Guidance:
Approval Criteria #7 - Privacy of subjects' participation and confidentiality of data

Overview

Criteria #7 is as follows: **When appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data. (**45 CFR 46 | HHS.gov)

Confidentiality and privacy are important aspects of ethical research because a participant ought to have control over whether it becomes public knowledge that they participated in a research study, as well as the information they provided while participating in the research.

The IRB must decide on a protocol-by-protocol basis whether there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of the identifiable data at each segment of the research from recruitment to maintenance of the data. This guidance document details items to consider when determining whether criteria #7 has been met.

Privacy is about people. Confidentiality is about data.

Privacy

Privacy is an individual's desire to control access of what is shared about themselves with others. This control can extend to timing, extent, and circumstances. Information can include one's physical attributes, behaviors, or intellect. For example, persons may not want to be seen entering a place that might stigmatize them, such as a pregnancy counseling center clearly identified by signs on the front of the building.

The evaluation of privacy also involves consideration of how the researcher accesses information from or about potential participants (e.g., recruitment process). IRB members consider strategies to protect privacy interests relating to contact with potential participants, and access to private information.

Privacy considerations

The IRB protocol application form should detail how the privacy of participation will be protected. There are many components that should be considered.

- 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:

  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 subjects or existing database (e.g., registry); then have a researcher with no previous contact with potential subject recruit; this method violates the individuals' privacy
  - recruit subjects 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:
  - How to access the minimum amount of information necessary to complete the study.
  - Nature of the requested information
  - The settings in which an individual will be interacting with an investigator.
  - The appropriateness of all personnel present for research activities.

- Data collection strategies:
  - Will subjects feel comfortable providing the information in this manner?
    - Phone calls on a land line – subjects may not want others to know they are in the study; how does the researcher introduce themselves. How are messages left on machines or with an individual?
    - Sending letters to home addresses that contain private information, even something as simple as a study title can share private information…living with HPV, understanding attitudes of bi-sexual college students and risk taking behavior
    - emails and text messages that might be seen by others (e.g. children may not have complete control of their phones and email);
    - Facebook or other social media
    - If passively observing the subject; 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?

- Maintaining privacy
    - Not leaving questionnaires, interview transcripts, or field notes with participant identifications sitting out where others might see them but rather locking them up
    - Using electronic data security measures to lower the odds that, even if one's laptop is stolen, information on it will be easily readable; this might include password protection, encryption, or other measures
    - Privacy guidelines developed by relevant professional associations and scholarly disciplines (e.g., oral history, anthropology, psychology).

Confidentiality

Confidentiality refers to the researcher's agreement with the participant about how the participant's identifiable private information will be handled, managed, and disseminated.

The research proposal should outline strategies to maintain confidentiality of identifiable data, including controls on storage, handling, and sharing of data.

Benefits of maintaining confidentiality

- It helps establish trust between the research participant and the researcher.
- It reduces worry on the part of the individual.
- It maintains the participant's dignity.
- The participant feels respected.
- It gives the participant control and promotes autonomy

Confidentiality considerations

Not every study requires absolute confidentiality. The level of protections need to ensure the confidentiality of subjects' private information will vary from study to study, but the questions to be addressed remain the same. The IRB protocol application form should detail how the confidentiality of data will be protected. There are many components that should be considered.

- Limitations to access: What sort of limitations should be placed on access to the study data?
- Retention of identifiable data: How long will identifiable data be retained? What about documents linking participant with a study code?

- Access to study documents: Who should be permitted access to the study documents? There should be limited access to the information to those who need to know
- Access to participants names: Who should be allowed to know the identities of those participating as subjects?
- Adequate security plan: Is the security plan sufficient? (password protections, locked cabinets, encryption methods, separate storage of Master Lists from study data) is sufficient to adequately protect the subjects given the inherent sensitivity of the data?
- Will confidentiality of data be assured? Will confidentiality of identifiable data be offered? Care should also be taken not to promise more than one can truly attain. That is to say, the consent form should not promise to keep the subject's data strictly confidential unless one is able to guarantee that this will be the case.
- Will release of data cause risk or harm? there will be cases, such as a high security data repository, that will maintain a significant level of confidentiality studies dealing with sensitive information.

Maintaining confidentiality

Protocols should be designed to minimize the need to collect and maintain identifiable information about research subjects. When it is necessary to collect and maintain identifiable data, the IRB will 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.

Confidentiality is not the same as anonymity.

Deidentifying data

If possible, data should be collected anonymously, or the identifiers should be removed and destroyed as soon as possible. Access to research data should be based on a "need to know" and "minimum necessary" standard. Some ways identifiable can be protected include:

- Giving participants pseudonyms: Changing details of the write-up other than just names in order to prevent readers from identifying participants; in some kinds of research it is common to generate a "typical" participant who is not based on any one actual participant but who captures important elements of multiple participants
- Using initials rather than full names
- Retaining links between names and study codes saved separate from other documenyts
- Limit access to those who have access to study links
- Not writing down any identifying information in the first place, even if the researcher knows participant names
- Arranging to interact with participants in such a way that the researcher never knows the participants' names in the first place; this is sometimes known as anonymity

- Removing certain demographic information from quantitative research, either temporarily or permanently
- Using a consent process where a participant consents without their name being captured either on paper or on a recording
- Destroying identifying information as soon as possible
- Storing field notes, transcripts or questionnaires that have been purged of identifying information separately from any identifying information (e.g., a day timer with appointment names and addresses)
- Avoiding the collection or tracking of IP addresses during online research

Provisions to maintain confidentiality of data

- Will confidentiality of identifiable data be offered?
- Are there other regulations to adhere to; e.g., HIPAA, FERPA, GDPR.
- Are there any state specific requirements?
- Will release of data cause risk of harm; e.g.; participation in illegal activities, gender identification, etc.?
- Will participants request to have identifiable data destroyed if they chose to withdraw participation?
- If the research involves observation or intrusion in situations where the participants have a reasonable expectation of privacy, investigators should examine the design of the research to determine whether the intrusion can be avoided or reduced.
- If the investigators want to review existing records to select subjects for further study, the investigator must already have the appropriate access to this data and consent to contact subjects for future research.
- Does the informed consent document identify who may have access to identifiable data? For example, Federal regulators, study sponsor, IRB, university auditors.

A breach of confidentiality is an unanticipated problem that must be reported to the IRB.

There are times when a breach of confidentiality may be required by university, state or federal law. The participants should be made aware of this possibility.

- HIV Antibody Testing: If the study involves HIV testing, investigators are cautioned that a discovery or diagnosis of HIV or AIDS in a patient must be reported to the State Health Department. A positive diagnosis may have serious legal and financial consequences for research subjects
- Reportable Diseases: Other reportable diseases include Hepatitis A, Syphilis, Tuberculosis, etc. If during the course of research procedures any reportable disease is discovered, participant confidentiality may be limited by state reporting laws.
- Intent to harm self or others
- Child abuse/neglect link to policy

Other considerations

- Genetic Testing: Investigators must establish a method to secure information related to genetic testing in a highly secure and confidential manner, and communicate this method in a manner satisfactory to the IRB. Identifiable results cannot be disclosed to the subject or anyone else except in compliance with an approved protocol for contacting subjects and/or family members. If there is a potential risk to the patient's insurability or employability as a result of participation in the study, the consent document should disclose this.
- Tissue/Specimen Use and Repositories: The IRB expects a detailed description of the privacy and confidentiality protections for research proposals that include tissue/specimen use be provided.

Certificates of Confidentiality

A Certificate of Confidentiality (COC) protects research subjects' privacy and confidentiality by prohibiting disclosure of individuals identifiable and sensitive information to anyone not connected with the research. It provides ab extra layer of privacy protection that enables researchers to refuse disclosure in any civil, criminal, administrative, legislative, or other proceeding, whether at the federal, state, or local level. For example, if the information obtained about subjects might interest law enforcement or other government agencies to the extent that they might demand personally identifiable information, the investigator may want to obtain a Certificate of Confidentiality to protect the research data and the identity of the participants, as applicable.

References

45 CFR 46 | HHS.gov