Research Databank and Biobank Governance Plan

**How to use this template:** instructions for each section are in grey and should be removed when this document is finalized. <> placeholders should be filled in by the Study Lead.

|  |  |
| --- | --- |
| **Background** | The following outlines the governance plan of the Data Access Committee (DAC) that will apply to circumstances where the <databank / biobank name> are created for a study and stub-studies.  This governance plan will ensure there is oversight for <databank / biobank name> and related databases as a result of sub-studies. |
| **Mandate** | DAC will oversee the primary <databank / biobank>, including reviewing requests to use and/or disclose data within the <databank / biobank> . |
| **Composition** | Members include:  *The following are the minimum number of members that should be included*   * <4 investigators> * <1 privacy expert from a data-contributing or managing organization> * <1 community/unaffiliated scientist> |
| **Decision Making** | * Quorum will be 50% of membership * Decisions and approvals will be made by <majority/consensus/unanimously> and must be made by no more than 50% of the core investigators |
| **Role & Responsibilities** | DAC will review and approve:   * Decisions about changes to the <databank / biobank> including:   + the purpose / future uses of the <databank / biobank>   + the data elements collected or generated   + technical architecture (including data flows and/or user roles), and   + users requesting access to the <databank / biobank> or data * Procedures to provide access to the data (extracts or direct access), including:   + Submission of proof of REB approval   + Proof of consistency with the original purpose the <databank / biobank> , and identify conflicts of interest   + Method of extracting and providing data (if applicable)   + Method of providing and revoking direct access to the <databank / biobank> (if applicable)   + Method of tracking and logging requests for access to the data or <databank / biobank> * How access will be limited, namely:   + If direct access to data is provided to sub-study researchers, access should be limited to de-identified information only. If that is not possible, access should be limited to the data elements listed in the REB approved research plan.   + If data is extracted to be provided to a sub-study researcher, only de-identified data should be provided. If identifiers are required and approved by an REB, identifiers listed in the REB approved protocol may be provided along with the approved data elements. * Whether the <databank / biobank> will reside with the institution or with the PI, if the PI leaves the institution.     DAC will review and advise on:   * Agreements related to the <databank / biobank>, including   + Data Sharing Agreements with recipients of the data.   + Service Agreements with vendors and other third party service providers. * Changes to policies, processes and standard operating procedures for the <databank / biobank>. * Risks associated with the <databank / biobank> including those identified in Privacy Impact Assessments. |
| **Meeting Frequency** | * Meetings will be held < prior to the REB approval of a sub-study>. |
| **Date of last review** | * Governance Plan to be reviewed annually by committee membership and approved by <committee/ oversight body/REB>. * Last Reviewed: <MM/DD/YYYY> |

# Data Sharing Agreement

At a minimum, the Data Sharing Agreement should include the following terms:

* Agreement that identifiable data will adhere to the requirements of the original <databank / biobank> including:
  + Purpose for sharing.
  + Consent will be obtained from participants to share the information.
  + Users with access to the information will be limited.
* Agreement that only the information necessary will be shared.
* Agreement that attempts to re-identify anonymized data should not be made unless where expressly authorized by law.
* Agreement that de-identified data will not be re-identified.
* Agree that all actual or suspected privacy breaches will be reported to the Privacy Office and that the recipient will support managing the privacy breach, as required.

# <Databank / Biobank> Privacy Procedures

The following procedures should be in place to manage the operations of the <databank / biobank>:

* Consent management: procedures for obtaining consent, consent messaging that will be provided to the participant, and procedures for managing the withdrawal of consent.
* Retention, Transfer and Destruction: procedures for the transfer, deletion and destruction of information.
* User Access Management: procedures for user access provisioning and de-provisioning to the <databank / biobank>.
* Auditing: procedures for providing logs and/or reports of user activity in the <databank / biobank> to the Privacy Office.