




**Anonymization:
Determining when PHIPA applies**

**Carole Lucock, LL.B,
LL.M
LL.D Candidate,
Faculty of Law
University of Ottawa**



Roadmap

1. Identifiability and the definition of personal health information?
2. Standard of de-identification / anonymization?
3. The act of de-identification / anonymization of information?

Caveats

- Not providing legal advice
 - Raising questions, no clear answers
- Not an overview of the application of PHIPA
 - Narrow focus is on identifiability & de-identification

Definition of Personal Health Information

“**IDENTIFYING** information about an individual in oral or recorded form if the information” relates to or contains information enumerated in PHIPA

(Enumerated; e.g. mental or physical health information, health history, health number)

PHIPA s. 4(1)

Definition of Personal Health Information

Identifying Information (covered or not) =

?

Definition of Personal Health Information

Identifying Information =

“Information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual.”

PHIPA 4(2)

Definition of Personal Health Information

Identifying Information (covered or not) =

??

Standard of de-identification / anonymization

- Loose use of terms (de-identify, anonymize)
- Use in different contexts

✓ Privacy protecting

✓ Excluded from PHIPA

Standard of de-identification / anonymization

Canadian Institutes of Health Research: *Best Practices for Protecting Privacy in Health Research* (September 2005)

Direct identifiers. These are variables such as name and address, health insurance number, etc., that provide an explicit link to a respondent.

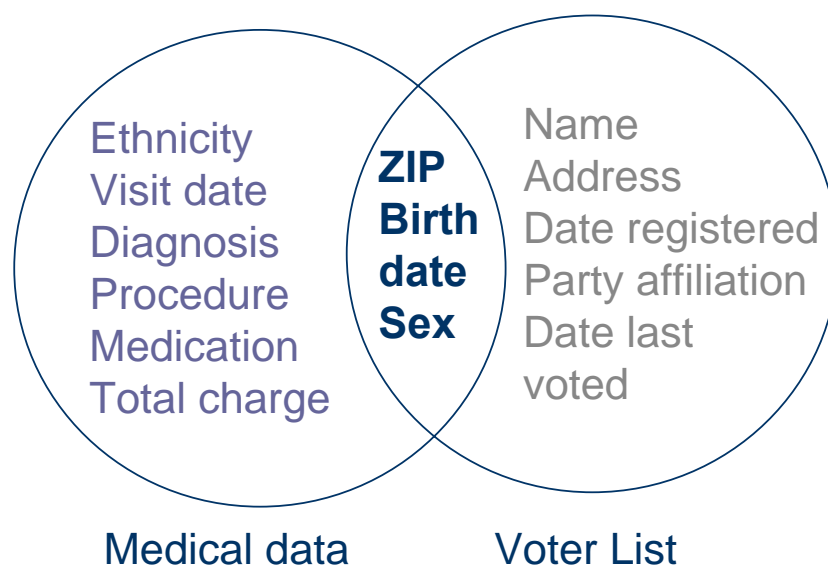
(Statistics Canada)

Indirect identifiers. These are variables such as date of birth, sex, marital status, area of residence, occupation, type of business, etc. that, in combination, could be used to identify an individual.

(Adapted from Statistics Canada)

Standard of de-identification / anonymization

Latanya Sweeney



L. Sweeney. *k*-anonymity: a model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*. 10 (5). 2002: 557-570. Figure 1.

Standard of de-identification / anonymization

What Standard?

- Dr. Khaled El Emam – availability of external source data
- Dr. Khaled El Emam – REB's lack of knowledge re variables, decisions based on intuition and hearsay, statistical methods not used
- Dr. Don Willison et al – REB's considerable variation in ability to recognize which variables to remove

Standard of de-identification / anonymization

What Standard?

- CIHR
- UK Data Commissioner
- US HIPPA

Standard of de-identification / anonymization

CIHR: Gradation of data identifiability according to capacity to re-identify

Directly identifiable to non-identifiable

(see handout, footnote 6)

Standard of de-identification / anonymization

CIHR

Non-identifiable: Any element or combination of elements that allows direct or indirect identification of an individual was never collected or has been removed, although some elements may indirectly identify a group or region. **There is no code** linking the data back to the individual's identity.

Standard of de-identification / anonymization

Note PHIPA s. 47: analysis of health system for Minister by a health data institute.

Results of analysis to be provided to Minister in de-identified form; however, health data institute would likely continue to hold the key

Standard of de-identification / anonymization

U.K. Data Commissioner

If there is any code linking back to an identifiable individual (even if there is no intention to re-link data) then the information continues to be personal information and subject to the act

Standard of de-identification / anonymization

U.S. HIPPA

If any of 18 data elements listed (handout p. 5) are excluded AND no knowledge that remaining information could be used alone or in combination to identify

Standard of de-identification / anonymization

U.S. *HIPPA*

Alternative to removing all 18 elements:

- Use of statistical methods
- Certification by expert
- “very small risk” of re-identification

The act of de-identification / anonymization

- Is it a use?
- Is it permitted without consent?

The act of de-identification / anonymization

Is the act of de-identification a use?

- Source Informatics
- Federal & Alberta Privacy Commissioners
- PHIPA
 - modifying to conceal is a permitted use
 - de-identification for specified purposes
a required use

The act of de-identification / anonymization

PHIPA

Consent required unless permitted or required

The act of de-identification / anonymization

- Complex
- Caution

QUESTIONS?