Access to Information and Protection of Privacy

Sheldon Toner

Caroline Wawzonek

DRAGON TONER
LAW OFFICE

What is ATIPP?

- Access to Information
- Right to access records held by public bodies
- Right to request access and correct individual's personal information

- Protection of Privacy
- Limited exceptions to rights of access
- Prevents unauthorized collection and use of personal information

Review and Recommendations

First Level – Information and Privacy Commissioner
Second Level – Supreme Court of the NWT

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NORTHWEST TERRITORIES

Access to Information

- Why is this happening?
  - Bill 29 – An Act to Amend the Access to Information and Protection of Privacy
  - Transparency and Accountability (Municipal Context)
    - Conflict of Interest Act
    - Codes of Conduct
    - Ombudspersons
    - ATIPP

Access to Information

- What can be accessed?
  - Any record in the custody or under the control of the public body
- Who can access it?
  - Any person (includes companies, societies, media outlets)

Access to Information

- What do I need to know?
  - Access to information is a *right*
  - Public bodies have *duties*
    - Reasonable effort to assist and respond
    - Reasonable effort to create records
  - Timelines must be met
  - Refusals must have written reasons
  - Subject to review by Information and Privacy Commissioner

Access to Information

- What do I need to do?
- Manage information
  - Collect and use information properly
    - Authorized under enactment
    - Purposes of law enforcement
    - Purposes of program or activity
  - Assume information will be accessed
- Prepare for requests
  - Designate a coordinator
  - Maintain information securely
  - Reminder system for timelines
  - Seek legal advice on exceptions

Privacy Protection

One of the fundamental purposes of the Act:

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

What is “personal information”

- “About” someone and “identifiable”
  - Fingerprints, blood type, inheritable characteristics
  - Educational, financial, criminal or employment history
  - Anyone else’s opinions about the individual
  - The individual's personal opinions (except where about someone else)

Fundamentals

Know what personal information you have, where it is, and what you are doing with it.

- Collection
- Protection while in possession
- Use/Disclosure

Collection: do you <u>really</u> need a copy?

- Collect only what you truly "need" to fulfill your purpose
  - SIN numbers?
  - Names of family members' health providers?
- *Cautionary tale: NIHB forms*

Collection: when

- Personal information may only be collected by or for a public body IF:
  - Expressly authorized by an "enactment"
  - Law enforcement purposes
  - The information relates directly to and is necessary for an existing program or a proposed program where collection is authorized by the head with Executive approval
- *Cautionary tale: social media pages*.

Collection: must do's

- Collect the information directly from the individual to whom it relates
  - unless you fall under a s 41 exception such as "where authorized"
- Inform the individual of the purpose, authority and contact person
- Seek informed and voluntary consents

Protect the information in your possession

- Physical controls
  - Locked cabinets
  - Restricted access areas
- Technical controls
  - Password protection
  - Considering encryption
  - Up to date virus protection
- Administrative and personnel security controls
  - Encourage a culture that protects privacy through training & policies
  - Maintain an inventory of portable devices and monitor use

Use

- Scope:
  - purpose
  - Informed consent
  - Part C exceptions
- Accuracy
- Opportunity for correction

Disclosure: danger zones

- Disclosure may only occur in accordance with Part C, section 48
- Beware:
  - Email: switching similar names, misspells on impersonal email addresses, group emails dispersed too widely
  - Information overlap: where info about one person includes information about others (e.g. program access or attendance records)
  - Oversharing: information that relates to a person sharing might also relate to others involved (e.g. in a harassment investigation)
  - When a single office fills multiple roles: information about a harassment complaint made to a complaint officer then being offered during a subsequent human resources staffing process

Avoiding Privacy Complaints

- Designate and make available a privacy and information coordinator
- Establish policies: collection, use and disclosure; access to and correction of information; retention and disposal; security controls
- Train staff regularly about privacy protection
- Limit collection of information
- Protect information: lock it, encrypt it, track it
- Respond to access requests in a timely manner


thank
you