**UMW Institutional Review Board**

**Anonymity, Confidentiality, & Privacy**

***Anonymity***

To preserve anonymity of participants, researchers do not collect ***any*** identifiers (e.g., name, address, telephone number) that link responses to a specific individual. Even the researcher does not know the identity of the respondents.

Data collected *in person* (e.g., interviews, video-recording, etc.) can never be "anonymous." If researchers record a list of codes associated with identifiers (e.g., names), those data are *not* anonymous.

If a *combination of indirect identifiers* (e.g., gender, race, age) could identify a specific respondent, particularly with small samples, researchers should not identify the study data as anonymous.

When data are not anonymous, participants may experience risk if a breach of confidentiality occurs and their identifiable information is released without their permission.

**Direct Identifiers:** See here for the [18 personal identifiers designated by HIPAA](https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html%22%20%5Ct%20%22_blank%22%20%5Co%20%2218%20HIPAA%20identifiers), as well as a definition of PHI (Personal Health Information).

**Indirect Identifiers:** Even when researchers do not collect direct identifiers (see above), a combination of other data could reveal a participant's identify, especially with small sample sizes: gender, age, race/ethnicity; size of town, community character (e.g., industrial, agricultural center, suburban, education community), and general location; characteristics of family structure (size, sex distribution of children, ages, marital evolution); details of personal characteristics or expressions of individuality.

***Confidentiality***

Confidentiality represents an agreement (via informed consent) between the researcher and potential participants that their individual responses and identities will not be disclosed beyond the research team unless they have expressly agreed otherwise.

Researchers cannot guarantee absolute confidentiality, however, and must inform participants of this. For example, a researcher cannot control whether members of a focus group share others' information. Or, in the case of a participant complaint, the IRB may need to review data and possibly consult with appropriate University officials. Researchers also must comply with applicable mandatory reporting laws, such as if a participant expresses the intent to harm self or others. UMW faculty and staff must also follow [FAQ on Updated Title IX Guidance](https://diversity.umw.edu/title-ix/).

Finally, if researchers transmit data via the internet (e.g., online or email surveys, Skype interviews, etc.), a low risk of a breach of confidentiality exists.  Researchers can minimize this risk by encrypting data transmission.

***Privacy***

"Privacy" refers to a participant’s control over the extent, timing, and circumstances of sharing personal information (physical, behavioral, or intellectual). Researchers must protect participants’ privacy during study *recruitment* and *data collection*. Researchers also must store data securely to prevent, where possible, identification of participants

Privacy pertains to *people* whereas confidentiality pertains to *data*; privacy is a right that can be violated whereas confidentiality is an agreement that can be broken.

Researchers may not collect data (words, behavioral observations) without permission if a participant has an "expectation of privacy" (the reasonable expectation that no observation or recording is taking place). An individual would not have an expectation of privacy if engaging in loud conversations or actions in a public space. However, in a classroom an individual would not expect someone to record notes for research purposes.

***Best Practices for Researchers***

**Study data:** Never gather more data than necessary to answer research question(s).

**Recruitment:** With "snowball sampling," provide potential participants with study information that *they can forward* to others who may be interested in the study. Potential or actual participants should never provide names/contact information of other potential participants without their permission.

**Informed consent process:** Clarify to participants how their data will be kept confidential, including:

* *Who* will have access to the data;
* *Where and how data* will be stored;
* How the researcher will *report* data/results (e.g., in aggregate, using pseudonyms); and,
* How the researcher will use *results* (e.g., in reports, publications, presentations).
* How the researcher will *destroy* copies of video or audio recordings upon study completion, or whether the researcher will use such recordings for presentations, websites. Researchers must obtain explicit consent for such use, and explain whether participants will be identifiable and/or identified.

**Web-based surveys:** (e.g., Qualtrics) Such online surveys can allow for anonymous data collection, but researchers must disable the feature collecting IP (internet protocol) addresses, in addition to *not* collecting enough indirect identifiers (gender, age, race, work‐site, etc.) to identify specific individuals, particularly with small, unique populations.

**Reporting results:** (e.g., in a research article/paper, report, presentation, news release) No time limit exists on the confidentiality of subject information. Researchers cannot identify participants without explicit permission, and direct quotes/descriptive information could reveal an individual's identity.