Introduction
The Common Rule (45 CFR 46, Subpart A) states that when reviewing research proposals, Institutional Review Boards (IRBs) must determine that there are adequate provisions for protecting the privacy of subjects and maintaining the confidentiality of data.

The Common Rule is just one document that directs researchers to consider privacy and confidentiality when conducting research. The guidelines of the American Anthropological Association, the Oral History Association, the American Psychological Association, and the American Sociological Association identify protecting privacy and ensuring confidentiality as key components of respecting the safety and dignity of research subjects.

This module will define "privacy" and "confidentiality." It also will discuss some research methods and topics that raise concerns about privacy, identify some standard methods for providing confidentiality, and discuss relevant laws, other than the Common Rule.

Definitions
According to the IRB Guidebook, published by the Office for Human Research Protections (OHRP 1993):

"Privacy can be defined in terms of having control over the extent, timing, and circumstances of sharing oneself (physically, behaviorally, or intellectually) with others. Confidentiality pertains to the treatment of information that an individual has disclosed in a relationship of trust and with the expectation that it will not be divulged to others, in ways that are inconsistent with the understanding of the original disclosure without permission."

Although privacy and confidentiality are closely related, they are not identical. Privacy is related to methods of gathering information from research subjects; confidentiality refers to the obligations of researchers and institutions to appropriately protect the information disclosed to them.

Confidentiality procedures, as described during the informed consent process, allow subjects to decide what measure of control over their personal information they are
willing to relinquish to researchers.

It is not always the case that identifiable information provided by research participants must be protected from disclosure. Some participants want to be identified and quoted. Some agree to have their photographs, audio, or video recordings published or otherwise made available to the public.

**Identifying Private Information**

Federal regulations (Protection of Human Subjects 2009) define "private information" to mean "information about behavior that occurs in a context in which an individual can reasonably assume that no observation or recording is taking place, and information which has been provided for specific purposes by an individual and which he or she can reasonably expect will not be made public (for example, a medical record)."

Applying the reasonable assumption standard is not a simple task. It would be unreasonable to assume that behavior on a street corner or a public park is private, but reasonable to assume that behavior in our homes is private. However, given that technology makes it possible to film and record conversations from considerable distances, a third kind of space may be emerging: private spaces in the midst of very public ones. Parents taking their children to a city park might justifiably consider it a violation of privacy if the interactions of their children were audiotaped using long-range recording devices.

"Reasonable assumptions" regarding privacy will vary from culture to culture and setting to setting. For example, in some cultures health information is considered very private, but in others, information about people's health is part of the community dialog and widely shared.

Reasonable assumptions about privacy may vary among generations. The legal maxim that privacy is the "right to be let alone" (Warren and Brandeis 1890) comes from a world where privacy was seen as threatened by, among other things, the technologies that allowed still photographs to appear in mass-circulated newspapers. Now, through social media, younger generations use images to document their behavior and that of their friends and family, sometimes without restricting public access to the images.

**Controlling Access to Private Information**

Individuals' ability to control access to their persons and to their personal information is determined by a variety of factors, including socioeconomic status, age, and circumstance. For example, information about welfare rolls is public information while information about personal stock portfolios is not. Children have different rights to privacy than adults. Institutionalized persons may have significant limitations on their ability to control personal information.

**Privacy and Study Questions**

Invasions of privacy can occur if subjects are asked questions that they find intrusive. If a survey instrument or an interview script contains questions that individuals are likely to
find intrusive, they must be informed about the nature of the questions in advance. Studies about sexual behavior, childhood abuse, use of psychotropic medications, and other personal topics should include a disclosure in the consent form about the sensitive nature of the questions. The survey instrument or interview process must be designed so that subjects may choose not to answer any question that makes them uncomfortable, or that they want to skip for any reason.

Cultural standards should be taken into account when designing research. Topics that are considered appropriate in one setting may be offensive and off-limits in another.

**Protecting Communications with Subjects**
If a study is obviously about stigmatizing conditions, illegal activities, or life experiences that subjects may not want others to know about, communications with the subjects should not reveal their participation in the study to others because to do so would violate the subjects' right to privacy. Study titles should be carefully considered; it is often best if the title does not reveal sensitive information about participants. A method of communication that is of particular concern is email. Employee email is not secure and some personal accounts may be accessed by anyone in the family. Telephone calls to subjects at home may be of concern. It may be appropriate to script calls carefully so that no information is revealed about the caller or the subject to anyone other than the subject. In some cases, it may be appropriate to remind subjects to prevent possible violations of their privacy in their homes by, for example, closing browsers after completing an online survey on a sensitive topic.

**Confidentiality**
Researchers provide confidentiality to their subjects by appropriately protecting information the subjects disclose. The potential risk of harm to subjects if identifiable data were inadvertently disclosed is the key factor for determining what kinds of protection are needed.

The ideal way to protect research data is not to collect information that could identify subjects, that is, neither direct identifiers such as names or email addresses, nor indirect identifiers such as information that could be used to deduce subjects' identities.

If researchers plan to retain individually identifiable data that if inadvertently disclosed could place participants at risk of harm, researchers need to design procedures to protect the data during collection, storage, analysis, and reporting. These procedures could include creating keys linking subjects' names to unique numbers associated with the data, storing encrypted data on secure servers, removing identifiers when data collection is completed, reporting data in aggregate, and creating misleading identifiers in articles or presentations.

Consent forms should clearly explain who will have access to identifiable data, both in the present and in the future, and describe any future uses of the data. For example, if researchers want to show video clips of research subjects during conference presentations or use them in a classroom, the subjects must be asked for permission to use their images
in those ways.

References

Original Release: January 2004
Last Updated: November 2014