

# IRB Application Template

Below is boilerplate language prepared by Databrary that researchers can use to help draft applications to their institutional review board (IRB). This document is intended to help researchers who plan to store and share video data in Databrary prepare IRB materials for approval.

Researchers should confirm institution/agency/directorate/program-specific application requirements before submission.

Please contact us at [contact@databrary.org](mailto:contact@databrary.org)<sup>1</sup> for further assistance.

## Secondary Reuse.

This project will conduct secondary analyses of participant data obtained from Databrary, an online platform for the storage, sharing, and re-use of video and other research data. Participants' consent for study participation and release of data were obtained by the original researcher under the oversight of their institutional review board. Because there is no direct contact with participants as a part of this project, the level of additional risk to participants is low.

## Primary data collection.

Data will be handled by the team of researchers approved on the IRB protocols of all Principal Investigators and Co-Investigators. Data are linked to participants by subject ID. However, video data are potentially identifiable because participants' faces are visible and their names may be heard. With participant consent, study data will be stored on Databrary<sup>2</sup>, a secure web-based video library housed at NYU, allowing permission-based access to coders from all labs comprising the project team. At the end of each lab visit, caregivers will be asked whether they are comfortable: 1) storing their videos and children's birthdates and other metadata on Databrary, and 2) sharing their data with authorized researchers outside of this protocol who are members of the academic research and clinical communities authorized to access Databrary. If caregivers agree to video sharing, the videos will be made available to authorized researchers as outlined below. If caregivers do not agree, their videos will be accessible only by researchers on the project protocol and not shared with the larger community. The policies for sharing videos and other potentially identifiable data on Databrary<sup>3</sup> have been carefully developed and monitored with the advice of the legal counsel, grants/contracts office, and IRBs of both New York University and The Pennsylvania State University. Currently, more than 360 institutions in the U.S. and around the world have formally approved the Databrary Access Agreement to enable video sharing and reuse. Parents also will be told that they can share portions of data or ask for particular sessions not to be shared while sharing other sessions.

## Policies for Databrary access and data sharing.

Sensitive or identifiable data shared with Databrary will only be viewable to and downloadable by authorized users who have been granted secure access by Databrary's administrators. Select data may be made available to the public, but only as determined by the researcher and on the basis of participant permission. Only researchers with Principal Investigator status from institutions with Institutional Review Boards or similar review entities, and researchers affiliated with Principal Investigators and under their supervision, are authorized for access.

Authorized users are required to sign a user access agreement that specifies that they will: (1) be responsible for maintaining the confidentiality of the data; (2) abide by ethical principles for treatment of human subjects as mandated by their local Institutional Review Boards; (3) agree not use the data for commercial purposes; and (4) treat data in Databrary with the same high standards of care that they would treat data collected in their own laboratories.

Only videos and other identifiable data that have been permissioned for sharing by all the depicted individuals in each recording are made available to the community of authorized Databrary users. In consultation with ethics board officials at New York University and the Pennsylvania State University, Databrary has developed template Sharing Release forms<sup>4</sup> that contributors can add to their IRB protocol. These forms allow researchers to ask participants for permission to share their data.

---

<sup>1</sup><mailto:contact@databrary.org>

<sup>2</sup><https://nyu.databrary.org/>

<sup>3</sup><https://databrary.org/about/policies.html>

<sup>4</sup><https://databrary.org/support/irb/release-template.html>

Federal policies do not require re-consenting of minor participants when they reach the age of majority, if re-consenting is impractical or otherwise increases risks to participants (e.g., by requiring researchers to maintain links between identifiable information and collected data for extended time periods).

### **Policies and provisions for reuse and redistribution.**

Access to videos and metadata will be available for educational and research purposes, subject to participant consent. Such access will be provided using the Databrary web-based application. Materials generated under the project will be disseminated in accordance with the policies of [GRANT-GIVING ORGANIZATION] and participating institutions. Publication of data shall occur during the project, if appropriate, or at the end of the project, consistent with normal scientific practices.

### **Archiving and preservation of research data.**

Data in Databrary will be preserved indefinitely in a secure data storage facility at New York University (NYU); the facility is managed by the university's Information Technology Services department. Central IT staff handle storage, network, and backup systems. NYU does routine tape backups that are stored off site and performs regular file fixity checks to monitor the integrity of stored assets. Federal regulations do not require that data be destroyed after a particular time period if they are stored indefinitely in a recognized repository.

### **Data Security.**

Data and metadata stored in Databrary are subject to the security policies and best practices implemented by NYU. For more information about these policies and services, please visit NYU ITS Computer & Network Security at <https://www.nyu.edu/life/information-technology/cybersecurity.html>.