UCLA Research Administration
Human Research Protection Program

Quick Guide: Protecting Privacy and Maintaining Confidentiality

(updated October 21, 2020)

This reference tool is intended to aid researchers and IRB members to ensure that adequate provisions exist for the protection of research participant privacy, the maintenance of confidentiality of identifiable research data and data security.

Protecting Privacy - Issues to Consider

Privacy is about people. Privacy is the control over the extent, timing, and circumstances of sharing oneself (physically, behaviorally, or intellectually) with others.

Privacy is:

- a sense of being in control of access that others have to ourselves;
- a right to be protected;
- and is in the eye of the participant, not the researcher or the IRB.

Subject Population	• What are the cultural norms of the proposed subject population? Some cultures are more private than others. • What are the ages of the proposed subject population? There may be age differences in privacy preferences (e.g., teenagers less forthcoming than older adults)
Recruitment Methods **See also: Recruitment and Screening Methods and Materials**	How are potential participants identified and contacted? ***Acceptable methods:*** • advertisements, notices, and/or media • Send introduction letter to colleagues to distribute to eligible individuals – interested individuals contact researcher • Primary care staff contact those patients that qualify to determine interest ***Unacceptable methods:*** • search through medical records for qualified participants or existing database (e.g., registry); then have a researcher with no previous contact with potential participant recruit; this method violates the individuals' privacy • recruit participants immediately prior to sensitive or invasive procedure (e.g., in pre-op room) • retain sensitive information obtained at screening without the consent of those who either failed to qualify or refused to participate for possible future studies participation
Sensitivity of the Information Being Collected	The greater the sensitivity, the greater the need for privacy
Method of Data Collection (Focus Group, Individual Interview, Covert Observation)	• Will participants feel comfortable providing the information in this manner? • If passively observing the participant; could the individual have an expectation of privacy (e.g., chat room for breast cancer patients)? • Will the researcher collect information about a third party individual that is consider private (e.g., mental illness, substance abuse in family)? If yes, informed consent should be obtained from third party?

The California Consumer Privacy Act (CCPA) went into effect on January 1, 2020, which grants California residents ("consumers") rights with respect to the collection and use of their personal information by businesses. Since University of California (UC) is not a business, the CCPA does not directly apply to UC. However, research sponsors may require compliance with certain provisions of the Act and additional information disclosed in the consent form. If you have questions about CCPA please contact OHRPP.

Maintaining Confidentiality

Confidentiality is about data. 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 without permission in ways that are inconsistent with the understanding of the original disclosure. Confidentiality is:

- About identifiable data;
- An extension of privacy; and
- An agreement about maintenance and who has access to identifiable data.

With respect to HIPAA, confidentiality protects patients from inappropriate disclosures of "Protected Health Information" (PHI).

Research Design	Protocols should be designed to minimize the need to collect and maintain identifiable information about research participants. If possible, data should be collected anonymously or the identifiers should be removed and destroyed as soon as possible and access to research data should be based on a "need to know" and "minimum necessary" standard.
Collecting and Maintaining Identifiable Data?	When it is necessary to collect and maintain identifiable data, the researcher needs to ensure that the protocol includes the necessary safeguards to maintain confidentiality of identifiable data and data security appropriate to the degree of risk from disclosure.
Provisions to Maintain Confidentiality of Data	If yes to any of the following, measures to maintain confidentiality should be incorporated into the protocol: • Will confidentiality of identifiable data be offered? • Are there legal/ethical requirements (e.g., HIPAA)? • Will release of data cause risk of harm?
Limit Access to Data	• When FDA-regulated products are being studied; participants must be informed that the FDA may have access to their study records to protect their safety and welfare. Any information derived from the research project that personally identifies the participant will not be voluntarily released or disclosed by these entities without the participant's separate consent, except as specifically required by law. • Research records provided to authorized, non-UCLA entities should not contain identifiable information about the participant. • Research consent form should state who will have access to identifiable data.

Zoom Privacy

All researchers who wish to use Zoom to conduct interviews should only use the following UCLA Zoom platforms:

- Use HIPAA Zoom for meetings that pertain to medical treatment or counseling sessions
- Use UCLA Health Zoom for members of the UCLA Health and Health Sciences schools
- UCLA Zoom for all other research

When scheduling your meeting:

- Generate a unique meeting ID
- Require a meeting password and distribute the password to only those who need access
- Enable the waiting room feature
- When scheduling the Zoom meeting, turn off “video” for participants (to allow participants choice of if/when to turn on their video)
- Researchers should configure the videoconferencing software to prohibit recording by participants
- When possible, disable the Zoom function that automatically collects electronic identifiers, such as IP addresses or cookies

During your meeting:

- Remove and/or manage participants
- Lock your meeting once all your participants have joined to avoid uninvited guests
- Participants should be instructed to not record/take screenshots
- All participants should be reminded of the unique limitations to privacy on digital platforms and to use discretion when sharing
- If recording videos, avoid using the Zoom cloud recording storage. Instead use the local storage option, which stores the recording on your own device.

Researcher hosts:

- Can enable mask phone number in the participant list under the telephone subtab

For participants:

- When the participant joins a Zoom meeting, they can change their name before joining a meeting to maintain confidentiality

For additional resources, please visit UCLA guidelines for Zoom security best practices. Videoconferencing functions and security are evolving, so check with IT support for the system you are using to determine if additional security options or vulnerabilities have become available in order to address and minimize risks to participants.

NOTE: Research use of Zoom must be described in the webIRB application.

Additional References

UCLA OHRPP Guidance

- Certificates of Confidentiality
- Data Security in Research
- Health Insurance Portability and Accountability Act (HIPAA)
- DOE checklist
- DOJ checklist

UCLA Guidance

- Protecting Privacy & Data During Remote Working & Using Zoom
- Zoom Security Best Practices

Change history:
8/25/2020: Added information on California Consumer Privacy Act and updated links.
10/21/2020: Added Zoom privacy section.