University of Wisconsin-Oshkosh
Institutional Review Board (IRB)

STANDARD OPERATING PROCEDURES (SOPs)	
SOP Number: 15 Effective Date: 12/7/21 Last Reviewed: 12/7/21 Attachment: Page 1 of 3 Prepared By: Kelly Schill	**Title:** **Guidance for Protecting Privacy and Confidentiality**

Guidance for Protecting Privacy and Confidentiality

I. Purpose of Guidance:

This guidance is intended to assist researchers in developing a research protocol plan which protects the privacy of research subjects and confidentiality of the data. Criteria for IRB approval is regulated under HHS regulations 45 CFR 46.111(a)(7) and FDA regulations 21 CFR 56.111(a)(7).

The IRB is responsible for evaluating proposed research to ensure that adequate provisions are in place to:

1) protect the **privacy** interests of research subjects, and
2) maintain the **confidentiality** of identifiable data

II. Definitions to Assist with Completion of UWO's IRB Research Protocol Application
(IRB Application: Part X: Privacy of Subjects/Confidentiality of Data)

1) Privacy (applies to the human research subject)

Privacy refers to an individual's desire to control the access of others to themselves. This includes access to the individual's personal/private information. For guidance on what information is considered personally identifiable information (PII) and protected health information, see IRB Identifiers Guidance.

The researcher should outline strategies to protect privacy, including how the investigator will access information from or about participants. In developing strategies for the protection of subjects' privacy, consideration should be given to:

- The methods used to identify and contact potential participants.
- The settings in which an individual will be interacting with the researcher.
- The appropriateness of all personnel present for research activities.
- The methods used to obtain information about participants.
- The type of information being collected, with special consideration for personal, sensitive and/or identifiable information.
- Private health information (PHI) collected from a HIPAA-covered entity must follow the safeguards outlined in the HIPAA Privacy Rule. Information considered PHI is outlined in the IRB HIPAA Quick Reference Guide.
- A plan to access only the information necessary to conduct the study.

Discipline specific privacy guidelines, often developed by professional associations, may be helpful and referenced in the research protocol (i.e., psychology, anthropology, oral history, etc.).

2) Confidentiality (applies to the handling of data/identifiable private information)

Confidentiality refers to the researcher's agreement with the participant about how the research participant's identifiable private information will be handled, managed, and disseminated. In other words, it refers to how and where research documents and data will be stored.

The researcher should outline strategies to protect confidentiality and include this information to the potential research subject in the informed consent document. In developing strategies for the protection of subjects' data, consideration should be given to:

- The methods of data collection (paper, audio, video, digital).
- The methods for protecting data throughout the research process (during data collection, data analysis, data transfer, data storage, and data retention).
  - Is it necessary to record identifiable information in the research record?
  - Who will have access to identifiable information in the research records?
  - If coding, use of pseudonyms, and/or other data protections will be in place, include those details. Who will have the key to identifiers and the ability to link the data to the direct identifiers?
  - How will you minimize re-identification risks?
  - Will audio or video be recorded for transcription purposes? If so, how will the files be stored and how will they be protected. Will files be deleted immediately following transcription?
  - If signed consent forms will be used, details about storage, protection, and retention of the signed consent forms should be addressed.
  - What will be done with the data during and after a research project? A data management plan should be in place when working with private, identifiable information.

If identifying information of a sensitive nature will be collected from research subjects, and the disclosure of such information could harm the research subjects, the researcher may wish to apply to the federal government for a Certificate of Confidentiality (CoC). The researcher should indicate in the application to the IRB that they will seek a CoC after the IRB has approved their application. Some grant agencies automatically issue a CoC at the time of award: https://grants.nih.gov/policy/humansubjects/coc.htm

3) Data Management Plan (data use during and after project)

A data management plan outlines what a researcher will do with data during and after a research project. A data management plan is a best practice and is required by many funding agencies.

Below is a list of typical data management plan considerations: (Note: funding agencies may have specific guidelines or elements to include in a data management plan).

- Roles and Responsibilities: Who will be responsible for aspects of data management throughout the project and what resources will be used?
- Data Type/Source: What is the source of your data and what types of data will be collected?

- Formats and Standards: What standards will be used for your files and metadata? How will data be organized?
- Data Storage and Security: How and where will you store and secure your data?
- Privacy and Confidentiality: What protections are in place for privacy and confidentiality?
- How may other researchers use your data? How many other researchers may access your data?
- Dissemination Methods: How will you provide access or share data with other researchers? Is intellectual property involved? How will the data be disseminated/made available and discoverable to the research community?
- How will the data be preserved for long-term access?

The NIH has the following resource for developing a data management plan:

- NIH Data Sharing Policy and Implementation Guidance

References:

This guidance was developed in part using material from the following resources:

1. UW-Madison:
   Privacy vs. Confidentiality; https://kb.wisc.edu/sbsedirbs/43425

2. University of Kentucky:
   Privacy vs Confidentiality (uky.edu)

3. Cornell University:
   Data Management Planning | Research Data Management Service Group (cornell.edu)

4. MCW:
   https://www.mcw.edu/-/media/MCW/Departments/Human-Research-Protection-Program/Researchers/IRB-SOPs/IRB-SOP-Privacy-and-Confidentiality-FINAL.pdf?la=en

5. NIH Data Sharing Policy:
   NIH Data Sharing Information - Main Page