Level I Data Security Recommendations:

Based on the information the PI provided, this study will be collecting data that does not require additional security measures. However, it is still recommended that the PI 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 ITS 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 the administering department's IT support staff.**

Level II Data Security Requirements:

Based on the information the PI provided in the IRB application, this 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, the PI is required to implement the following security measures on any computer(s) that will store or access information collected for this study. The PI should coordinate efforts in this area with the unit's IT data security personnel receiving this email.

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 ITS 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 the administering department's IT support staff.**

Additional IT Security Resources

- ITS Security
- Carolina Population Center Security Guidelines
- SOM Information Security
- ITS Research Computing

Due to the nature of this research study, the senior IT official in the administering department is receiving this email about the study and may contact the PI or technical contact(s) to discuss any data security questions on concerns they may have. If the PI has indicated that the research will take place in another unit on campus (i.e., a Center or Institute), that group will also be notified.

Additional IT Security Resources

- ITS Security
- Carolina Population Center Security Guidelines
- SOM Information Security
- ITS Research Computing

Level III Data Security Requirements:

Based on the information the PI provided in the IRB application, this 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, the PI is required to implement the following security measures on any computer(s) that will store or access information collected for this study. The PI should coordinate efforts in this area with the unit's IT data security personnel receiving this email.

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 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. Study data must be encrypted where technologically feasible. The University has encryption products that your IT staff can assist you in deploying to encrypt your data. 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 ITS Security is highly recommended). 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 ITS 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
- Carolina Population Center Security Guidelines
- SOM Information Security

- **ITS Research Computing**

Due to the sensitivity of this study's data, the IT data security staff in your school or department are being notified about this study and may contact the PI or technical contact(s) to discuss any data security questions on concerns they may have. If the PI has indicated that the research will take place in another unit on campus (i.e., a Center or Institute), that group will also be notified.