Module 5: Privacy and Confidentiality

Introduction to Privacy and Confidentiality

Welcome to the fifth module in the Social and Behavioral Research Best Practices for Clinical Research course. Throughout this module, we'll cover privacy and confidentiality practices before, during, and after social and behavioral research studies.

Let's get started by hearing from Christa, who ran a clinic based study involving college-age students and sexually transmitted diseases. Along the way, she experienced some concerns about maintaining the privacy of participants and confidentiality of study data.

Approaching Potential Participants

During the final preparation stages for the study, we were almost to the point where we could submit our documents to the I.R.B., but I was still struggling to find ways to recruit participants. Anything related to sexual behavior or sexually transmitted diseases is incredibly private, and it can be really difficult to find willing participants. I had some ideas for ways to recruit participants but wanted to be sensitive to privacy concerns.

Storing the Data

Once the I.R.B. protocol was approved and the study was underway, we successfully recruited a large group of participants, and I filmed each of the one-on-one conversations. Needless to say, my video files became really big and I needed to free up some disk space before I had the chance to get the sessions transcribed.

Scheduling a Meeting

As the interviews were taking place, I had one participant who found it difficult to get to the research building for our interview. She said it would be easier to schedule if we could meet her at her house. I *wanted* to accommodate her, but we hadn't specified an off-site setting in the I.R.B. protocol.

Course Study Manual

Take a minute to explore the Resources section of this course in the top right corner of your screen. Here you'll find your Social and Behavioral Research Course Study Manual for this course, Privacy and Confidentiality. Be sure to print this before you continue.

Throughout this module you'll be able to pause the course and take notes specific to your institution. In the end, you'll have a roadmap to a successful social and behavioral research study.

What is Privacy?

First, let's talk about privacy. Privacy can be defined as an individual's right to control information about themselves. In the context of social and behavioral research, privacy might refer to physical, biological, behavioral, and other psychosocial information.

During the course of a study, you can ask yourself a few questions to help protect a participant's privacy:

Are interviews being conducted in a private room? If a private room cannot be found, make sure you are talking in a quiet voice.

Have you asked family members or other people with the participant to leave the room?

Are you protecting the disclosure of sensitive information, like illegal drug use, HIV status, or information about sexual behaviors?

Certain elements of privacy vary from culture to culture. To take these cultural considerations into account, you must fully understand the study group population when designing and implementing study procedures.

What is Confidentiality?

On the other hand, confidentiality is considered an *extension* of privacy. It refers to how information is kept; who can see it, who handles it, and how it is stored. Confidential information is that which is identifiable, or can be linked to protected information of a participant.

Take a moment to write down your own concerns regarding privacy and confidentiality in your course study manual. Click Next when you're ready to move ahead.

Identify a Breach

Now that we've covered the elements of privacy and confidentiality, let's take a moment to practice. See if you can identify which scenario is a breach of privacy or confidentiality, and which is not.

Privacy and Confidentiality Protection Strategies

Strategies for maintaining privacy and confidentiality are best laid out in the initial design stages of a study but should be remembered throughout the life of a study. Click on each item or event on-screen to learn more about these strategies. Click Next when you're ready to move on.

Recruitment

During the recruitment stage, it's appropriate to engage potential participants in a way that helps preserve their privacy. All contact must be respectful, and potential or current participants should feel comfortable enough to opt out of a study. You can ensure this by being aware of your surroundings and noting whether other people can hear your discussion. Plan ahead and find a private space or room to discuss the study. If you're making phone calls, consider who else is in the room with you and who might answer the phone. Throughout recruitment and the remainder of the study, a researcher or other study team member must always be completely open and honest of who they are, and what their involvement in the study is.

Site Selection

The selection of your study site is critical in terms of privacy. Sometimes just participating in the study can put a participant at risk, depending on where the study is being conducted. For example, a study that examines gang member-related activities could put a participant in extreme danger if it was obvious he or she was participating in the study. Researchers must choose sites that will provide participants a safe environment.

Focus Groups

Focus groups are not a private setting and all participants should be reminded of this. Every person in the room can hear the information discussed, and the researcher will not be able to guarantee confidentiality.

Also, if a transcript of the group's dialogue is created, all data that could identify a participant should be removed. Remember to frequently remind the group that, what happens in the focus group, stays in the focus group.

Group Interventions

Group interventions are a common method in social and behavioral research. Many of the concerns of a focus group are also legitimate in a group intervention, as confidentiality cannot be fully guaranteed. Be sure to remove all references to identifiable data and reiterate the importance of keeping what is said in the group within the group setting.

Sites Outside the Clinic

As a researcher, it may be necessary to travel off-site for a study. Extra care should be taken to plan for privacy protection at off-site locations, well in advance of study initiation. In addition to environmental privacy concerns, consider how you will maintain confidentiality while transferring data or information from the offsite location back to your office. Take a moment to research your own institution's policies on this and make a note in your course study manual.

Home Visitation

If a visit to a participant's home is required, it may be necessary to ask any non-participants - such as a spouse, parent, or friend - to leave the room when discussing the study. Sometimes, you'll need to read the participant's body language to see if he or she feels comfortable in this setting.

Forms of Communication

Web-based surveys, social media, and mobile device apps give study teams many methods for collecting data, but their use can put participant data at risk. Internet Protocol (or I.P.) addresses can reveal someone's identity and collecting digital data often involves the transmission of information over a network which could be compromised. Discuss any safety or protection measures for your digital data collection with your I.T. department.

HIPAA

Keep in mind that some health information is considered to be individually identifiable. Visit the federal HIPAA website for more specific information.

Privacy and Confidentiality Protection Strategies Continued

Let's continue to look at a few more strategies to protect your participants' privacy and confidentiality. Click each strategy to learn more. When you're done, click Next.

Data Collection

A participant needs to be fully aware of how and when data are collected. However, unless the I.R.B. has approved a waiver of consent, data cannot be collected prior to obtaining consent. Collecting data from a participant who has not consented to the study is a severe invasion of privacy, a violation of the clinical protocol, and sometimes, a federal violation.

Data Security

Data security is critical to maintaining confidentiality. The use of portable storage devices should be approved by the I.R.B. and encrypted. Additionally, be sure to keep files in a locked cabinet and password-protected computers. Always follow your institution's polices for proper and secure data storage.

You can further protect confidentiality by keeping any identifier documents separate from your collected data. This protects the confidentiality of any participant information.

Data Sharing

A good study design lays out who on a study team has access to data. If you are working on a multi-site study, develop a data use agreement, make a plan for how you will share data and have the plan approved by your I.R.B.

Password Protection

Always have a password on any computer or device that has access to study data. You can check with your own I.T. department to determine which server is the most secure for sensitive data storage.

Study Team Access

Only those listed on the I.R.B. application should be able to see and access identifiable data. This typically includes the P.I., coordinator, and research assistant. This information should be handled on a need-to-know basis. Be sure to update this list and the associated permissions whenever a member joins or leaves the study team.

Electronic Backup

It might be tempting to store identifiable data on a backup device, but you must never use a laptop, an un-encrypted flash drive, or other non-secure data storage methods to keep your files. Contact your I.T. department for approved secure storage locations.

Recording Restrictions

Video and audio recordings can be extremely valuable to a study. However, intentions for the use and storage of the recorded data must be laid out in the I.R.B. protocol and informed consent document. Participants must be fully aware that they will be recorded, and also have a full understanding of how the video or audio will be stored and eventually destroyed. Be sure to remove any identifiable information from a transcription.

Transcripts

Transcripts must have all names removed and alpha numeric codes should be used. It is important to remove all direct identifiers and to maintain code lists and data files in a separate, secure locations.

Certificates of Confidentiality (Issued by N.I.H.)

Certificates of confidentiality are issued by the National Institutes of Health (or N.I.H.) to protect identifiable research information from forced disclosure. Information that can be protected in a certificate of confidentiality includes, but is not limited to, substance abuse or other illegal behaviors, sexual attitudes, orientation, or practices, genetic information, and psychological well-being.

Take a moment to visit the Office of Human Research Protection's website explaining certificates of confidentiality. Write down any notes or questions you might have - you can get answers from your I.R.B. at a later time.

Reporting Strategies

Even in the most thorough study, an accident can happen and a breach of privacy or confidentiality may need to be addressed. How can you anticipate and plan for such an event?

As always, you must begin with a detailed plan that has been communicated with each study team member so that everyone can identify and react to a breach. Be sure to include how to communicate and report breaches in your I.R.B. and clinical protocol documents.

If a privacy or confidentiality breach occurs, you must report the incident, the manner in which it occurred, how it was discovered, and the extent of the breach. The amount or type of compromised data will determine the severity of the breach, and will dictate whether the reporting process extends to entities beyond your institution.

Any breach of confidentiality or privacy is considered a reportable event or occurrence. Regardless of terminology, your institution will have guidelines on the reporting mechanism. Take a moment to visit your I.R.B.'s website and note where to find these applicable procedures in your course study manual.

Course Study Manual Check-In

By now you should have filled in the Privacy and Confidentiality section of your Course Study Manual. If you haven't, take some time to complete this job aid. And don't forget to check out the Resources section for additional information and links, as well. When you're ready, click Next to move to the final assessment for this module.

Lessons Learned

Looking back, our study was really successful! We were able to protect our participants' privacy and we collected quality data. Our up-front communication with both the I.R.B. and our I.T.

department really helped us anticipate the privacy and confidentiality challenges we encountered along the way.