Fact Sheet: Data Matching and Data Derived from Personal Information

A public body may carry out data matching to create data derived from personal information under the *Protection of Privacy Act* (POPA).

What is "data matching"?

Data matching means linking personal information between two or more databases or other electronic sources of information.

Section 17 of POPA sets out the rules related to data matching and the creation of data derived from personal information by a public body. Sections 18 through 20 outline the requirements for retention, use, disclosure and protection of data derived from personal information. The Protection of Privacy (Ministerial) Regulation details requirements on data matching and management of data derived from personal information.

What is "data derived from personal information"?

Data derived from personal information means data created by data matching and identifies any individual whose personal information was used in the data matching. Both elements of the definition need to be met in order to be considered data derived from personal information, meaning it must be the merging of two or more sources to create new information about an individual. The personal information in the data must still be identifiable.

There is an important difference between the use of data derived from personal information and the use of personal information. Data derived from personal information can only be used for the purpose for which it was created, while personal information can be used for various authorized purposes, including for a use that is consistent with the original purpose of collection.

Authority to carry out data matching and creation of data derived from personal information.
Section 17(1) prescribes the circumstances when data matching can occur. If authority does not exist under this provision, then a public body cannot use data matching to create data derived from personal information.

Research and analysis:
Research means for the purpose of the systematic investigation and analysis or study of materials or sources in order to establish facts or to verify theories.

Analysis refers to the process of examining and interpreting collected information to identify patterns, relationships, and trends. It often involves breaking data down into smaller parts, comparing findings, and drawing conclusions.

The creation of data derived from personal information for research and analysis enables public bodies to make accurate and informed decisions.

Planning, administering, delivering, managing, monitoring or evaluating a program or service:
Planning means to think about and decide what to do or how to do something.

Administering means to control the operation or arrangement of something.

Delivering means to provide a service.

Managing means to be responsible for controlling or organizing something.

Monitoring means to watch and check something carefully over a period of time.

Evaluating means to judge or calculate the quality, importance, amount, or value of something.

One or more prescribed purposes
A prescribed purpose is one that is allowed through regulation. At this time, there are no prescribed reasons for a public body to carry out data matching.

Some examples of data matching activities:

- Mental Health and Addiction collecting personal information from Seniors, Community and Social Services' to data match the information from Navigation Centres to evaluate programs serving homeless populations.
- A public body using the personal information from its own programs to conduct data matching to determine if individuals are receiving overlapping benefits.

Collection of personal information for purposes of data matching

Section 17(3) outlines the authorities around collection of personal information for data matching. A public body cannot collect personal information directly from the individual the information is about for the purpose of data matching. It can only carry out data matching with personal information it collects from another public body or information it already has in its custody or under its control.

Privacy Management Programs

As part of their privacy management programs (PMPs), public bodies are required to establish a security classification system for data derived from personal information in the custody or under the control of the public body. Additionally, public bodies with custody or control of a high volume of personal information or highly sensitive information must include, in their programs, all policies related to data matching activities. See Fact Sheet: Privacy Management Programs.

Privacy Impact Assessments

Any practice, program, project or service that involves data matching between two or more public bodies requires a privacy impact assessment (PIA) to be prepared. This includes establishing a clear governance structure respecting the responsibilities and accountability of each public body engaged in data matching. A joint PIA may be prepared by the public bodies involved and addendums may be prepared to address any unique circumstances that apply to that public body. It is recommended that any agreements between public bodies related to data matching also be included with the PIA.

Any PIA prepared in response to data matching must be submitted to the Office of the Information and Privacy Commissioner. See Fact Sheet: Privacy Impact Assessments.

Retention of data derived from personal information

Section 18(2) of the Act requires that a public body must destroy the data derived from personal information or transform it into non-personal data once the original purpose has been fulfilled. The intent is to have the data destroyed or changed into data that no longer identifies an individual, as soon as it is practical, to protect it from unauthorized access, use, or disclosure.

Disclosure of data derived from personal information

Section 19(1) of the Act indicates that unless subject to the specifics of subsections (2) and (3), a public body is prohibited from disclosing data derived from personal information created under 17(1). Data derived from personal information cannot be disclosed under a formal access to information request under the *Access to Information Act.*

Section 19(2) only allows a public body to disclose data derived from personal information back to the public body that originally provided personal information if that public body requires it for the purpose it was created.

The intent is to allow the sharing of data derived from personal information to assist public bodies that are involved in the data matching. To ensure compliance with the Act, public bodies should implement a policy on the disclosure of data derived from personal information and ensure all authorities, uses and requirements for disclosure are clearly laid out in their PIAs.

For example: If public body A discloses personal information to public body B for the purpose of data matching to create data derived from personal information and public body A requires the data for the same purpose for why it was created, public body B is permitted to share the data with public body A.

Protection of data derived from personal information

Section 20 of the POPA specifies that the head of the public body must protect data derived from personal information and extends to all public body employees. It requires a public body to protect data derived from personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, or destruction. In addition, 17(2) of the Act also prescribes that data matching carried out to create data derived from personal information under 17(1) must be carried out in accordance with the prescribed security arrangements.

Some examples of such policies include:

- Limiting employee access of data derived from personal information to need to know only
- Regular review of the processes, forms, etc. related to the collection of personal information from another public body for the purpose of data matching to create data derived from personal information

- Regularly reviewing security measures, to ensure they are adequate
- Having a privacy incident procedure in place
- Having information management policies in place to securely destroy data derived from personal information when it is no longer required
- Requiring employees complete regular training related to their privacy protection obligations

Implementing such policies shows that a public body is taking its obligation to protect data derived from personal information seriously to strengthen its compliance with section 25 (Privacy Management Programs) of the POPA.

Public bodies must also ensure that contractors follow proper privacy protection procedures. When contracting for services involving data derived from personal information, public bodies should incorporate privacy protection provisions in the contract.

Additional resources

***Protection of Privacy Act* Guide**

Fact Sheet: Privacy Management Programs

Fact Sheet: Privacy Impact Assessments

Fact Sheet: Creation and Use of Non-personal Data

Fact Sheet: Disclosure of Non-personal Data