Researcher Guidance for Data Handling

**This guidance may be updated with additional information as it becomes available.*

Introduction

Researchers should follow data handling guidelines for several reasons, including 1) protecting participant confidentiality, 2) ensuring data accuracy and quality, 3) complying with legal and ethical requirements, and 4) facilitating data sharing and reproducibility. These guidelines apply to all data collected in the course of research, including records, interview data, survey responses, and more.

Data Classifications

All data, regardless of the platform, must be handled in accordance with policy related to its classification. We have 3 data classifications at Pepperdine: Public, Confidential, and Restricted, and policies for how to properly handle each classification.

Public data refers to information that is freely available to the general public and can be accessed and shared without restrictions. This may include things like news articles, government reports, or social media posts.

Confidential data is information that is considered sensitive and should only be accessed by authorized individuals. This may include some forms of personal identifying information (such as audio recordings of interviews, most survey/questionnaire responses, contact information (phone numbers, email and physical addresses), text messages and email content, digital images, financial information (such as bank account numbers or credit card information), proprietary information (such as trade secrets or confidential business plans), and other personal information or data that is *not* protected health information (which is governed by HIPAA).

Restricted data is a subset of confidential data and refers specifically to information that is subject to legal or regulatory restrictions. This may include things like classified government documents, sensitive research data, or information protected by privacy laws such as HIPAA. In general, the level of protection required for data depends on the potential harm that could result if the data were compromised. Public data can be freely shared because there is no potential harm, while confidential and restricted data require more stringent security measures to ensure that they are protected from unauthorized access.

Data Handling for Confidential Data

The majority of the data that researchers at Pepperdine will be gathering and storing is Confidential in nature. All Confidential data must be stored with password protection. Password protection examples includes data stored on a personal or Pepperdine-issued computer (that is

properly configured to require a user/password for login), Google Drive (with sharing permissions set properly), GMail, University provided network share drives (S or U drive), Pepperdine-issued Zoom account cloud (for zoom recordings only, please see *Zoom Guidance document* for more information), and many more. Confidential information should only be made available to those users who are authorized to have access, and must be protected by a username/password for access.

Audio/Video Recordings and Data Retention

Audio and video recordings are considered confidential, identifiable data and must be handled in accordance with institutional data protection requirements.

In many qualitative studies, recordings are used as an intermediary step to create transcripts or coded data. In such cases:

- The de-identified transcripts and analytic materials are considered the official research record and must be retained for at least three (3) years in accordance with 45 CFR 46.115(b).
- Audio and video recordings are not required to be retained in their original identifiable form, unless necessary for scientific, regulatory, or funding purposes.

Because recordings contain identifiable information and present increased confidentiality risk, the IRB may recommend or require that recordings be deleted after transcription and verification.

If a researcher intends to retain recordings, a clear justification must be provided in the protocol and additional safeguards may be required.

Data Handling for Restricted Data

For Restricted data, additional controls are required for the storing and transmission of the data. Restricted data requires encryption at rest and in transit. If Restricted data is ever to be downloaded, stored, or printed, a University owned and managed device with Whole Disk Encryption must be used. You may send Restricted information using Pepperdine's Secure Attachments system, but only in attachments to the message (the message body is not permitted for Restricted information transmission or storage), and any recipients must be authorized to receive and properly handle the Restricted information.

If your study involves Restricted data, please contact the IRB office to discuss additional precautions for restricted data (e.g., limits on downloading, transforming, and altering data) and rules for sharing among researchers (e.g., cannot be shared with those outside of the University).

Additional Resources

Here are some additional resources for your reference to the policies. If you have any questions regarding any data handling, please contact the IRB office and the office can facilitate a more in-depth discussion with Pepperdine's Information Security team.

Information Classification and Protection Policy
https://community.pepperdine.edu/it/security/policies/icpp.htm

Information Classification and Protection Policy Schedules

https://community.pepperdine.edu/it/content/information-classification-protection-schedules.pdf

Google Workspace Information Storage Policy
https://community.pepperdine.edu/it/tools/gsuite/drive/storagepolicy.htm

Google Workspace Information Security Standards
https://community.pepperdine.edu/it/tools/gsuite/drive/securitystandards.htm

Restricted Information Cleanup & Control
https://community.pepperdine.edu/it/security/ric/