

Alberta

Freedom To Create. Spirit To Achieve.

Striking the Right Balance: Alberta's *Personal Information Protection Act*

Policy & Governance

Service Alberta

September 22, 2011

Government
of Alberta ■

What we will cover today

- Who we are at Policy and Governance?
- Information and Privacy Commissioner
- What is the *Personal Information Protection Act*?
- What is privacy?
- What is personal information?
- Overview of PIPA's principles
- Including practical application and best practices
- Security considerations
- Working with Government offices
- Resources
- Questions



Policy and Governance, Service Alberta

- **FOIP Services (includes PIPA!)**
 - Corporate administration of Alberta’s access and privacy legislation in both public and private sectors
 - Department access and privacy services for Service Alberta and Treasury Board including: access requests, privacy impact assessments; and liaison with the OIPC
 - Leadership, support and services to assist public bodies and private sector organizations in complying with their privacy and access obligations
 - Accompanying resource development, education, training and reporting; including FOIP and PIPA Help Desk Services
- **Policy and Legislative Services**
 - “Centre of Excellence” for policy development in Service Alberta
 - Manage Service Alberta’s 38 Acts and 82 Regulations
- **Foreign Ownership of Land – “FOLA”**
 - Administration of the *Agricultural and Recreational Land Ownership Act* and the *Foreign Ownership of Land Regulations*

Information and Privacy Commissioner

- Information and Privacy Commissioner is an Independent Officer of the Legislature
- Frank Work is Alberta's Information and Privacy Commissioner
- The Office of the Information and Privacy Commissioner (OIPC):
 - conducts reviews and investigations to ensure compliance with the FOIP Act and PIPA
 - comments on FOIP and privacy implications of proposed legislative schemes or public body programs



PIPA is distinct from other legislation

- ***Personal Information Protection Act (PIPA)***
 - private sector privacy legislation; applies to “organizations” in Alberta
- ***Freedom of Information and Protection of Privacy Act (FOIP Act)***
 - public sector access and privacy legislation; applies to “public bodies” in Alberta
- ***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 Alberta’s FOIP Act**
 - access and privacy obligations for federal government departments and agencies

What is PIPA?

- Protection for personal information held by private sector (non-government) **organizations**
- Provincial legislation that came into force January 1, 2004 to balance the needs of organizations and the rights of “**privacy**”
- “Common sense” rules for the collection, use, disclosure (sharing), retention and security of **personal information**
- Recognizes “right” of individuals to protect their personal information and the “need” of organizations to collect, use and disclose personal information for ***reasonable purposes***

Organizations

What is an Organization under PIPA?

- ✓ Corporations
- ✓ Trade Unions
- ✓ Agents, contractors, service providers
- ✓ Associations not Incorporated
- ✓ Partnerships
- ✓ Self-employed

What is not an Organization under PIPA?

- ✓ A person acting in a personal or domestic way
- ✓ Public Bodies (covered under FOIP Act)

Special Rules:

- ✓ Professional Regulatory Organizations
- ✓ Non-profit Organizations

What does it mean to be a non-profit organization under PIPA?

Section 56 of PIPA defines a *non-profit organization* as an organization that is:

- incorporated under the *Societies Act*,
- incorporated under the *Agricultural Societies Act*, or
- registered under Part 9 of the *Companies Act*.

For these non-profit organizations, PIPA applies only when they collect, use or disclose personal information in connection with any *commercial activity*.

A *commercial activity* means:

- a transaction, act or conduct that has a commercial character to it, such as selling, bartering or leasing donor, membership or other fund-raising lists and includes operating a private school or college or an early childhood services program.

For non-profit organizations, PIPA does not apply to personal information collected during a transaction that is not a commercial activity. Nor does it apply to the personal information of employees or volunteers of a non-profit organization.

PIPA applies fully to all other organizations that are not incorporated or registered as described above, whether they operate on a not-for-profit basis or as for-profit organizations.

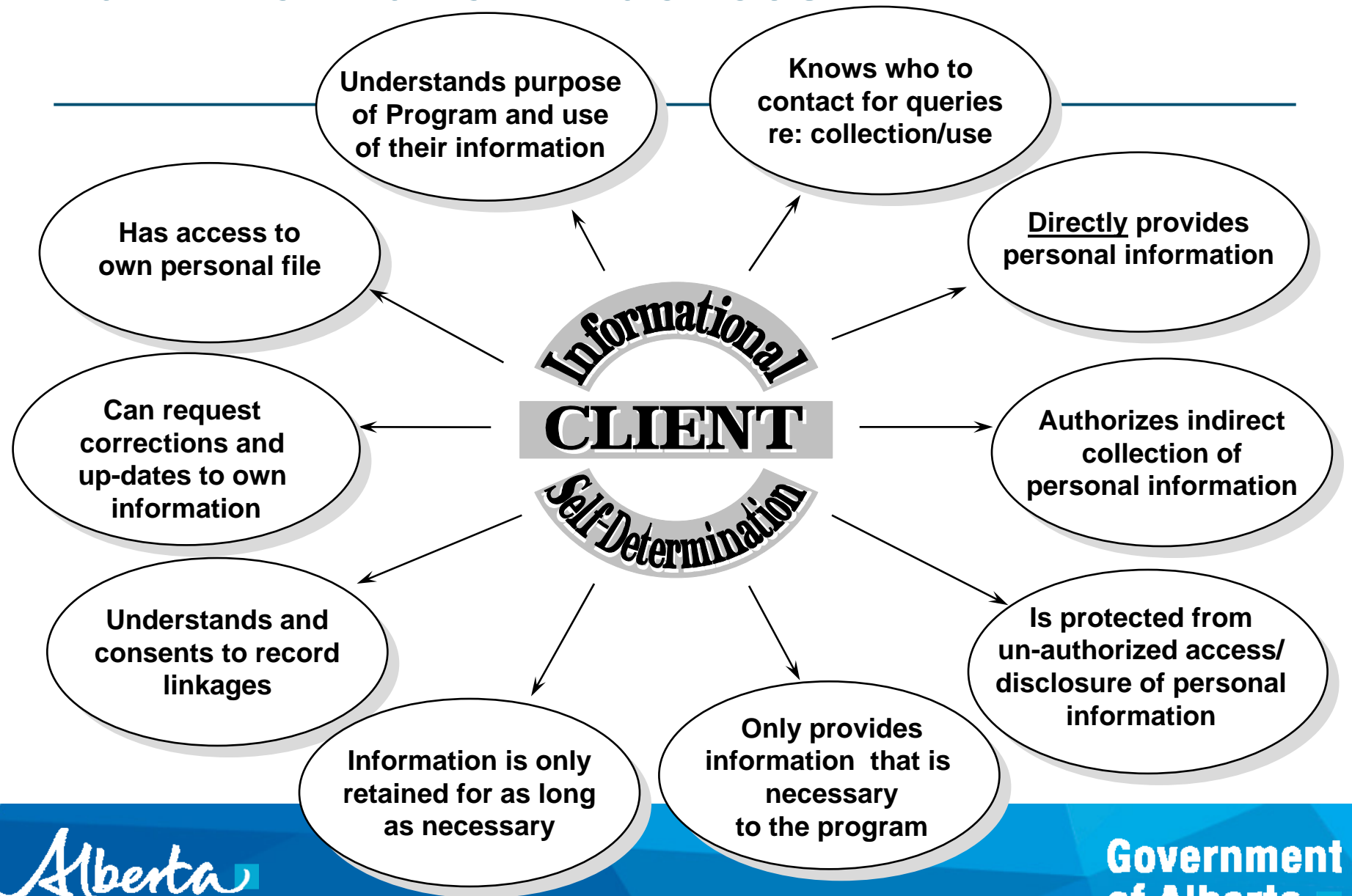
Why does PIPA matter for non-profit organizations?

- Albertans are increasingly concerned about privacy, are well-informed and expect accountability
- Risks like identity theft and privacy breaches seem to be increasing, especially in an electronic world
- Sound privacy practices benefit ALL organizations and the people they serve
- Implementing best practices to protect personal information benefits non-profit organizations in a number of ways:
 - Positive image
 - Enhanced loyalty from members, clients and employees
 - What if it is *your* personal information?

What is privacy?

- Not defined in 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
- Subjective and context sensitive
- Different types of privacy:
physical, spatial, informational

Fair Information Practices



What is personal information?

- Personal Information is

“Information about an Identifiable Individual”

- Some examples of personal information:

Name, age, home address and phone number, SIN, race or ethnic origin, medical information, income, marital status, religion, education, opinions, employment information, photographs, video recordings

- Identifies an individual

- ✓ Name
- ✓ Home address
- ✓ ID numbers

- Is about an individual

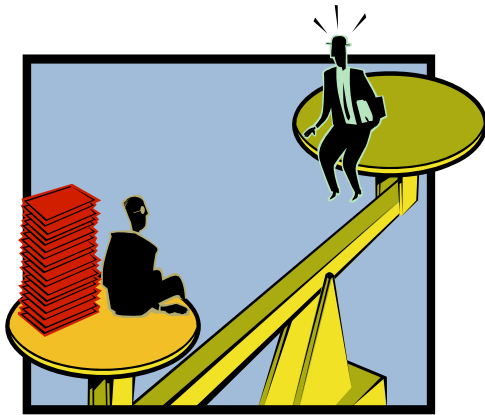
- ✓ Blood type
- ✓ Physical Description
- ✓ Education

(examples not exhaustive!)

Purpose of PIPA

Striking the Right Balance

PIPA balances an individual's ability to control their **personal information** and their right to have it protected,



with an organization's need to collect, use and disclose personal information for ***reasonable purposes.***

Reasonable Purposes

Example

- Grandma Milly goes missing from a care facility.
- The police ask the facility for information that could help them locate her.

To assist the police in locating Grandma Milly, what information is reasonable for this purpose?

- Her picture?
- Her age?
- Clothes she was last seen in?
- Bank account balance?
- Medical history?

Compliance with PIPA

- What would a reasonable person consider appropriate in the circumstances?
- Custody and Control
- Policies and Practices
- “Privacy Officer”



Privacy Officer

- Designate one or more individuals responsible for privacy (a privacy officer)
- Be responsible for all information under your control, including contractors



Obtain Consent

- PIPA is primarily consent-based for the collection, use and disclosure of personal information
- Consent may be:
 - ✓ Express (written/oral)
 - ✓ Implied (i.e. deemed)
 - ✓ Deemed (RE: transfer and benefit)
 - ✓ Opt Out
- Consent requires notification provisions be met
- Withdrawal of Consent

Consent Provisions

- ✓ Indirect collection requires consent unless that consent is otherwise not required
- ✓ Do not make consent a condition of supplying a product or service beyond what is necessary to provide the product or service
- ✓ Explain to individuals the implications of withdrawing or varying their consent but do not prohibit the withdrawal unless it would frustrate the performance of a legal obligation
- ✓ Do not obtain consent by deceptive means

Collection Notification

- An organization must identify, verbally or in writing:
 - the purposes for which it collects personal information
 - upon request, who can answer questions about the collection
- Notification provisions apply to information in the custody of a service provider outside Canada



What are examples of some purposes for the collection of personal information?

Identifying Purposes

Examples of purposes might include:

- opening a file
- verifying references
- providing referrals for services
- assisting clients completing applications and forms
- sending out membership information
- providing support to caregivers
- providing employee benefits

Collection must still be reasonable and appropriate in the circumstances

Would the following collection be reasonable?

Examples

A senior requires in-home care services. The organization collects their name and address and advises they also want their Alberta Personal Health Number on file.

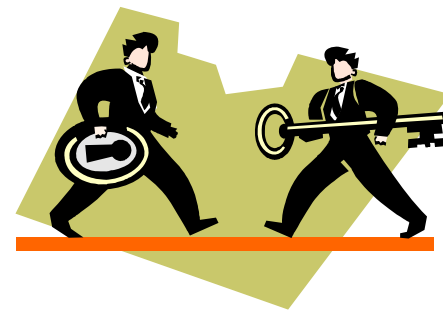
Is this reasonable?

Senior's Centre wants to introduce fingerprint readers at all building access points.

Is this reasonable?

Limited Exceptions to the Requirement for Consent in Collection, Use and Disclosure

- First, the legislation states the requirement for consent
- Second, the legislation provides for exceptions to when consent is not required
 - Section 14 – Collection
 - Section 17 – Use
 - Section 20 – Disclosure
- Third, the legislation provides “special rules” for Personal Employee Information



What is personal employee information?

Personal Employee Information

Personal information collected, used or disclosed by an organization that is reasonably required to establish, manage or terminate an employment or volunteer work relationship

OR

manage a post-employment or post-volunteer work relationship

What is *not* personal employee information?

- “Work products” such as every letter or document an employee writes or signs
- *Business contact* information

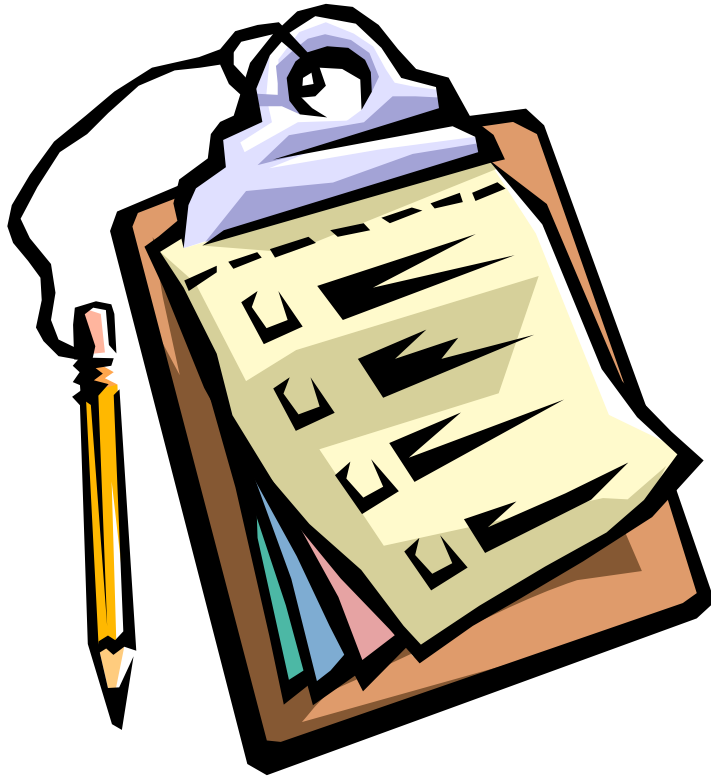


More Special Rules

- For Business Transactions involving organizational:
 - ✓ Purchase
 - ✓ Sale
 - ✓ Lease
 - ✓ Merger
 - ✓ Amalgamation
 - ✓ Acquisition
 - ✓ Business disposal, or
 - ✓ Securing interest
- See section 22 of PIPA



Limit collection, use and disclosure of personal information



- Do not collect, use or disclose personal information indiscriminately
- Information must be necessary to fulfill identified purposes (i.e. reasonable and appropriate)
- Only to the extent reasonable to meet those purposes

Access – Correction – Annotation – Accuracy

- Upon request, provide individuals with access to or correction of their personal information
 - If correction is not made must be annotated
- Upon request, provide information about the use or disclosure of their personal information
 - Identify the purposes it has been or is being used for; and
 - Identify to whom and the circumstances of disclosure
- Make a reasonable effort to ensure personal information collected, used or disclosed is accurate and complete
 - To the extent reasonable for the original purposes for collecting, using or disclosing

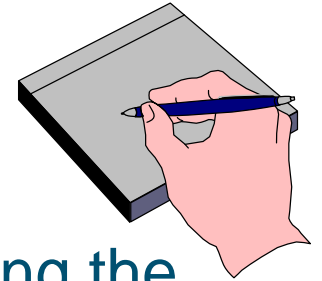
Right of Access – to Individual's Own Personal Information Only

- ✓ Written request required
- ✓ Sufficient detail necessary
- ✓ Duty to Assist
- ✓ Limited exceptions
- ✓ Respond within *45 calendar days*
- ✓ Extensions
- ✓ Fees



What is Needed for an Access Request ?

Example



- Applicant handwrites a letter to the assisted living facility, providing his name and address, and stating the following:

“Give me a copy of my father, John Smith’s, records since June 1, 2007”

- Applicant fails to use the organization’s formal request form or even cite it as an access request under PIPA.
- What are the organization’s obligations?

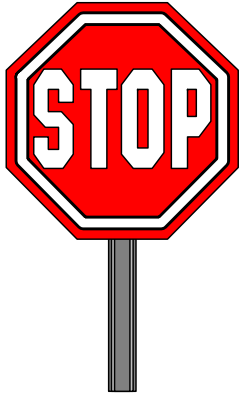
Protect Information – Reasonable Security

- An organization 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)
 - Organizational measures (security clearances, training)

Security Tips

- Train staff, conduct periodic reviews, ensure all staff are aware of obligations and understand privacy policies and procedures
- Ensure sufficient monitoring and supervision is given to staff
- Support staff – ensure employees have access to managers or other experts when questions arise
- Ensure an emergency plan is in place to deal with unintentional disclosure (do employees know who to report problems to?)
- Ask questions; encourage a privacy aware culture

Breach Notification Required



Notice must be provided to the Information and Privacy Commissioner of any incident involving the loss or unauthorized access to or disclosure of personal information:

- Without unreasonable delay
- Where real risk of significant harm to the individual reasonably exists
- Information is prescribed in the regulations that must be included in the written notice:
 - ✓ Describe circumstances
 - ✓ Provide date or time period
 - ✓ Describe personal information involved
 - ✓ Risk assessment
 - ✓ Estimate impact
 - ✓ Describe steps taken to reduce risk
 - ✓ Describe steps taken to notify impacted individuals
 - ✓ Provide contact person
- The Commissioner will determine whether notification of impacted individuals is necessary

Protect Personal Information...

...throughout its lifecycle (e.g. accessing current file, storing inactive records and destroying records)



Limit Retention

Personal information may be retained only for as long as it is **reasonably** required for *business or legal purposes* even when consent is withdrawn or varied.



Within a **reasonable** period of time after the personal information is no longer **reasonably** required and there are no *business or legal purposes* for keeping it, organizations must destroy the personal information or render it non-identifying.

Ensuring compliance with privacy requirements and protection of personal information

- Assign responsibility
- Become familiar with legislative requirements
- Conduct a Privacy Audit and make appropriate changes
- Develop a Privacy Policy
- Train staff
- Ask questions; find or provide answers
- Develop or review and revise forms and communication materials as necessary
- Review and revise service contracts as required

Working with Government Organizations



- Be clear about Custody and Control
- Understand legislative boundaries and responsibilities
- Contractual Provisions
- Know that the same principles apply – with differences
- Questions?

RESOURCES & RELATED LINKS

- PIPA Help Desk @ 780-644-7472
- **Service Alberta Resources – Personal Information Protection Act:**
<http://servicealberta.ca/pipa/>
- **Alberta Legislation – QP Laws On-line:**
http://www.qp.alberta.ca/Laws_Online.cfm
- **Personal Information Protection Act at QP Laws On-line:**
http://www.qp.alberta.ca/574.cfm?page=P06P5.cfm&leg_type=Acts&isbncln=9780779748938
- **Office of the Information and Privacy Commissioner:**
www.oipc.ab.ca
- **Service Alberta Resources – Freedom of Information and Protection of Privacy Act:** <http://www.servicealberta.ca/foip/>

Alberta

Freedom To Create. Spirit To Achieve.

Questions?

Joanne Gardiner

Access and Privacy Advisor

Policy and Governance

780-422-7326

Thank You

**Government
of Alberta** ■