

pipa

Introduction to PSP Legislation

Preeti Adhopia

Office of the Information &
Privacy Commissioner of Alberta

Jim Burrows

Office of the Information &
Privacy Commissioner of British Columbia

September 2007



Office of the Information
and Privacy Commissioner
of Alberta



OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

Overview

- **What is the Personal Information Protection Act (PIPA)?**
- **Who / what does PIPA apply to?**
- **Overview of PIPA's requirements**
- **What to do to comply**
- **Resources for organizations**
- **Questions**

What is PIPA?

- **Personal Information Protection Act and Regulation – January 1, 2004**
- **Common sense rules for *collection, use and disclosure of personal information* by private-sector organizations**
- **Balances the right of an individual with the need of organizations to collect, use and disclose PI for reasonable purposes**

What is PIPA?

- **Federal and Provincial Commissioners are working to harmonize practices and protocols**
- **Alberta, B.C., and Quebec all have their own PIPA (other provinces therefore governed by PIPEDA)**

PIPA applies to...

“Organizations” which includes:

- **Corporations and unincorporated associations**
- **Trade unions (*Labour Relations Code*)**
- **Partnerships (*Partnership Act*)**
- **Individuals *acting in a commercial capacity***
- **Non-profit organizations (all in B.C. and to a limited extent in Alberta)**
- **Professional Regulatory Organizations (Alta.)**

PIPA applies to ...

- **“Personal Information” - information about an identifiable individual**
- **Includes “personal *employee* information”**
- **Applies to recorded information or unrecorded (ex. verbal)**
- **Does not apply to aggregate / anonymous information**

What is Personal Information?

PI can include, but is not limited to:

- Name
- Address
- Gender
- Education
- Income
- S.I.N.
- Birth date
- Employment history
- Medical history
- Financial information
- Credit card numbers
- Driver's license number
- Photographs
- Vehicle information

PIPA does not apply to...

Some examples ...

- **Personal information collected, used, disclosed for**
 - **Personal or domestic purposes**
 - **Artistic, literary or journalistic purposes**
 - **Business contact information**
 - **Personal information about someone dead for 20+ years**

PIPA does not apply to...

Some examples ...

- **Personal information collected, used, disclosed for**
 - **Personal information contained in a record in existence for 100+ years**
 - **Records transferred to archival institutions**
 - **Court files/records**

What does it mean if PIPA applies to an organization?

- **Organizations are accountable for personal information in their custody or control**
- **Need to identify someone to be responsible for ensuring compliance with the Act**
- **Need to develop policies and procedures to ensure compliance - and make them available on request**
- **Responsible when engaging services of another person (e.g. contracting)**

Generally...

- Organizations need consent for collection, use and disclosure of personal information
- Need consent to collect personal information from anyone other than the individual
- May collect, use or disclose personal information only for purposes that are reasonable, and to the extent that is reasonable for meeting those purposes

Generally...

- **Notify individual about the purposes for collection up front (at or before the time of collection) to the individual and contact info**
- **Limit collect, use or disclose of personal information to those stated purposes**

Consent

- Can be express, implied, or deemed/ “opt-out” (give notice and ask them to advise you if they don’t consent)
- Verbal or written is acceptable
- Should be obtained *before* or *at time of* collection

Consent

- **May be withdrawn or changed by the individual**
- **Invalid if obtained by deceptive or misleading means**
- **Organization must not require an individual to consent to collection, use or disclosure of PI beyond what is necessary to provide the product or service**

Collection, Use, and Disclosure *without* consent

- When it is clearly in the interests of the individual
- When another Act or regulation authorizes it
- For “investigations” or “legal proceedings”
- When the information is “publicly available”
- To collect a debt or repay monies owed

Collection, Use, and Disclosure *without* consent

- to create a credit report
- to determine suitability for honour or award
- for archival or research purposes
- from a public body authorized / required to collect, use or disclose personal information

Special Rules for *Use without* consent

All the purposes listed under rules for collection *without* consent, AND ...

- to respond to an emergency threatening the life, health or security of individual or public

Special Rules for *Disclosure without* consent

All the purposes listed under Collection and Use *without* consent AND ...

- in accordance with a treaty
- to comply with a subpoena or court order
- to assist a public body or law enforcement agency in an investigation

Special Rules for *Disclosure without* consent

All the purposes listed under Collection and Use *without* consent AND ...

- to contact next of kin of injured or deceased
- to disclose to a surviving spouse or relative of a deceased individual, if reasonable
- to protect against fraud or market manipulation, to any agency empowered by legislation

Personal *Employee* Information

- Personal information reasonably required solely for the purposes of establishing, managing or terminating the employment or volunteer work relationship.
- “Employee” includes a person employed by the organization to perform a service
 - e.g., apprentice, volunteer, student, contractor, agent or prospective employee

Personal *Employee* Information

- Employment is not consent-based
- Collect, use & disclose without consent when reasonably required within the employer-employee relationship
- Does not include personal information unrelated to the employment or volunteer relationship
- Must still notify current employees of purpose(s) for collection, use and disclosure

Whistleblower Protection

An organization cannot take adverse employment action against an employee who, acting in good faith and on reasonable belief, informs the Commissioner of a possible breach of the Act

Providing Access

- **Individuals can request access to their own personal information contained in a record and details about how their personal information is used and disclosed**
- **An organization:**
 - **Must assist and respond within 30 business days in B.C. or 45 calendar days in Alberta (can extend under certain circumstances)**
 - **May charge a reasonable fee (but not for personal employee information)**

Providing Access

- **An organization:**
 - **Has a duty to assist**
 - **May (or must) withhold certain information**
 - **Be familiar with the exceptions**
- **Rights may be exercised by a person on another's behalf**

Exceptions to Access -Discretionary

- **Legal privilege**
- **Confidential commercial information**
- **Collected for investigation or legal proceeding**

Exceptions to Access -Discretionary

- **Information would no longer be provided to the organization, and it is reasonable that it would be**
- **Collected by a mediator or arbitrator under an agreement, Act, or by a court**
- **Relates to or may be used in exercise of prosecutorial discretion**

Exceptions to Access - Mandatory

- **Disclosure would threaten the life or security of another individual**
- **Disclosure would reveal personal information about another individual**
- **The information would reveal the identity of someone who provided an opinion in confidence**
- **Must sever information where reasonable to do so**

Accuracy

Organizations must make reasonable efforts to ensure that any personal information collected, used or disclosed by or on behalf of an organization is accurate and complete

Corrections

- **Individuals can ask to have their personal information corrected**
- **Fix it promptly if you agree it is wrong**
- **Notify those to whom the incorrect information had been disclosed**

Corrections

- **If you don't agree it is wrong, then annotate your records to show the info is disputed**
- **Must not correct or alter opinions**
- **There are no fees for correction**

Retention

- Keep personal information for as long as is required for “legal or business purposes”.
- If you don’t need it anymore for business, tax, legal purposes or other legislative requirements (i.e. the *Residential Tenancies Act* requires you to keep it), then destroy it.
- You may set your own retention period for records based on your own business needs or legal requirements.

Security & Safeguarding

- **Organizations must protect personal information in their custody or control**
- **Have reasonable security arrangements against unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction**

Security & Safeguarding

- **Administrative, technical, physical controls**
- **Includes secure destruction / disposal - must retain personal information only as long as reasonable**

Information Security

- **Assess information security risks**
- **Write policies and procedures to mitigate risks**
- **Train employees**
- **Assess compliance**

Information Security

- **Important risk areas:**
 - **Access control and user permissions**
 - **Firewall and anti-virus (malicious code)**
 - **Backup and recovery**
 - **Disposition of media**
 - **Remote access**

Information Security

- **Data transmission**
- **Wireless**
- **Portable devices**
- **Computer/network “hardening”**
- **Physical access control**
- **Third parties (business partners)**

Common Security Breaches

- **Information left on hard-drive or other media, then sold**
- **Records lost in transit – poor management of backup media**
- **Stolen laptop computers and workstations containing personal information**

Common Security Breaches

- **Improper use of information by authorized user (insider)**
- **Records not shredded**
- **Use encryption**

Records Management Implications

- **Privacy compliance requires sound records management practices**
- **Need to locate records quickly in order to process requests within time limit**
- **In deciding how long to keep a record, an organization should be guided by legal and business purposes**

Grandfathering

**Personal information collected *before*
January 1, 2004 ...**

- **Deemed to have been collected with consent**
- **May be used and disclosed for the purpose for which it was collected**

Summary - Fair Information Practices

1. **Accountability**
2. **Identifying Purposes**
3. **Consent**
4. **Limiting Collection**
5. **Limiting Use, Disclosure & Retention**
6. **Individual Access**
7. **Accuracy**
8. **Safeguards**
9. **Openness**
10. **Challenging Compliance**

10 Steps to Compliance

- 1. Put someone in charge of privacy (i.e. property manager)**
- 2. Become familiar with the Act**
- 3. Review how you handle personal information**
- 4. Put your practices to the test (compare against requirements of the Act)**
- 5. Develop privacy policies and practices**

10 Steps to Compliance

6. **Develop an access & complaints handling process**
7. **Create notice statements**
8. **Review and revise contracts**
9. **Consider employees' personal information**
10. **Train staff**

Office of the Information and Privacy Commissioner (OIPC)

- **Information and Privacy Commissioner**
 - **Independent Officer of the Legislature**
 - **Enforces PIPA and FIPPA/FOIP (and HIA, in Alberta)**
- **The Commissioner can:**
 - **investigate complaints**
 - **initiate own investigations & issue orders**
 - **provide non-binding advice and advance rulings**

Office of the Information and Privacy Commissioner (OIPC)

- **General powers of Commissioner include:**
 - **conduct investigations to ensure compliance**
 - **review an organization's response to a request for access to personal information**
 - **conduct inquiries and issue binding orders**

Office of the Information and Privacy Commissioner (OIPC)

- **General powers of Commissioner include:**
 - **publish orders and investigation reports**
 - **conduct research & provide general advice**
 - **comment on existing / proposed programs**
 - **point out failures to assist applicants**

PIPA Resources

Alberta PIPA Help Desk

(780) 644-PIPA (7472)

Dial 310-0000 for toll-free

www.pipa.gov.ab.ca

Alberta OIPC

1-888-878-4044

www.oipc.ab.ca

British Columbia OIPC

1-800-663-7867

www.oipc.bc.ca

“Common sense”
guides to cyber-security

www.isalliance.org

Carnegie-Mellon

www.cert.org

Security Now!

www.grc.com/SecurityNow.htm

(podcasts)