Databrary

Best Practices for Data Security

Data security evolves. This document represents a set of best practices that Databrary recommends all *Authorized Researchers* and *Sponsored Researchers* adopt:

Personally Identifying Information (PII)

- PII consists of the following:
  - Full name
  - National identification number (e.g., Social Security number)
  - Internet Protocol (IP) address
  - Vehicle registration plate number
  - Driver's license number
  - Health certificate or insurance number
  - Fingerprints, or handwriting
  - Credit card or financial account or access numbers
  - Digital identity (e.g., Facebook, Twitter, LinkedIn, email account names)
  - Date of birth
  - Birthplace
  - Address
  - Telephone number
- And, faces and voices.
- Special care must be taken with PII.
  - Participants should be identified by a code that does not include PII – names, initials, birthdates, phone or ID numbers, etc.
  - Personally identifying information (PII) should be removed from text/flat files before it is shared with Databrary. This is called *de-identifying* data.
    - The exception to this concerns **date of birth**, which is vitally important for developmental research. Date of birth need not be removed from text/flat files.
  - If you collect PII 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.
  - No PII may be included in audio or video recordings or photographs with these exceptions:
    - Names and voices in audio or video recordings or photographs need not be removed before sharing with Databrary.
    - If date of birth information is recorded, that also need not be removed from recordings prior to sharing with Databrary.

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.
- Some experts recommend using a password manager/generator.

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 identifiable information may be released inadvertently.
- You may take screen shots, but if the screen shots contain PII, they must be stored securely.

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.