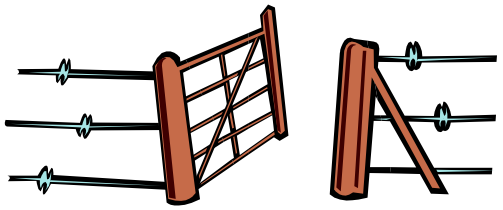
Security Tips

- Security is only as good as its weakest link (train staff, conduct periodic reviews)
- Use secure internal resources (e.g. email, flash drives, etc.)
- Consider internal security 'threats' – including those from privacy-unaware staff (limit access to "need to know"; consider audit trails)
- Protect personal information throughout its lifecycle (e.g. "clean desk" policy for current records; properly storing inactive records; properly disposing of records and equipment)

Information Incidents

Information Incidents are ALL unauthorized event(s) that threaten the privacy or security of information

Includes privacy breaches: a collection, use, disclosure, disposal, storage of or access to personal information, whether *accidental or deliberate*, that is not authorized by the *Freedom of Information and Protection of Privacy Act*



Examples of How Information Incidents occur

- Employee errors such as mis-stuffed enveloped or incorrect email addresses
- Hacking or phishing
- Sale of unwiped hardware or blackberries
- Wrong fax numbers or addresses
- Deliberate employee misconduct

When things go wrong...

- Doctor inadvertently faxes medical records to a newspaper whose fax number was on speed dial.
- Law firm stores files, awaiting pick up for shredding, in an unlocked storage bin in a back alley, where they are captured on videotape blowing down the alleyway.
- National bank puts un-wiped hard drives, containing detailed financial information on clients, up for sale on the web.
- Hospital janitor disposes of old hospital records by lighting a bonfire on a public beach - a ferry passes by, sending waves onto the beach that put out the fire and wash the half-burned records down the shoreline
- Closed case files end up as props on the set of the TV series X-Files.
- An AIDS patient list, including addresses, is accidentally emailed to more than 800 unauthorized recipients.

Information Incident Response

- An information incident can affect any organization, even if it has good privacy and security practices. Are you ready for a privacy breach and do you know what to do when one occurs?
- New Government of British Columbia Information Incident Management Process - ministries must follow. All public bodies should create their own policy and process.
  - See the Office of the Government Chief Information Officer website for information: http://www.cio.gov.bc.ca
  - OIPC Breach Resources for Public Bodies at: http://www.oipc.bc.ca

Step 1 REPORT

Any government employee who discovers an actual or suspected information incident must report it immediately (24x7)!

1. Notify your supervisor

2. Report to the Office of the Chief Information Officer (OCIO) by calling 250-387-7000 and selecting option 3 (toll free: 1-866-660-0811).

3. Complete a General Incident/Loss Report (GILR) within 24 hours.

Step 1 In response....

Triage and intake

An Investigator will ask:

- What happened and when?
- What actions have been taken so far and has the incident been contained?
- Does the incident involve information about identifiable individuals, including clients or employees? What kind?
- Who will the Ministry contact person be if other than caller?

Assignment and notification to your Ministry Chief Information Officer and specified ministry personnel

The Team Approach: The Incident Action Team

- **Involves:** OCIO Investigator, lead from ministry/program area -- and others as appropriate
- Emphasis on rapid, collaborative assessment with appropriate experts
- Conference calls where appropriate to discuss agreed upon next steps

Step 2

RECOVER

- Recover information or assets
- Contain the incident

Step 3 REMEDIATE

- Incident Action Team collaborates with Investigators
- Determine the specifics of the
- incident
- Remedial action determined

Step 3 Notify?

- Notification is assessed for each individual whose privacy has been breached.
- Notification may be required where an individual could be at risk of harm as a result of an information incident.
- The Harm's Test – key aspects of harm to be considered:
  1. Risk of identity theft or fraud
  2. Risk of physical harm
  3. Risk of hurt, humiliation or damage to reputation
  4. Risk to business or employment opportunities
- Other considerations: legal, contractual.

Step 4 PREVENT

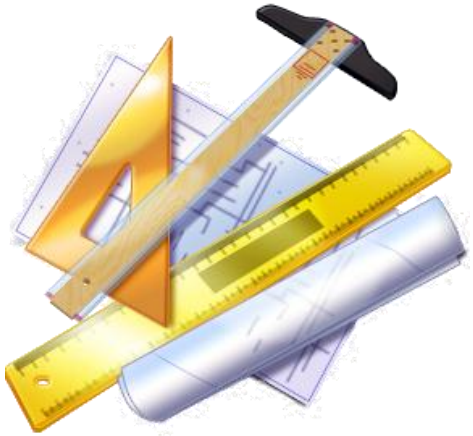
- Major focus
- Most changes are:
  - Education/ Awareness
  - Practice/ Procedure
  - Policy
  - Business Process

It's better to prevent a privacy breach in the first place!

Prevent breaches through compliance with the general FOIPPA requirements, for example:

- Awareness of the disclosure authorities and other provisions of the FOIPPA
- Reasonable policy and procedures for disposition of personal information (not selling old hard-drives; etc)
- Reasonable security arrangements, including physical, technical and policy measures (encryption; establishing sound access user profiles; etc)

Privacy Tools



Privacy and the administration of personal information

- Organizations and public bodies have millions of pieces of personal information, on paper, in databases, on laptops, etc.
- What tools are available to keep track of this information and ensure it is administered appropriately?

Privacy Impact Assessment (PIA): When should one be done?

- New program, project, system, legislation, technology, or other initiative;

OR

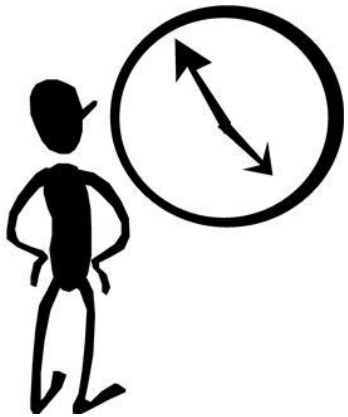
- If there are significant changes to them (a PIA is a living document)

Privacy Impact Assessment: Benefits

- If used as part of normal business processes, the PIA can ensure that privacy requirements are identified and satisfied in a timely and cost efficient manner.
- PIA process is also designed as an educational tool – participating in privacy impact assessments promotes privacy awareness.
- The PIA can make the difference between a privacy invasive and a privacy enhancing initiative, without compromising business objectives or adding significant costs.
- Meet your legislated requirements to do one.

When do I do a PIA?

- During the development phase of a new program, project, system, legislation, technology, or other initiative; OR
- Before the implementation of a significant change to an existing program, project, system, technology or information system, or legislation takes place; OR
- For all significant existing programs/initiatives
- Whether personal information is, is not, or could be collected, used or disclosed!



Where do I go for help with my PIA?

Ministries - Legislation, Privacy and Policy Branch, OCIO

- Privacy and Access Helpline: 250 356-1851
- Email: Privacy.Helpline@gov.bc.ca
- Website: http://www.cio.gov.bc.ca/cio/priv_leg

Other Public Bodies – OIPC

- Phone: 250 387-5629
- Email: info@oipc.bc.ca
- Website: www.oipc.bc.ca

Information Sharing Agreements (ISA)

What is an ISA?

- When should an ISA be used?
- Components of an ISA
- What are the benefits of an ISA?

ISA Best Practices / Guidelines:
http://www.cio.gov.bc.ca/local/cio/priv_leg/documents/foippa/guidelines_isa.pdf

Privacy Protection Schedule

Mandatory for ministries; recommended for other public bodies and organizations.

Advice for other public bodies

- The PPS for use by other public bodies may be completed and attached as a schedule to any contract between a public body and a contractor under which the contractor will be collecting, creating, using, disclosing or storing "personal information" (as defined in FOIPPA) unless it is not intended that the public body will own or control the personal information.

Useful Links

- Legislation, Privacy and Policy Branch: www.cio.gov.bc.ca/cio/priv_leg/lpp.page?
- OCIO – Freedom of Information and Protection of Privacy - Public Sector (includes Policy & Procedures Manual; PIA Process with Template; Contracting link to PPS; etc): http://www.cio.gov.bc.ca/cio/priv_leg/foippa/guides_forms/guide_index.page?
- The Freedom of Information and Protection of Privacy Act: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00
- BC Office of the Information and Privacy Commissioner: www.oipc.bc.ca
- Federal – Office of the Privacy Commissioner of Canada: www.priv.gc.ca

Useful Resources

- FOIPPA Policy and Procedures Manual
  http://www.cio.gov.bc.ca/cio/priv_leg/manual/index.page
- Key Steps to Responding to Privacy Breaches -
  http://www.oipc.bc.ca/guidance-documents/1428
- Protecting Personal Information Outside the Office
  http://www.oipc.bc.ca/guidance-documents/1447

Contact Information

BC Privacy and Access Helpline: 250-356-1851

(Enquiry BC 1 800 663-7867)

Privacy.Helpline@gov.bc.ca

BRITISH COLUMBIA