Tipsheet -- Privacy During Recruitment, Informed Consent, and Data Collection

Privacy protections must be carefully designed to maximize people’s ability to control access to themselves in the specific context of your study. There are no one-size-fits-all methods -- needs vary depending on the nature and context of each study. These tips offer a starting point of protections to consider as you develop plans for your project.

Tips for Privacy During Recruitment

- Send recruitment messages individually, not to groups; use blind carbon copy (bcc) if group emails are necessary.
- When appropriate, ask a collaborating entity to forward your recruitment messages to potential participants.
- Obtain participant permission before leaving voicemails/messages. If messages must be left, do not share the purpose of the study, why the person is eligible, etc. Just indicate you are calling about an Iowa State study.
- Implement private methods for participants to “sign up” or schedule visits; do not pass a sign-up sheet throughout a group or use online calendaring apps that show lists of names.
- If social media is used:
  - Disable commenting/tagging/sharing; instruct participants to share posts privately and not to “tag” or mention others.
  - Instruct participants to directly contact researchers with questions rather than commenting.
  - Monitor recruitment posts to delete any responses that tag people or otherwise disclose private information.
  - Delete recruitment posts when enrollment has closed.
  - Note: Using social media for recruitment is generally not advised for research on highly sensitive or risky topics (e.g., illegal behaviors, sexual practices, substance use/abuse, specific medical conditions, etc.) where there is risk of potentially “outing” people to others.
- If screening involves asking for information, advise participants of the nature of the information and ask whether the participant is comfortable sharing before proceeding.
- Avoid/minimize recruitment methods that require intrusion into settings where people have a reasonable expectation of privacy (e.g., their doctor’s office, home, workplace, etc.). If such methods are needed, obtain advance permission.
Tips for Privacy During Data Collection

- Use secure, ISU-supported platforms (Qualtrics, WebEx/Teams/Zoom, ISU email, etc.).
- Minimize information collection to that which is scientifically necessary, particularly if sensitive or potentially identifying.
- Allow private completion and anonymous submission of surveys and questionnaires, if feasible.
- Conduct sensitive interviews/discussions/procedures in private spaces.
- Conduct anthropometric measurements (weight/height/etc.) and apply biometric sensors behind screens or in private rooms.
- Instruct focus group participants to keep confidential what they hear as well as who else is participating.
- Avoid group discussions/activities for highly sensitive research.
- Inform participants to refrain from sharing identifiable information about themselves or others in their open-ended responses when it is not necessary for the research.
- Obtain participant permission before leaving voicemails/messages.
- Encourage participants to use personal accounts for study-related communication, instead of emailing or texting using a work-related email account or phone number.
- Devise plans to keep participant information secure while in the field and/or during transmission (e.g., in a lock-box, use of codes rather than names on materials, etc.).
- Remove participant information or recordings from devices as soon as possible after uploading data to a secure platform such as CyBox.
- When appropriate, advise participants of precautions they can take (e.g., closing browsers, avoid using shared devices, deleting history/cookies, etc.).