**IRB Tipsheet: Data Security Confidentiality Statement for Consent Forms**

# **I. Applicability:**

Tips for any human subjects research projects including data that are more sensitive in nature without anonymity (e.g., if audio/video recordings are made, or potentially identifying information is collected in surveys)

# **II. Writing Your Confidentiality Statement:**

When preparing the confidentiality statement that you are including in your human subjects research protocol, use this structure.

1. **Begin with the statement**: “All data will be kept confidential to the extent legally allowable. Although no data can be 100% securely stored, several precautions will be taken to maintain data confidentiality and protect your privacy, such as...”
2. **Then add the relevant precautions being taken.** Some ways to help maintain confidentiality or protect privacy are listed below:

* Storing hardcopies in locked cabinets/rooms
* Storing data on encrypted computers/servers and/or password-protected devices
* Storing data, master code lists, and completed informed consents in separate, secure locations
* Limiting access to identifiable data to as few researchers as possible
* Using number codes or pseudonyms rather than names when recording/transcribing data
* Having participants give oral rather than written, signed consent
* Not collecting any personally identifying information from participants
* Not audio or video recording participants
* Transcribing recorded data and deleting recordings as soon as possible
* Collecting/reporting minimal demographic data using only broad categories to reduce the potential of being able to identify participants from such data
* Verifying that an online survey is not recording IP addresses (e.g., checking “anonymize responses” in Qualtrics)
* Transferring data (from person to person or place to place) promptly and securely (e.g., using encrypted file transfer)
* Deleting identifiers as soon as possible
* Uploading data promptly to encrypted servers

1. If the project has **Generative Artificial Intelligence (AI) components**, a relevant statement like this should also be included:

* Removing identifying information before the AI tool has access to the data
* Removing demographic information before the AI tool has access to the data
* Using a subscription-based AI tool with enhanced privacy controls
* Changing default user settings so the data are not used to train the AI model

***NOTE:*** *Your protocol and process must match what you claim in your confidentiality statement. Keep that in mind as you are writing this statement.*