UNITY HEALTH TORONTO

PRIVACY GUIDELINE: Minimum Requirements for the Governance of Research Biobanks and Databanks

Created July 2020; updated August 2023

Purpose

This guideline describes the minimum privacy requirements for the governance of biobanks (also known as biorepositories) and databanks (also known as data repositories, registries and databases), as well as sub-studies. This guideline recognizes that additional requirements must be adhered to for the certification and sustainment of biobanks, which are outside of the scope of the biobank's privacy governance controls.

Definitions

A "***databank***" is an organized collection of identifiable and quasi-identifiable information from multiple patients/participants with something in common (e.g., a disease state), the creation of which is not dependent on a specific hypothesis or research objective, as the purpose is to have the information stored long-term and readily available for future studies (sub-studies). A "databank" may refer to multiple stores of data that are linked under a single project, as in the case where identifiers are stored in a linkable format in a separate location.

A "***biobank"*** a collection of samples from multiple patients/participants that is created for long-term storage and makes samples available for future studies (sub-studies) on specific hypotheses or research questions.

A ***"data access committee"*** (DAC) is a group, with a distinct scope to review requests to use and/or disclose data within a databank or biobank, by following a defined decision-making process.

Background

The following requirements are the minimum controls needed to address the unique privacy risks related to databanks and biobanks, in addition to REB approval, based on law, expectations from privacy commissioners, and emerging best practice that must be implemented. Other controls may be needed and will be identified by the Privacy Office. Exceptions to the requirements must be evaluated.

For the purposes of this guidance, databanks and biobanks will be collectively referred to as "the repository".

Requirements

1. The scope of the data and the data elements collected or created must be justified and limited to the minimum amount needed to meet the purpose.
2. A 'Data Access Committee' (DAC) or similar body must be established for the oversight of the repository.
    - The DAC should be comprised of a minimum of 5 diverse members, with some voting members not investigators involved in the creation of the registry ('core investigators')
        - Membership cannot be comprised of PIs, Co-PIs, or study staff only.
        - At least one member must be a community/unaffiliated scientist or expert.

    - Repositories with complex technical architecture or consent process must have a privacy expert from a data-contributing or managing organization.
    - Membership can include a community member, where appropriate.
  - The DAC will review and approve access requests. REB approval, consistency with the original intent of the repository, data limitation, and no apparent risk of bias against a certain group, or re-identification, will be taken into account.
  - The DAC will review and approve amendments to the repository's architecture, controls or procedures (including but not limited to sub-study requests, data collected, technical architecture, privacy or security controls, access to the systems)
  - The DAC will review and approve policies, processes, and protocols of the repository (including but not limited to processes for user access provisioning, roles and responsibilities of maintaining the repository, and procedures for extracting, transferring or otherwise providing access to the data).
3. Principal site should implement the following agreements to clarify roles and responsibilities:
  - A data sharing agreement must be established with sub-study researchers and any other data recipients, which limits the use of the data disclosed to that which is approved by the REB and DAC.
  - Individuals working to build or support the repository must sign a Confidentiality Agreement and receive privacy training.
  - A service agreement must be established with vendors and third party service providers providing products and/or services in relation to the repository that includes the standard clauses contained in the Information Practices Schedule.
4. Identifiable data elements should be segregated.
5. The participant should be aware of the policies and processes implemented to protect the data and of their rights.
  - Fulsome, express consent must be obtained, unless sufficient justification (and REB approval) is provided
  - Participants must be able to withdraw consent for participation in the repository. Withdrawal must result in deletion of the identifiers and related data. (Participants may be told that extracts of data previously provided to sub-studies may still be used.)
  - Contact information for the repository PI and/or team must be made public to support participants with questions or seeking to withdraw consent.
  - A publicly published list of sub-studies using the data must be maintained (e.g. on a website or in an accessible brochure)
6. Data should be collected, transferred and retained in a secure manner (including but not limited to encrypted at rest and in transit).
7. Data should reside in Canada.
8. Where data will be collected from participants in the European Union, GDPR requirements must be met.

UNITY HEALTH TORONTO

Sub-Study Requirements

1. The purpose of a sub-study must be reviewed by the DAC to verify the purpose aligns with the primary repository's original intent, as consented to by the participant.
2. REB approval must be obtained for the sub-study.
3. A Data Sharing Agreement (DSA) must describe the purpose and expected requirements that will apply to the sub-study data recipients to ensure alignment with the primary repository, and no unplanned linkages or re-identification will occur.

Sources

Canadian Standards Association Model Code for the Protection of Personal Information. **https://www.msccanada.org/PRIVACY/CSA-CODE.pdf** - establishes the foundational principles for Canadian privacy legislation, including the *Personal Health Information Protection Act, 2004*.

Global Alliance for Genomics and Health- Framework for responsible sharing of genomic and health-related data. https://www.ga4gh.org/genomic-data-toolkit/regulatory-ethics-toolkit/framework-for-responsible-sharing-of-genomic-and-health-related-data/#fp - establishes a set of foundational principles for responsible research conduct and oversight of research data systems in the realm of genomic and health-related data sharing.

Information and Privacy Commissioner of Ontario- Manual for the Review and Approval of Prescribed Persons and Prescribed Entities- https://www.ipc.on.ca/resource/manual-for-the-review-and-approval-of-prescribed-persons-and-prescribed-entities-2/- establishes program requirements to oversee and manage a repository of data (registry) used for secondary purposes.

Information and Privacy Commissioner of Ontario- De-identification Guidelines for Structured Data. https://www.ipc.on.ca/wp-content/uploads/2016/08/Deidentification-Guidelines-for-Structured-Data.pdf - describes the recommendations for taking a risk-based approach to de-identification.

Information and Privacy Commissioner of Ontario- Big Data Guidelines. https://www.ipc.on.ca/wp-content/uploads/2017/05/bigdata-guidelines.pdf - describes the recommendations and issues for big data.