



Mount Royal University The Protection of Privacy Act ("POPA" 101) Awareness Training

Jeremy Duffin, BA, MAS, ECMs
Info Mgt & Privacy Advisor (The MRU Access & Privacy
Office)

Presentation (POPA 101) Overview

1. Quick High-Level Summary - Government repeals the FOIP Act

1. The requirements (+/-) for MRU and its Employees to Protect Privacy:

- How to collect...identifiable personal information
- How to use...identifiable personal information
- How to disclose...identifiable personal information
- How to protect...identifiable personal information
- *(+/-) most POPA rules remain identical to FOIP w/minimal differences

1. The “brand new” requirements for MRU and its Employees concerning: Data Matching (PI)>(Non-Personal Data)(NPD) activities to Protect Privacy:

- How (When) to create...data derived from (PI) for Data Matching
- How (When) to use.....data derived from (PI) for Data Matching
- How (When) to disclose...data derived from (PI) for Data Matching
- How (When) to protect...data derived from (PI) for Data Matching

High-Level Summary - Government repeals FOIP

- Government repealed the FOIP Act (circa 1995) on June 11, 2025
- FOIP is now replaced with 2 different Acts:
 - The Alberta Protection of Privacy Act (the “POPA”)
 - The POPA applies to MRU operations and controls how the University must:
 - (collect/use/disclose/protect) identifiable personal information, and;
 - (create/use/disclose/protect) data derived from personal information concerning Data Matching (DM) processes.
 - The Alberta Access to Information Act (the “ATIA”)
 - The ATIA applies to the MRU (Access and Privacy Office) must legally respond (with the support of MRU Departments providing responsive records) to a formal access to information requests submitted to the University in writing.
 - Similar to FOIP - A formal access request is typically engaged (required) when the records being requested - contain third party information, business proprietary information, or other (sensitive) information that must be withheld (redacted) accordance with the Act.
 - **Note:** These awareness slides mainly discuss the POPA - as this Act impacts overall MRU operations for all Employees.

Definition of Personal Information (POPA):

Recorded information about an identifiable individual...

- Name
- Address
- Phone #
- Email
- *Personal/Business
- Identifying Numbers or Symbols
- Educational, Financial or Employment History
- Race
- Religion
- Political Beliefs
- Age
- Marital Status
- Biometric Info
- Blood Type
- Gender Identity (new)
- Sexual Orientation (new)
- Anyone else's opinions about the individual.
- An individual's personal views or opinions, except if they are about someone else.

Collection Rules (POPA) - #1 Purpose of Collection (PI)

1. Personal information (PI) may only be collected by or on behalf of a public body under certain limited purposes authorized under the POPA.

I. Mandated Purposes = “MRU Operations or Integrated Programs”:

(PI) is collected... as it relates directly to (and is necessary for) an operating program or activity of the public body, including a common and or integrated program or service. (**Necessary means “demonstrable need” to have the info**)

I. Authorized by Law (Alberta or Canada) = The “PSLA”:

(PI) is collected... as the collection of that information is expressly authorized by an enactment of Alberta or Canada.

I. *Law Enforcement:

(PI) is collected... as the collection of that info is for the purposes of law enforcement. (****rarely used in PSI environment**)

Collection Rules (POPA) - #2 Manner of Collection (PI)

2. Personal information (PI) must be collected by or on behalf of a public body directly from the individual the info is about under POPA.
 - Similar to FOIP - limited allowances to collect the individual's (PI) indirectly from other sources. (e.g. determining suitability of individual for honour/award.)
3. MRU must provide a Collection Notice (POPA) to individuals when directly collecting their (PI).
 - Collection Notice language has changed compared to FOIP.
 - Departments will need to revise their former FOIP Notices to the POPA requirements (next slide).
 - MRU (Legal & Privacy) have provided the language template (online)
 - https://www.mtroyal.ca/FOIP/PoliciesGuidelines/standard_consent_for_ms.htm

Collection Rules (POPA) - #2 Manner of Collection (PI)

New Notice Requirements...

- When collecting (PI) directly from the individual, MRU must inform them of the following...
 - The purpose (reason) for collecting the information;
 - The specific legal authority for the collection;
 - The contact information to which questions can be directed:
 - Email address (and/or) telephone number (and/or) other info.
 - MRU's intention (if any) at time of collection - to input the (PI) into an automated system (e.g. Artificial Intelligence)(AI):
 - To generate content, make decisions, recommendations or predictions.

Collection Rules (POPA) - #2 Manner of Collection (PI)

New Notice Requirements...

- Example of new POPA Notices:

The Protection of Privacy Act - Standard Notification Statement Example (1 of 2)

The personal information that you provide to Mount Royal University is collected under the authority of the *Post-Secondary Learning Act* (s.65) and the *Protection of Privacy Act* (ss. 4(a) & (c)). The information will be used for the purposes of [blank].

Questions regarding the collection of personal information can be directed to:

Department Name - Mount Royal University - Phone (and/or) Email (and/or) Department Website (url)

The Protection of Privacy Act - Standard Notification Statement Example - (Artificial Intelligence) (2 of 2)

The personal information that you provide to Mount Royal University is collected under the authority of the *Post-Secondary Learning Act* (s.65) and the *Protection of Privacy Act* (ss. 4(a) & (c)). The information will be used for the purposes of [blank].

The University may ["will" if known at time of drafting notice] input the collected personal information into automated systems to fulfill the purposes stated above. This may include such activities as to generate content, evaluate programs or make institutional recommendations and predictions.

Questions regarding the collection of personal information can be directed to:

Department Name - Mount Royal University - Phone (and/or) Email (and/or) Department Website (url)

Use Rules (POPA) - of Personal Information (PI)

1. Personal information (PI) may only use collected (PI) authorized under the POPA or following circumstances...

I. Consistent Purposes:

(PI) is used... in a manner that is consistent with the purposes (reasons) provided in the initial Collection Notice (POPA).

I. Individual Consents:

(PI) is used... in a manner where the individual has signed expressed consent for MRU to use their (PI) in that way. (e.g. student signs consent for MRU to interact with a parent, etc).

I. If a circumstance exists (under POPA) to use the (PI):

(PI) is used... in a manner where a circumstance is listed under POPA that allows the use of the individual's (PI) in that way. (e.g. section 13)

*Note: Use of the (PI) may only be used (or limited) to the extent necessary to enable MRU to carry out the purpose in a reasonable manner. (e.g. Use of (PI) on a "need to know" basis)

Disclosure Rules (POPA) - of Personal Information (PI)

1. Personal information (PI) may only disclose collected (PI) authorized under the POPA or following circumstances...

I. Consistent Purposes:

(PI) is disclosed... in a manner that is consistent with the purposes (reasons) provided in the initial Collection Notice (POPA).

I. Individual Consents:

(PI) is disclosed... in a manner where the individual has signed expressed consent for MRU to disclose their (PI) in that way. (e.g. student signs consent for MRU to disclose their (PI) externally to a third party as in a parent, etc).

I. If a circumstance exists (under POPA) to disclose the (PI):

(PI) is disclosed... in a manner where a circumstance is listed under POPA that allows the disclosure of the individual's (PI) in that way. (e.g. section 13)

*Note: Disclosure of the (PI) may only be disclosed (or limited) to the extent necessary to enable MRU to carry out the purpose in a reasonable manner. (e.g. Disclosure of (PI) on a "need to know" basis)

Disclosure Rules (POPA) - Listed circumstances

Personal information (PI) may only disclose collected (PI) authorized under the POPA (e.g. section 13 - Non Exhaustive Examples)...

➤ MRU may disclose (PI) in the following circumstances....

- Internally (Inter-Dept): to (another) employee of MRU if the (PI) is necessary ("demonstrable need") for the performance of the duties of the employee.
- Externally (Inter-Gov): to (another) employee of another public body (gov) if the (PI) is necessary for planning, administering, delivering, managing, monitoring or evaluating a common or integrated program or service and for the performance of that employee. (e.g. CBE Practicums, etc)
- Business Card Rule: an employee's business address, business phone, business email, title, employment responsibilities.
- Receipt of Honour/Award: receipt of an honour or award granted by (or through) MRU

*Note: Disclosure of the (PI) may only be disclosed (or limited) to the extent necessary to enable MRU to carry out the purpose in a reasonable manner. (e.g. Disclosure of (PI) on a "need to know" basis)

Disclosure Rules (POPA) - Listed circumstances (Cont'd)

Personal information (PI) may only disclose collected (PI) authorized under the POPA (e.g. section 13 - Non Exhaustive - “Need-to-know”]

Examples...

➤ **MRU may disclose (PI) in the following circumstances....**

- **Managing Personnel**: to (another) employee of MRU if the (PI) is necessary for the purpose of managing or administering personnel of MRU, including for conducting workplace investigations.
- **Student Confirmation (Degree Awarded/Enrolment)**: MRU can confirm with external inquiries simply that a Degree was awarded (and/or) confirm the student is enrolled in a Program. (Cannot disclose specific courses/grades)
 - **Note(1)** : Info cannot be disclosed if student has requested to MRU that the info not to be disclosed.
 - **Note(2)**: Good Practice to check w/ Office of the Reg. (beforehand)
- **Legislative Compliance**: for the purpose of complying with an enactment of Alberta or Canada or with a treaty, arrangement or agreement made under an enactment.

Protection Rules (POPA) - of Personal Information (PI)

Personal information (PI) must be protected by MRU by making reasonable security arrangements against such risks as...

- Unauthorized access, collection, use, disclosure or destruction.
- In the event of a privacy breach where there exists a real risk of significant harm “RROSH” to individuals, MRU must mitigate the incident and notify the following (MRU Access and Privacy Office must be contacted):
 - The individual(s) to whom there exists a real risk of significant harm;
 - The Privacy Commissioner, and;
 - The Minister of Technology and Innovation.
- “RROSH” means the incident of (PI) will result in real risk of significant harm based on the following factors:
 - Likelihood of Misuse of (PI);
 - Caused by or likely will be used for Malicious intent;
 - Data sensitivity (Health or Financial) (Minors and Vulnerable Individuals); and
 - Mitigation measures that have been taken that reduce the risk of harm.

Protection Rules (POPA) - of Personal Information (PI)

POPA has increased penalties for employees for knowingly contravene the Act.

➤ Physical Measures:

- Locking rooms, offices, cabinets that hold records when vacant or absent.
- Securely shredding or deleting records when no longer needed (in accordance with MRU Records Retention Policies) (Transitory vs Official Records)
 - Transitory Records (copies) can be destroyed when no longer needed for reference.
- When destroying records making sure they are unreadable (esp. if they contain sensitive information).

➤ Administrative Measures:

- Institutional policies, Dept internal SOP's, personnel screening (Dept. floor awareness), established authentication processes prior to disclosing (PI) over online or the phone (Dept).

➤ Technical Measures (ITS):

- Incorporating strong user passwords and protocols. (Cybersecurity) (ITS)
- Locking Office Computers when away from desk (CTRL - ALT - DELETE)
- Ensuring mobile devices are physically secured when left unattended (laptops - not left in vehicles).
- Limiting storing data (both sensitivity and volume) on portable flash drives.
- Encrypting (password locking) flash drives that hold sensitive data.
- Using Bcc (Blind Carbon Copy) to protect privacy when sending mass emails (to external third parties)

Data Matching (PI) Rules (POPA) - New

POPA has brand new rules for MRU concerning Data Matching (PI) activities.

- Applies in limited/specific circumstances when Departments conduct Data Matching (PI) >(Non Personal Data)(NPD) activities.
 - To qualify as a Data Matching (PI) activity - it must have the following “qualities”:
 - The Data must initially contain identifiable personal information (PI);
 - The Data must be “created” through a process that links (PI) between (2 or more databases or electronic sources).
 - “Created” meaning *bring into existence something new, to cause or bring about.*
 - “Collected” meaning *to accumulate, gather, group, hold or store (often for reference purposes).*
- Data = “Collected” under standard POPA (FOIP) Rules:
 - e.g. Collected Data about Students held in Banner;
 - e.g. Collected Data in Banner moved/integrated into other SaaS systems.
- Data Matching (PI) = “Created” under New Data Matching Rules:
 - e.g. The Office of Institutional Research and Planning - linking (PI) through 2 or more systems to create new data sets to evaluate programs, services or trends;
 - e.g. Community Engagement (Division) - linking (PI) through 2 or more systems to create new data sets to evaluate programs, services or trends.

Data Matching (PI) Rules (POPA) - New

POPA Data Matching (PI) activities (MRU Operational examples)

Data = " <u>Collected</u> " Standard PI Rules	Data = " <u>Created</u> " New Data Matching (PI) Rules
Banner Data = <u>Collected</u>	The Office of Institutional Research and Planning = <u>Created</u>
Security Services (CCTV) = <u>Collected</u>	Community Engagement Division (Alumni) = <u>Created</u>
*Data <u>collected</u> and referred to for operational purposes *Unchanged or remains identifiable or integrated software or data moved - for operational purposes.	*Data <u>created</u> into new Datasets for analysis to evaluate trends. *Data contains personal information (PI) *Data <u>linked between 2 or more systems</u> *Data linkages *Anonymized Data (linked) used for evaluation of trends *The more <u>enterprise-wide</u> the greater the risk

Data Matching (PI) Rules (POPA) - New

POPA Data Matching (PI) > (NPD) activities Rules Framework...

Data = " <u>Created</u> " New <u>Data Matching (PI)</u> Rules	Data = " <u>Created</u> " New <u>Non-Personal Data (NPD)</u> Rules
<u>Creation</u> MRU may only <u>create</u> Data thru <u>Data Matching (PI)</u> for certain authorized purposes. (e.g. program evaluations)	<u>Creation</u> MRU may only <u>create</u> Data thru <u>(NPD)</u> for certain authorized purposes. (e.g. program evaluations)
<u>Retention & Use</u> MRU must only <u>retain the (PI)</u> from the Data Matching process for <u>only as long as reasonably necessary</u> for MRU to complete its intended purpose (anonymization is preferred).	<u>Use</u> MRU may <u>use</u> <u>(NPD)</u> for any purpose.
<u>Disclosure</u> MRU is <u>prohibited from disclosing</u> Data created from <u>Data Matching (PI)</u> . <i>*Disclosure allowed under limited circumstances.</i>	<u>Disclosure</u> MRU may only <u>disclose</u> <u>(NPD)</u> (externally) only under certain (limited) controlled circumstances.
<u>Protection</u> MRU must <u>protect</u> <u>Data Matching (PI)</u> by making reasonable security arrangements.	<u>Protection</u> MRU must <u>protect</u> <u>(NPD)</u> by making reasonable security arrangements.

An aerial photograph of a university campus, featuring various academic buildings, green spaces, and trees. The entire image is covered with a semi-transparent blue filter. The word "Questions?" is centered in white text.

Questions?