IRBMED
MEDICAL SCHOOL OFFICE OF RESEARCH

U-MIC TRANSCRIPT
Privacy and Confidentiality

Federal regulations require researchers and IRBs to make sure that studies include "where appropriate, adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data."

We use the term *privacy* in reference to individuals and their right to control what other people know about them and their interactions with others.

Confidentiality refers in particular to the security of records and information about individuals.

Privacy applies to people. Confidentiality applies to information.

Protecting the privacy of your subjects and potential subjects involves choosing appropriate settings for all study procedures and discussions, including the informed consent process. Choose locations where people outside your study won't see or overhear your interactions. Avoid discussing study participation in public. It may be appropriate to let individuals contact you to talk about your study or to arrange a convenient and comfortable time to meet.

Since some people are more private than others, make sure, case by case, that your privacy measures meet the particular needs and expectations of your study population.

Confidentiality—an extension of privacy—relates to the data you gather about your subjects. Information you take from a subject's medical record is protected under the *Health Insurance Portability and Accountability Act,* or HIPAA. The Office of Human Research Protections requires that you maintain the confidentiality of any information you collect from non-public records, as well as information you collect from subjects directly in the course of your study. The National Institutes of Health (or NIH) address two key concepts relating to the confidentiality of research data. Those are *sensitive information* and *identifying characteristics*.

Sensitive information includes anything that a subject may not want everyone to know—for example, genetic profile, sexuality, illegal behavior, mental health, and any information that could lead to stigmatization or discrimination.

Identifying characteristics are details that might enable those outside your study team to recognize a subject. Examples of identifying characteristics include a subject's name, Social Security number, detailed physical description, and genetic profile.

No one outside your study team should have access to the identifying characteristics that link your subjects to their sensitive information. Password protection and encryption software are useful safeguards when storing confidential study data on computers. Never use shared or public computers to view or store information about your subjects. To prevent internet hacking, store confidential data on computers not connected to the internet. Avoid storing study data on portable devices that are easily misplaced or stolen.

In your study's informed consent document, you must explain to subjects how you plan to keep their information confidential. Indicate all parties who may have access to sensitive information, and describe the methods you will use to prevent others from gaining access to it.

U-MIC TRANSCRIPT
Privacy and Confidentiality

If your study does involve the collection of sensitive data, you may decide to apply to NIH for a *certificate of confidentiality*, even if your study is not NIH-funded. This would protect subjects' sensitive information from court orders demanding access to your study data. Any researcher who plans to gather sensitive information about study subjects may apply to NIH for a certificate of confidentiality.

Ethical research practice means protecting subjects' and potential subjects' personal privacy, as well as the confidentiality of the information you gather about them.

Contact IRBMED for more information about privacy and confidentiality.

Posted: 5/14/2012