

# Privacy Definitions – Personal Information

NH Privacy Office – Spring 2022

## BC Freedom Of Information And Protection Of Privacy Act (FOIPPA) coverage

FOIPPA applies to all records in the custody or under the control of a public body.

## Record

includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records.

For example, each row of information stored in a computer database is typically considered to be a *Record*. For audio and video technologies, voicemail (or other audio recordings) plus video recordings, are also considered to be a *Record*.

## Custody

Physical possession of record; responsible for providing access to, security for, and disposal of the record.

## Control

Authority to manage, restrict, or regulate use or disclosure of record.

## Public body

Public sector in BC (Ministries, crown corporations, service providers etc.).

## Personal information (PI)

means recorded information about an identifiable individual other than [business] contact information.

personal information includes, but is not limited to:

- Nationality, ancestry, ethnicity, skin color
- Religious or political beliefs or associations
- Age, sex, gender, sexual orientation, marital status
- Fingerprints, blood type, DNA information, biometrics
- Health care, educational, financial, criminal, or employment history
- Anyone else's opinions about you and your own views or opinions

"personal health information" means recorded information about an identifiable individual that is related to the individual's health or the provision of health services to the individual.

Generally speaking, if information either identifies an individual (including through a unique identifier) or the information could, when combined with other available information, reasonably identify an individual, it will be personal information.

### Personal identity information

means any personal information of a type that is commonly used, alone or in combination with other information, to identify or purport to identify an individual.

personal identity information may include, but is not limited to:

- Name, age, sex, weight, height
- Home address and phone number
- Income, purchases and spending habits

### PI Direct Identifiers

These are variables that can directly identify individuals, either individually or in combination. A data set cannot be considered anonymized if these variables are included.

personal information direct identifiers may include, but are not limited to:

- Name, email address, telephone number, home address
- Social insurance number, IP address, personal health number

### PI Indirect Identifiers

These are variables that do not directly identify an individual but can be used for indirect re-identification. There is no universal definition of what indirect identifiers are - context is everything.

personal information indirect identifiers may include, but are not limited to:

- Date of birth, gender, place of residence or unique personal characteristic

Indirect identifiers may differ across data sets. For example, gender will not be as meaningful an indirect identifier if all of the individuals in the data set are female.

Releasing indirect identifiers may result in the 'mosaic effect', which posits that the release of even innocuous information can jeopardize Privacy if a knowledgeable reader can piece that information together with other data or prior knowledge.

### De-identification

De-identification is a process that removes or transforms direct and indirect identifiers in a record.

De-identification methods for data can include redacting or severing.

De-identification can result in:

- Partial de-identification
- Complete de-identification (anonymization)

### Anonymization

Anonymization is a de-identification process that removes or transforms all direct and indirect identifiers in a record that could be used, either alone or with other information, to identify an individual.

Only removing name, medical record number, or personal health number from a large data set helps to achieve only partial de-identification, and does not meet the requirements for anonymization.

For any follow-up questions, you may contact the NH Privacy Office by email at [Privacy@northernhealth.ca](mailto:Privacy@northernhealth.ca).