
Yale University Institutional Review Board

Procedure 400 PR.1 Protecting Participants' Research Data

Methods for Protecting Participants' Research Data

The list below described various methods for protecting the privacy and confidentiality of the data obtained from research participants during a study. An investigator may choose to employ, and the IRB may require for approval, some or several of the described methods to ensure data protection, depending on whether the data is identifiable, the sensitivity of the data, and the potential harm to the participant should the data mistakenly be released or lost. Additional information for protecting electronic data can be found at www.yale.edu/its/secure-computing/index.html.

1. Identifiable research data, including recruitment and screening information and code keys are stored on a database located on a secure Yale-ITS 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 is collected electronically (e.g., laptop, jump-drive, CD etc) is stored temporarily on the device until the identifiable data can be uploaded to the secure database.
5. Moveable electronic media used to collect or store the data is equipped with encryption software recommended by the University (PGP).
6. Research computers are set to lock the screensaver after 15 minutes of inactivity requiring a password to unlock the screen.
7. Identified data sets will not be sent through e-mail or as an attachment.
8. Hard copy data is stored under lock and key. Signed consent documents must be confidentially retained for at least three years; HIPAA research authorization forms must be retained for at least six years.
9. The PI and other members of the research team work with coded or de-identified data when using moveable device(s) to perform data analysis.
10. Moveable media devices are used to collect research data which is limited to either de-identified or collected using the subject's unique code."
11. A Certificate of Confidentiality (CoC): A CoC is issued by 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.

Confidentiality in the Waiver of Documented Informed Consent

Federal regulations under 45 CFR 46.117(c) allow that, in studies that present no more than minimal risk of harm to subjects and involve no procedures for which written consent is normally required in the context of medical practice, oral consent may be approved by the IRB. Written consent may also be waived by the IRB if the consent form is the only record linking the subject to research involving sensitive

information and the primary risk of the research would be breach of confidentiality. The IRB will require that the information be presented to the subject as an information sheet.

Confidentiality in the Waiver of Informed Consent

Federal regulations under 45 CFR 46.116(d) allow for waiver of the requirement to obtain informed consent from subjects provided that the research involves no more than minimal risk to subjects, the waiver will not adversely affect the rights and welfare of the subjects, the research could not practicably be carried out without the waiver, and whenever appropriate, the subjects will be provided with additional pertinent information after participation. Investigators accessing personal information of subjects under an IRB-approved waiver of informed consent (e.g., 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.
