Procedures for secure data use and presentation:

1. Each team member has a unique login and password. You may never, under any circumstances, log someone else in. You may never, under any circumstances, share your login and password with anyone
2. You may never, under any circumstances, copy, move, or otherwise transport the data from the secure folders on the server, in whole or in part, without written permission from Dr. Aiello. This includes moving data to USB ports, hard drives, desktop, laptop, or anywhere else.
3. You may NOT, under any circumstances, show any individual without authorization any component or the whole of the data itself.
4. You may NOT, under any circumstances, discuss or present study data in general or the results of specific analyses with anyone outside of the core Aiello Research team without approval or until the data is published and in public domain. The core team includes current student research assistants who are responsible for conducting statistical analyses, research support staff (Study Manager and other senior staff members), and the PI (Dr. Allison Aiello).
5. Ascertain that whatever computer you are working on is set up to require login after 10 minutes of inactivity.
6. If you are working in the Aiello laboratory, remember to lock the door whenever you leave, even if you will only be gone for a few minutes. Securing our physical work spaces is a key first step in data security.
7. All project staff must read and comply with the UNC Information Security policies.
    a. http://its.unc.edu/about-its/university-it-policies/
8. Sensitive information **must** be encrypted. At no time shall a dataset, file, database, or document containing sensitive information be left unencrypted.
9. Email is **not** allowed for transferring sensitive data.
10. All data and secure materials provided to you must be saved in a secure location with a log-in at your home institution. If no secure location is available at the home institution, notify Dr. Aiello and a folder will be created for you on the University of North Carolina server. All datasets must be saved in the same location as original.
11. Data is only to be used for the proposed paper or abstract. If you would like to use the data for additional analyses or if your aims have changed, an updated or new Research and Data Request form must submitted to staff for approval.
12. For data requestors outside the UNC ARG team, upon completion of the approved project, all data must be destroyed. You may not keep data "just in case" you want to use it again. All analytical files you have created from this data must also be deleted. When you delete this data, please contact study staff to inform us that the data has been deleted. You may be contacted by study staff to inquire about the status of the data. Please respond to these communications.

Procedures for seeking advice from outside sources:

While we need input from outside sources, it is essential to maintain the security of our data while doing so. Accordingly, when seeking advice, be certain to adhere to the following guidelines:

13. You may outline the problem both verbally and in written form
14. You may show relevant code
15. You may NOT, under any circumstances, show any component or the whole of the data itself.

If you have any questions about the above guidelines, please feel free to address your concerns with the PI, Study Manager, or other senior staff members.

It is of the utmost importance that you maintain these security measures when working with the data. Non-compliance may result in disciplinary action from the Aiello Research Group. Please report any deviations from the above security guidelines to Dr. Aiello.

I have read, understand, and will follow the data security procedures as outlined above.

Signed_____ **Date**_____

Print Name_____