Best Practices for Data Security

Databrary requires all Databrary *authorized investigators* and *affiliates* to embrace best practices for data security.

Protect Confidentiality

Databrary contains identifying information, thus special care must be taken.

- Participants should be identified by a code that does not include names, initials, birthdates, phone or ID numbers, etc.
- Identifying information should be removed from text/flat files before it is shared with Databrary.
- If you collect sensitive information on paper, lock the paper records in file cabinets and ensure that the file cabinets are located in locked rooms that are not readily accessible to unauthorized people.

Password Generation

- Use a unique password or passphrase for Databrary.
- Do not share your password with others.
- Choose a password that has capital and lower case letters, special characters and numbers and is long, greater than 10-12 characters.
- Do not write your password down.
- Do not store your password in an unencrypted file on your computer.
- Change your password at least every 6 months.

Computers Used to Access and Download Databrary files

- Computers should have individual-level, password-protected user accounts.
- Computer account IDs or passwords should not be shared.
- Computer account passwords should differ from those used for Databrary (see above).
- Laptops may be stolen or lost, so it may be wise to enable system-wide file encryption.
- Set your computer to activate a password protected screen saver after 3 minutes of inactivity.
- Disable automatic log-in.
- Set your computer to automatically logout after 5 minutes of inactivity.
- Databrary logs the Internet Protocol (IP) addresses of computers that access the system, so you may wish to choose a specific computer or computers to use to access Databrary.

Data File Storage and Backup

- If flat-file data are stored on laboratory computers, those computers should be regularly (daily or weekly) backed up to a secure location offsite.
- More than one backup copy should exist. All backups should be secure.
- Since Databrary stores high resolution copies of recordings that can be downloaded at any time, recordings taken from Databrary need not be backed up. Indeed, creating multiple backups of recordings from Databrary increases the risk that sensitive information may be released inadvertently.

Physical features of laboratory or office

- Laboratories or offices that house computers where data are stored should be locked whenever the rooms are unoccupied.
- Laboratories or offices that house computers where data are stored should not be readily accessible to unauthorized people who are not supervised by a researcher.
- Be aware of whether the layout of your laboratory or office inadvertently allows other individuals to see your computer screen or reflections from your computer screen through doors or windows.