

II3E GD1 Protecting Participants' Research Data

II3E1 Methods for Protecting Participants' Research Data

The list below describes various methods University of Nevada, Reno (the University) and affiliate investigators may use to protect the privacy and confidentiality of the data obtained from research participants during a study. An investigator may choose to employ, and the Institutional Review Board (IRB) may require for approval, some or several of the described methods to ensure data protection, depending on whether the data contain personally identifying information, the sensitivity of the data and the potential harm to the participant should the data mistakenly be released or lost.

1. Identifiable research data, including recruitment and screening information and code keys are stored on a database located on a secure University network, which is backed-up nightly.
2. Subject identifiers and the means to link the subject names and codes with the research data are stored in separate locations within the database and with distinct access controls.
3. Access to the database is password protected and each research team member is required to have a unique ID and password to gain access to the database.
4. Identifiable data which are collected electronically (e.g., laptop, jump-drive, CD) are stored temporarily on the device until the identifiable data can be uploaded to the secure database.
5. Research computers are set to lock the screensaver after 15 minutes of inactivity requiring a password to unlock the screen.
6. Hard copy data are stored under lock and key and separately from signed consent and HIPAA documents.
7. Data sets containing subject identifiers will not be sent through e-mail, neither in the body nor as attachments.
8. Moveable electronic media used to collect or store data is equipped with encryption software.
9. The PI and other members of the research team work with coded or de-identified data when using moveable devices to perform data analysis. In the former case, the master code sheet must not be available on the device.
10. When moveable media devices are used to collect research data, the data are either limited to de-identified data or collected using the subject's unique self-generated or assigned code.

11. A Certificate of Confidentiality is obtained from the National Institutes of Health (NIH), the US Food and Drug Administration (FDA) or the Department of Health and Human Services (DHHS) to protect subjects' privacy and ensure the confidentiality of their study data and participation in a study (see II3E PR2 Certificate of Confidentiality).

II3E2 Confidentiality Considerations: Waivers or Alterations of Informed Consent

Federal regulations under 45 CFR 46.116(d) allow the IRB to approve a consent procedure that waives or alters the requirement to obtain informed consent from subjects provided that the following criteria are met:

1. the research involves no more than minimal risk to subjects,
2. the waiver will not adversely affect the rights and welfare of the subjects,
3. the research could not practicably be carried out without the waiver, and
4. whenever appropriate, the subjects will be provided with additional pertinent information after participation.

If under an IRB-approved waiver or alteration of informed consent, investigators accessing personal information of subjects in all aspects of the study including before consent, during recruitment and screening, under an exempt protocol) should be especially cognizant of the importance of keeping subjects' information confidential since their information is being accessed without the subject's knowledge or explicit permission.

II3E3 Confidentiality Considerations: Waivers of Documentation of Informed Consent

Federal regulations under 45 CFR 46.117(c) allow waivers of documentation of consent in two situations,

1. the consent form is the only record linking the subject to the research and the primary risk to participants would be a breach of confidentiality, or
2. the study presents no more than minimal risk of harm to subjects and involves no procedures for which written consent is normally required in the context of research.

The waiver of documentation of consent does not preclude the need for a consent process. Consequently, when the IRB approves a waiver of signed consent, the investigators must still include a process by which participants will be fully informed about the research and given the opportunity to agree or decline to participate. When the requirement to obtain signed consent from subjects is waived, the IRB may require that subjects be informed about the research via an information sheet or an informative cover letter or recruitment letter or email, depending on study design. When signed consent

is waived due to the need to protect participant' privacy, including their participation in the research study, the investigators and the IRB should carefully consider whether or not providing potential participants with written information about the research study is necessary and advisable.