Foundation Working Group Meeting #4

Framework for De-identifying Information for Disclosure to Third Parties

July 22nd, 2015

ieso
Independent Electricity System Operator

Session Agenda

- De-Identification Definition Recap (WG Meeting #3)
- Objective: To provide input to the IESO on:
  - Proposed Principles and Requirements to de-identify data
  - De-Identification Process Requirements

Definition: De-Identified Information

"De-identified information is information that cannot be used to identify an individual, either directly or indirectly. Information is de-identified if it does not identify an individual, and it is not reasonably foreseeable in the circumstances that the information could be used, either alone or with other information, to identify an individual."

Source: Cavoukian, Ann, Ph.D., and Khaled El Emam, Ph.D. "De-identification Protocols: Essential for Protecting Privacy." 25 June 2014. Web:

https://www.privacybydesign.ca/content/uploads/2014/06/pbd-de-identifcation_essential.pdf

Proposed Principles and Requirements for De-Identification

- Based on review of research material and the guidance provided by the FWG Meeting #3 Panel on De-Identification, we suggest the following Principles and high-level Requirements for establishing a process for De-Identification.
- We would like input from the FWG on these Principles and high-level Requirements.
- Proposed requirements are mapped to applicable standard or best practice guide. Referenced sources are provided in the Appendix.

De-Identification Principles

- Enable appropriate use of data while maintaining public trust, privacy and confidentiality.
- Ensure that identifiable data is held securely with access restricted to authorized organizations and users.
- Establish a documented, clear, transparent process for de-identification with objective measures of risk.
- Manage risk of providing data access and minimize those risks where possible, while acknowledging that risks cannot be entirely eliminated.
- Leverage available standards and best practices for de-identification process and techniques.

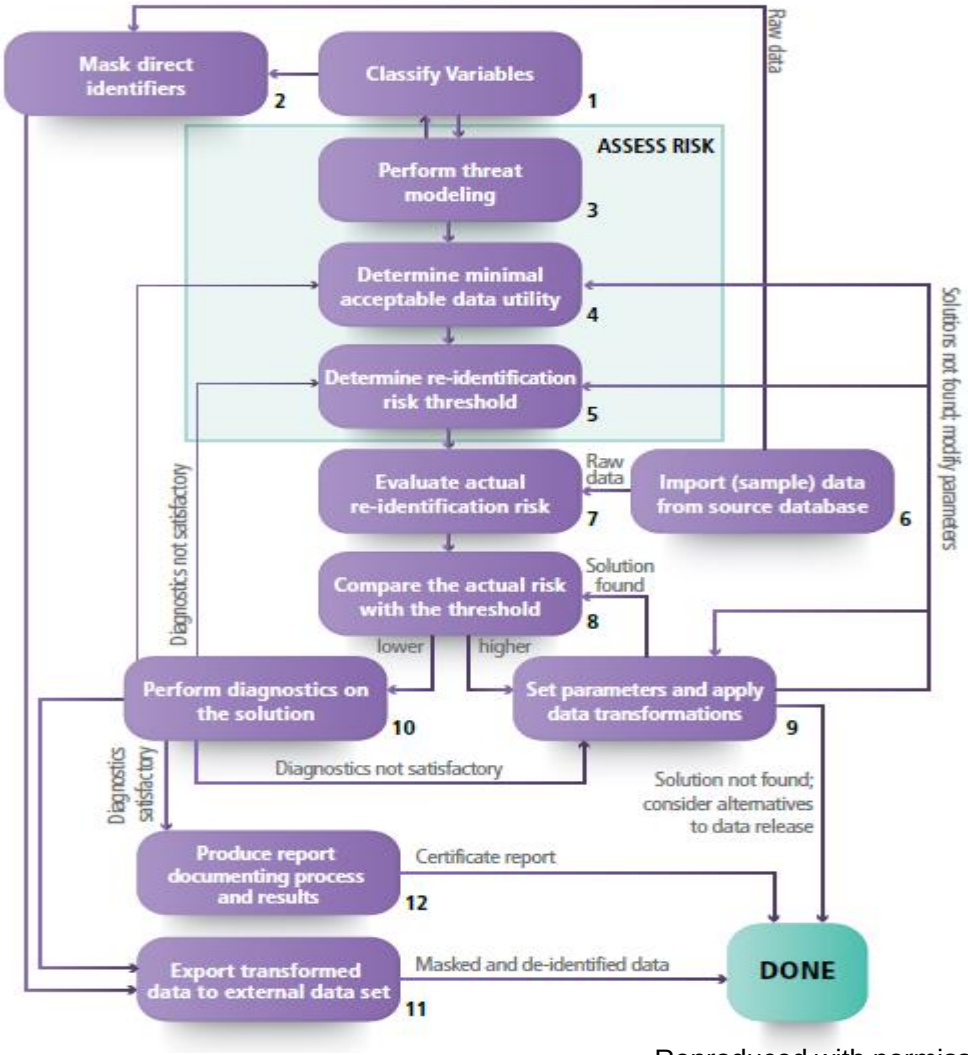
De-Identification Process Requirements

- Define the roles and responsibilities of the data custodian, data requestors and recipients.[Canadian Institute for Health Information (CIHI) 5.1, UK Information Commissioner's Office (ICO) 8]
- Define the activities for managing and fulfilling data access requests. [CIHI 5.1, ICO 8]
- Require the identification and classification of data fields that are direct identifiers and quasi-identifiers. [CIHI 6.2]
- Determine the acceptable data utility for each data access request. [CIHI 7.1, US Department of Health and Human Services (HHS) 2.8, ICO 2]
- Document and disclose the de-identification methodology without exposing specifics that could lead to re-identification. [ICO 3, Working Paper 22 (WP22)]
- Periodically review the process and methodology against current and foreseeable threats. [ICO 3, WP22]

De-Identification Process Requirements

- Inherent Risk Assessment [CIHI 3, HHS 2.6, CIHI 13, HHS Table 1, HHS 2.7]
  - Identify plausible adversaries and plausible attacks on the data
  - Determine re-identification risk threshold or tolerance
  - Evaluate re-identification risk
  - Compare evaluated risk with risk threshold
- Risk Mitigation [CIHI 6.1, ICO3, CIHI7.1, HHS 2.9, ICO, WP22]
  - Define a set of data transformations for de-identification to reduce the risk to an acceptable level
  - De-identify data by applying appropriate data transformations
  - Use comprehensive and enforceable data user-custodian agreements to ensure that users maintain the confidentiality of the information that they receive.
- Residual Risk Assessment [CIHI 8.1]
  - Assess residual risk and data utility after application of risk mitigations.

Sample De-Identification Steps



Reproduced with permission of El Emam 2015

Appendix - Why Standards Are Important

- Custodians hesitating because “there are no standards” and thus choose not to share or restrict sharing
- Improve actual de-identification methods used in practice
- Provide guidance for regulators when evaluating what is acceptable practice for de-identification
  - Helps alleviate the concerns when standards are followed
  - More defensible
- Establish community of practice around common approaches for de-identification
- Define body of knowledge for de-identification practices to lead to certification and accreditation

Appendix - References

- Canadian Institute for Health Information (CIHI)
- The Council of Canadian Academies, “Accessing Health and Health-Related Data in Canada - The Expert Panel on Timely Access to Health and Social Data for Health Research and Health System Innovation.” December 2014. http://www.scienceadvice.ca/en/assessments/completed/health-data.aspx
  - Discussion on sharing data for healthcare, de-identification methods (specifically a process for risk-based analysis)
  - Best Practice Guidelines from CIHI (Canadian Institutes for Health Information; risk based approach for de-identification and some specific techniques
- Health Insurance Portability and Accountability Act of 1996 (HIPPA)
- HITRUST “De-identification Framework”, A Consistent, Managed Methodology for the De-Identification of Personal data and the Sharing of Compliance and Risk Information. https://hitrustalliance.net/

Appendix - References

- Institute of Medicine of the National Academies "Sharing Clinical Trial Data – Maximizing Benefits, Minimizing Risk – Committee on Strategies for Responsible Sharing of Clinical Trial Data." 2015. https://www.iom.edu/~/media/Files/Report%20Files/2015/SharingData/ElEmamandMalin%20Paper.pdf
- Khaled El Emam, Ph. D.
  - "Guide to the De-Identification of Personal Health Information", 2013
- Khaled El Emam & Luk Arbuckle
  - "Anonymizing Health Data, Case Studies and Methods to Get you Started", 2013
- Office for Civil Rights (OCR)
- PARAT Methodology and Software
- PhUSE – Pharmaceutical Users Software Exchange
  - Standards for CDISC Documents; start with Safe Harbour and then recommends Expert Determination but does not require it

Appendix - References

- Privacy Analytics Inc. (www.Privacy-Analytics.com)
  - "An Overview De-identification Standards for Health Data", 2015 Training.
  - "The Twelve Characteristics of a De-Identification Methodology Whitepaper."
  - "De-Identification 101, 201, 301, 401 Whitepapers"
- Privacy by Design (Ontario's Information & Privacy Commissioner of Ontario) (www.privacybydesign.ca)
  - "De-Identification Developments", 2013.
  - "De-Identification Protocols: Essential for Protecting Privacy", 2014
- UK Information Commissioner's Office (ICO) Code of Practice
  - Principles and methods for de-identification
- US Department of Health and Human Services (HHS)
- Working Paper 22 (WP-22) from Federal Committee on Statistical Methodology
  - Specific techniques for de-identification, Cited in HIPPA