Level I Data Security Recommendations:

Based on the information you've provided, your study will be collecting data that do not require additional security measures. However, it is still recommended that you follow best computing and security practices in protecting any data.

**Recommended Measures for Level I Data Security**

1. Access to study data should be protected by a username and password that meets the complexity and change management requirements of a UNC ONYEN.
2. Study data that are accessible over a network connection should be accessed from within a secure network (i.e., from on campus or via a VPN connection).
3. Computers storing or accessing study data should have Endpoint Protection (AntiVirus/AntiSpyware) installed and be updated regularly where technologically feasible.
4. Patch management and system administration best practices should be followed at all times on systems storing or accessing your data.
5. Users should be granted the lowest necessary level of access to data in accordance with IT’s Security’s Standards and Practices for Storing or Processing Sensitive Data (when technologically feasible).

**These recommendations do not replace or supersede any security plans or procedures required by granting agencies or sponsors. Questions or concerns about compliance with these recommendations should be directed to your local IT support staff.**

**Additional IT Security Resources**

- [IT’s Security](#)
- [Caroline Population Center Security Guidelines](#)
- [SCM Information Security](#)

Level II Data Security Requirements:

Based on the information you’ve provided, your study will be collecting data that require additional security measures to ensure that they are adequately protected from inadvertent disclosure. Due to the nature of these data, you are required to implement the following security measures on any computer(s) that will store or access information collected for this study. We strongly suggest that you coordinate your efforts in this area with your unit’s IT support or IT security personnel.

**Required Measures for Level II Data Security**

1. Access to study data must be protected by a username and password that meets the complexity and change management requirements of a UNC ONYEN.
2. Study data that are accessible over a network connection must be accessed from within a secure network (i.e., from on campus or via a VPN connection).
3. Computers storing or accessing study data must have Endpoint Protection (AntiVirus/AntiSpyware) installed and updated regularly where technologically feasible.
4. Patch management and system administration best practices should be followed at all times on systems storing or accessing your data.
5. Users should be granted the lowest necessary level of access to data in accordance with IT’s Security’s Standards and Practices for Storing or Processing Sensitive Data (when technologically feasible).

**These requirements do not replace or supersede any security plans or procedures required by granting agencies or sponsors. Questions or concerns about compliance with these requirements should be directed to your local IT support staff.**

**Additional IT Security Resources**

- [IT’s Security](#)
- [Caroline Population Center Security Guidelines](#)
- [SCM Information Security](#)

Due to the nature of your study data, the senior IT official in your school or department will be also notified about your study and may contact you or your technical contact(s) to discuss any data security questions on concerns they may have. If you have indicated that your research will take place in another unit on campus (i.e., a Center or Institute), that group will also be notified.
Level III Data Security Requirements:

Based on the information you’ve provided, your study will be collecting sensitive data that require additional security measures to ensure that they are adequately protected from inadvertent disclosure. Due to the nature of these data, you are required to implement the following security measures on any computer(s) that will store or access information collected for this study. We strongly suggest that you coordinate your efforts in this area with your unit’s IT support or IT security personnel.

**Required Measures for Level III Data Security**

1. Access to study data must be protected by a username and password that meets the complexity and change management requirements of a UNCG ONYEN.
2. Study data that are accessible over a network connection must be accessed from within a secure network (i.e., from on campus or via a VPN connection).
3. Computer(s) storing or accessing study data must have **Endpoint Protection** (AntiVirus/AntiSpyware) installed and updated regularly where technologically feasible.
4. Patch management and system administration best practices should be followed at all times on systems storing or accessing your data.
5. Study data must be encrypted where technologically feasible. The University has licensed PGP encryption products that your IT staff can assist you in deploying to encrypt your data. [http://its.unc.edu/infoSecurity/services-offered/index.htm](http://its.unc.edu/infoSecurity/services-offered/index.htm)
6. Computers used to store study data must be scanned for vulnerabilities on an ongoing basis. Qualys scanning from IT’s Security is highly recommended. [http://its.unc.edu/infoSecurity/services-offered/index.htm](http://its.unc.edu/infoSecurity/services-offered/index.htm)
7. Users should be granted the lowest necessary level of access to data in accordance with IT’s Security’s Standards and Practices for Storing or Processing Sensitive Data (when technologically feasible).

**These requirements do not replace or supersede any security plans or procedures required by granting agencies or sponsors. Questions or concerns about compliance with these requirements should be directed to your local IT support staff.**

**Additional IT Security Resources**

- [ITS Security](http://its.unc.edu/infoSecurity/services-offered/index.htm)
- [Carolina Population Center Security Guidelines](http://its.unc.edu/infoSecurity/services-offered/index.htm)
- [SOCM Information Security](http://its.unc.edu/infoSecurity/services-offered/index.htm)

Due to the sensitivity of your study data, the senior IT official in your school or department will be also notified about your study and may contact you or your technical contact(s) to discuss any data security questions or concerns they may have. If you have indicated that your research will take place in another unit on campus (e.g., Center or Institute), that group will also be notified.