Procedures Regarding Human Subjects Protections

All UFSRC studies are reviewed by the appropriate Institutional Review Board (IRB) either through a submission by the Principal Investigator who is contracting our work, or by our unit directly.

All UFSRC policies are clearly taught in interviewer training and spelled out in the UFSRC Employee Handbook, then enforced via a three-warning system. In the event of a third violation of a single policy, they may be terminated.

Any violation of the policies below will trigger the filing of an offense. Taken together, these policies emphasize respondent privacy and protection of all data collected, including Protected Health Information (PHI).

Cell Phone/Electronics

All electronic devices must be put away while interviewers are in the lab. This includes cell phones, e-readers, calculators, and music players. There have been growing concerns with confidentiality and data security issues. This electronics policy falls in line with other reputable survey centers and reduces security risks in regard to respondent's personal information.

Respondent Information

All respondent information must be entered and stored only on UFSRC electronic equipment. Interviewers are not allowed to take or send any respondent information outside the UFSRC on an electronic device, paper, or by any other means. A shredder is kept behind the supervisor's desk and should the interviewer write any notes on paper, it is promptly destroyed.

Access to Internet

Our interviewing stations do not have access to the internet. An interviewer can access the survey and all training information, but cannot go outside of the UFSRC system.

Data Security Procedures

Before leaving their station for any reason, an interviewer must close WinCati Interviewer. They must lock the computer and if they don't, a screen saver will appear after three minutes of idle time, which locks the computer. Leaving the premises without properly logging out will result in a policy violation.

UF policy forbids any employee from sharing their profile password with anyone.
Password sharing may lead to a policy violation or possible termination.

IRB Confidentiality Statement

All studies include an IRB-approved disclaimer informing the respondent of his/her rights. This informed consent language is called the *IRB confidentiality statement*. Interviewers are required—*without exception*—to read the IRB confidentiality statement word for word prior to the start of the questionnaire.

This can be challenging since at the beginning of a call many respondents interrupt with questions, and the interviewer may provide answers from the documentation provided. Then they must return to the verbatim script in order to ensure that the respondent hears the entire statement before proceeding into the body of the interview.

The penalties for failing to read the IRB confidentiality statement exactly as written are as follows:

- 1st strike – Warning
- 2nd strike - $100 incentive deduction
- 3rd strike – Termination

Time Length

Interviewers are not allowed to say a particular time frame other than that which is scripted into the interview. The point of this protocol is to be as accurate as possible about time lengths with the respondent. Interviewers must give only estimates of percentage completed if respondents ask how much time is left until the survey is completed.

Falsifying Data

Illegitimate manipulation of data is prohibited. Attempts at data falsification might include:

- Entering data not provided by the respondent.
- Entering data different from what the respondent provided.
- Skipping one or more screens without reading the question.
- Failing to go back to a previous question to change a respondent's answer when the respondent indicates they answered a question incorrectly.

Data falsification is not tolerated nor possible at the UFSRC since 100% of our phone calls are recorded and saved for 6 months. A percentage of phone calls is monitored live and reviewed by recording, and any suspicion can be investigated by reviewing the recordings of an interviewer's work.

Secure Data Delivery

We have a secure web-based portal that requires authentication for the uploading of sample files and delivery of datasets. This provides HIPAA-compliant protection for our clients and colleagues who are outside the UF system.