

---

## CITI's Privacy & Confidentiality Information

### Content Author

- ▶ **Lorna Hicks**  
Duke University

This module consists of 7 sections and will require about 15-20 minutes to complete. ~~Take the short quiz at the end of this module before going to the next module.~~

---

### Introduction

The importance of protecting the privacy of research subjects and ensuring confidentiality of research data is widely acknowledged. The right to privacy is highly valued in the United States and secured by laws *other* than those for protecting research subjects. For example, the Family Educational Rights and Privacy Act (FERPA) is designed to protect the privacy of students' educational records. And the Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA) describes conditions under which researchers can access and use private health information.

Scientific societies have also adopted guidelines that stress the need to respect the privacy of subjects. For example:

- ▶ "Anthropological researchers must do everything in their power to ensure that their research does not harm the safety, dignity or privacy of the people with whom they work, conduct research or perform other professional activities." ([Code of Ethics of the American Anthropological Association](#)) (Links will open new windows in your browser. To return to the module, close the new windows.)
- ▶ "Psychologists respect the dignity and worth of all people, and the rights of individuals to privacy, confidentiality, and self-determination." ([Ethical Principles of Psychologists and Code of Conduct, 2002](#))
- ▶ See also, the [Oral History Association](#) and the [American Sociological Association](#).

This module will define privacy and confidentiality. It will discuss protecting privacy in the research context and will provide some guidelines for designing confidentiality procedures.

---

### Module Contents

1. Definitions.
2. Private vs. Public Behavior.
3. Controlling Access to Private Information.
4. Privacy and Exempt Research.
5. Privacy and Research Methods.
6. Confidentiality.
7. Privacy and Reporting Laws.
8. Certificates of Confidentiality.

---

## **1.0 Definitions**

The Common Rule states that in order to approve research the IRB shall determine that, when appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data.



According to the IRB Guidebook, published by the Office of Human Research Protections, 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.

Thus it follows that privacy, a right, can be violated. Confidentiality, an agreement, can be breached.

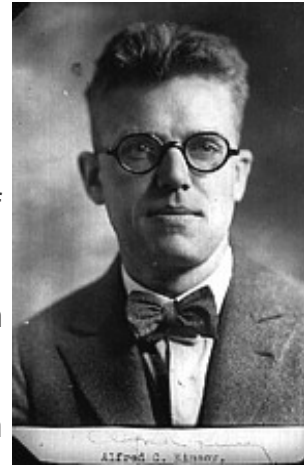
Confidentiality procedures, as described during the informed consent process, allow subjects to decide what measure of control over their personal information they are willing to relinquish to researchers.

It is not always the case that information provided by research participants must be protected from unauthorized or inadvertent disclosure. Some participants want to be identified and quoted. Some agree to have their photographs or audio- or video-tapes archived in collections available to the general public.

---

## 2.0 Private vs. Public Behavior

How can researchers determine which behaviors and information are private and which are public? The distinction is important because observation and/or recording of public behavior does not meet the definition of research with human subjects. The federal regulations 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 school record)."



Although this definition includes the phrase "reasonably assume" which requires interpretation, the definition does provide a yardstick for differentiating between public and private behavior.

It would be perhaps unreasonable to assume that behavior on a street corner is private, but reasonable to assume that behavior in our homes is private. However, individuals may identify private spaces in the midst of very public ones. For example, parents taking their children to a city park might consider it a violation of privacy if the interactions of their children were audio-taped using long-range recording devices.

"Reasonable assumptions" regarding privacy will vary from culture to culture and setting to setting.



Gathering Oral Histories from Local Native Americans

---

### 3.0 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; information about personal stock portfolios is not. Minors have different rights to privacy than adults. Institutionalized persons may have significant limitations on their ability to

control personal information.

---

### 4.0 Privacy and Exempt Research

Can research that uses individually identifiable information be exempt? Yes, a research project involving individually identifiable information about respondents can be exempt under two conditions:

1. The information is either not linked to the respondents' identities, that is, it is anonymous, or
2. The information is linked to the respondents' identities, but the nature of the information is such that disclosure will not be reasonably expected to cause harm. In other words, non-anonymous data recording can be exempt if any breach of confidentiality would not cause harm beyond that encountered in everyday life.

---

### 5.0 Privacy and Research Methods

While not an exhaustive list, the following material highlights some concerns about privacy in the context of research.

1. Observational Studies
2. Study Questions
3. Communicating with Subjects
4. Focus Groups
5. Snowball Sampling

---

#### 5.1 Observational Studies

Most research involves asking subjects to provide or release information voluntarily following an informed consent process.

Privacy issues arise in regard to information obtained for research purposes without the consent of the subjects.



Such studies may raise ethical concerns when they access identifiable information about subjects without the subjects knowledge. For example, a researcher may videotape subjects when the subjects presume they are on a break between study tasks. An ethical concern is whether an invasion of privacy - a violation of the principle of respect for persons - could be justified by the benefits of the study. Is the knowledge to be gained important enough to involve the subjects without their consent? What, if anything, will the subject be told later?

[Top](#)

---

## 5.2 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 contain 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 a subject can choose not to answer any question that makes him or her uncomfortable, or that he or she wants to skip for any reason.

Although there is considerable variation in how people define the right to privacy, there are nonetheless community and cultural standards that should be taken into account when designing research. Topics that are considered appropriate in one setting may be offensive and off-limits in another.

---

## 5.3 Communicating 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 alone is not sufficient to reveal sensitive information about participants. A method of communication that is of particular concern is e-mail. Employee e-mail is not secure and some home accounts may be accessed by anyone in the family. Telephone calls to subjects at home may also 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 educate subjects about

how to prevent possible violations of their privacy in their homes. For example, researchers may counsel subjects to make sure their home computers are secure or to close their browsers after completing an on-line survey on a sensitive topic.

---

#### **5.4 Focus Groups**

Protecting privacy within research using focus groups often requires researchers to modify the kinds of promises of confidentiality that they give in one-to-one interviews. Even though researchers can emphasize to all participants that the comments made during the focus group session should be kept confidential (when the topic warrants), researchers need to inform participants that it is impossible for the researcher to promise that participants will not repeat comments outside the group at some time in the future. Because maintaining confidentiality is not entirely under the control of the researcher, participants need to be encouraged to be as honest and open as they can, but remain mindful of the limits on the researcher's ability to protect confidentiality. In recruiting for focus groups, it is important to inform prospective participants how fellow participants are being selected. Privacy may or may not be an issue in the course of the group discussion, depending on whether individuals already know each other, and the topic. Participants need to know that information to help them decide about their comfort in being part of that group and dealing with the specific topics of the study.

---

#### **5.5 Snowball Sampling**

Snowball sampling is recruitment technique in which research participants are asked to assist researchers in identifying other potential subjects. If the topic of the research is not sensitive or personal, it may be appropriate for subjects to provide researchers with names of people who might be interested in participation. If the topic is sensitive or personal, such as the fact that someone was adopted, care should be taken so that potential subjects' privacy is not violated. In this case, subjects assisting with recruiting could provide information about the research to potential subjects, rather than giving the researcher names of potential subjects.

---

### **6.0 Confidentiality**

The ways in which data will be used and made available to others is part of the agreement researchers make with study participants and must be described during the informed consent process. The following questions are some of those that may be used to guide the design of study-specific confidentiality procedures.

1. Are identifiers really needed or could data be collected anonymously?
2. Can identifiers be destroyed, thus anonymizing data?
3. If identifiers are needed, can coded IDs be created to use

for data collection, merging, and analysis, with identifiers kept entirely separate and secure?

4. If subjects were chosen for the study due to a sensitive or stigmatizing condition or participation in illegal activities, are procedures in place from the very beginning to protect identities, such as a waiver of the requirement to document consent?
5. Once identifiers are used to create codes to identify various data, can actual identifiers and the list linking them with the code be destroyed, thus anonymizing the data?
6. How will the data be protected from inadvertent disclosure or unauthorized access during collection, storage, and analysis? Would password protection be sufficiently protective, or would data encryption be necessary in addition? Would the use of stand-alone computers, without network access help prevent access by unauthorized users?
7. Are de-identified data sufficiently protected from re-identification?
8. Should data be manipulated in specific ways to reduce specificity, by collapsing data into categories with small numbers of individuals, reducing age or geographic specificity, etc.
9. Does sensitive data need to be protected from subpoena by third parties? Should a Certificate of Confidentiality be obtained?
10. In studies where it is an issue, are there limits to the promises of confidentiality that the researcher can make to subjects due to state laws requiring researchers to report suspected child abuse or neglect?
11. How will data be reported? In aggregate? Using pseudonyms? Using real names? Answers to these questions should be shared with participants so they can decide if they are comfortable with the plan.
12. Does permission need to be obtained to attribute quotations to subjects in a way that reveals their identity?
13. Who else, besides the researchers, will have access to the data in the present AND in the future?
14. If audiotapes or videotapes are made, what will be done with them during and after the research? Will they be shown at scholarly conferences? If so, will all subjects be asked if they are willing for the tapes to be shown? Will audiotapes or videotapes be archived? Do releases need to be obtained for archiving material? Will the tapes be saved in case they have an as-yet-unknown, research

use?

---

## 7.0 Privacy and Reporting Laws

---

### 7.1 Federal Privacy Law

Federal laws protect the disclosure of educational records (FERPA) and of private health information (HIPAA).

Generally, the disclosure of these records to researchers involves securing written authorizations from the potential subjects, although in certain clearly defined circumstances the requirement to secure authorizations may be waived. The module Research in the Schools provides more information about the use of educational records. Researchers in the social and behavioral sciences and the humanities do not generate private health information covered by HIPAA, rather they ask for it to be disclosed to them, usually by asking subjects to sign authorizations permitting the disclosure. These authorizations must include particular elements. Most institutions covered by HIPAA have models of authorization forms that they expect researchers to use

---

### 7.2 State Reporting Requirements

State reporting laws may limit the promises of confidentiality that researchers can offer subjects. Most state laws identify individuals who must report suspected child abuse and neglect. This requirement should be described when child abuse and neglect might be revealed in a research study. Such studies could involve at-risk youth, school-based interventions, or parenting practices, among others.



On the other hand, there are many studies in which it is extremely unlikely that the topic would arise or that the researcher would be in a position to observe neglect or abuse. For example, a study of decision-making strategies using computer-based activities would not generate information about child abuse and there would be no need to discuss reporting requirements during the consent process.

State reporting laws may cover such matters as specific communicable diseases, the intent to harm oneself or others, and elder abuse. Consult with your IRB about the laws in your state.

---

### 7.3 International Privacy Laws

Researchers conducting research abroad should identify privacy laws at the research site that may be relevant for the conduct of research with human subjects.

---

## **8.0 Certificates of Confidentiality**

Certificates of Confidentiality are issued by the National Institutes of Health (NIH) to protect identifiable research information from forced disclosure. Certificates of Confidentiality may be granted for studies collecting information that, if disclosed, could have adverse consequences for subjects or damage their financial standing, employability, insurability, or reputation. A Certificate of Confidentiality will allow the investigator and others who have access to research records to refuse to disclose identifying information on individual research participants in civil, criminal, administrative, legislative, or other proceedings, whether at the federal, state, or local level.

Information that can be protected includes, but is not limited to:

- Substance abuse or other illegal behaviors.
- Sexual attitudes, orientation, or practices.
- Genetic information.
- Psychological well-being.

Certificates of Confidentiality may be secured for any sensitive research, regardless of funding source. In fact, the research does not have to be funded.

Revised and Posted June 22, 2008.