Office of Research Administration

University of Missouri – St. Louis
341 Woods Hall
One University Boulevard
St. Louis, Missouri 63121-4400
Telephone: 314-516-5899
Fax: 314-516-6759
E-mail: ora@umsl.edu

April 2003

ORA POLICY AND PROCEDURE:
Confidentiality in Research on Human Subjects

Confidentiality, Privacy and Anonymity

The term "confidentiality" is often confused with "privacy." Privacy refers to an individual person and to their interest in controlling others' access to themselves. Confidentiality refers to data and to limiting the access to private data about a person. Anonymity means that names and unique identifiers of subjects are never attached to the data, or known to the researcher.
All research involving human subjects must limit access to private information about the subject unless the investigator has the permission of the subject to do otherwise. Even projects considered exempt from full protocol review must include assurance of confidentiality. Maintaining confidentiality of private information entrusted to them by their subjects is a way that researchers protect their subjects from harm. Without assurance of confidentiality, potential participants may be unwilling to give honest answers about themselves. Researchers may be ordered by subpoena, or by other process of law, to disclose confidential information about a subject. Anonymity rather than confidentiality may be important in studies of sensitive behavior such as illegal conduct, drug use, sexual behavior or any other activity where disclosure of information may be damaging to the subject's financial standing, employability or reputation.

Legal Requirements Regarding Confidentiality

HIPAA, the Health Insurance Portability and Accountability Act, contains provisions that affect the handling and storing of any PHI (Personal Health Information) that could, potentially, be used to identify a research participant. You should refer to the HIPAA Summary and the list of HIPAA Identifiers to determine whether these guidelines apply to your research. The Office of Research Administration (ORA) and the Institutional Review Board (IRB) can help you ensure that your Consent and Assent forms, along with your data collection and storage procedures, comply with federal law.

Responsibilities of the Investigator

In developing the project design, the researcher should consider all risks to confidentiality that could occur and the appropriate means of assuring confidentiality. This includes risks at all stages of the study, including dissemination in the professional and popular media. Cultural differences may require different assurance issues. Prior to using human subjects, an agreement between the investigator and the subject should describe how confidentiality of records identifying the subject will be maintained.

How to Best Protect the Confidentiality of Human Subjects
Limit the amount of personal information to the absolute minimum.

If possible, gather information without names or unique identifiers attached to the data or known to the researcher. Some studies require consent forms identifying the subject, but these names do not necessarily need to be linked to the data.

Other identifiers such as age, income, and occupation, if they can be used to identify the subject by deduction, should be changed or aggregated. For example, age and income may be grouped into classes.

Legitimate Reasons to Identify Subjects
In many studies the researcher may need to re-contact the subject for follow-up information or to deliver the results of the study. Data sets from the same individual may need to be linked.

Data Gathering Procedures to Safeguard Confidentiality when Unique Identifiers are Unavoidable

- The researcher may temporarily identify responses and remove the subject names as soon as the data are analyzed.
- Names may be coded and the identifying list be kept in a safe or separate area from the study data. Some studies use aliases to protect the identity of subjects.
- If direct contact with the subject is not appropriate, a second or third party may be recruited for data collection.

Maintain Confidentiality in Data Storage
Data should be stored in files accessible only to the investigator and his or her assistants. If computers are used to store data, the investigator must be certain that access to sensitive files is limited. Audiotapes and videotapes may be particularly revealing and require special precautions to maintain confidentiality when airing or viewing and for storage.

If research is published, the investigator is accountable for the results and may be required to keep the data available for five to ten years. Also, when federal funds are used for research, the agency may require that the data be shared with other researchers.

What action can the researcher take to avoid subpoena of incriminating data when you need to identify subjects?
To keep identifiable data out of reach of subpoena a researcher may send the data to a colleague in a foreign country where it may be safely analyzed and stored. In studies using coded data, the master list of subject names linked to codes may also be handled in this way. Some federal agencies issue certificates of confidentiality for funded research.

Remember, whatever method is used to assure confidentiality, it must be explained clearly and simply to the subject.