General Information

1. General Information

1. Project Title

No Answer Provided

2. Project Personnel

1. List all project personnel beginning with principal investigator, followed by faculty advisor, co-investigators, study coordinators, and anyone else who has contact with subjects or identifiable data from subjects.

   - List ONLY those personnel for whom this IRB will be responsible; do NOT include collaborators who will remain under the oversight of another IRB **for this study**.
   - If this is Community Based Participatory Research (CBPR) or you are otherwise working with community partners (who are not functioning as researchers), you may not be required to list them here as project personnel; consult with your IRB.
   - If your extended research team includes multiple individuals with limited roles, you may not be required to list them here as project personnel; consult with your IRB.

   The table below will access campus directory information; if you do not find your name, your directory listing may need to be updated.

Data Security Requirements

Data Security

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.*

Additional IT Security Resources

- *ITS Security*
- *SOM Information Security*
- *ITS Research Computing*

Level II Data Security Requirements:

Based on the information the PI provided in the IRB application, this study will be collecting sensitive (University Tier 2 or 3) data that require additional security measures to ensure that the data are adequately protected from 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 information technology support staff.

Required Measures for Level II Data Security

1. *It is strongly recommended that you consult with an IT Professional and/or the Information Security Liaison in your unit to understand your responsibilities and the secure technology resources that are available from UNC-CH.*
2. *Both individuals and devices working with study data must be in compliance with the Information Security Controls Standard and other applicable policies.*
3. *Study data either stored with or shared with an external organization such as another research organization or using a cloud-based platform must be approved and rated for working with sensitive data. Previously-approved applications can be found at the Information Security Office's Purchasing Guide. Unless the application on the guide is available for general use, please open a request for a risk assessment and data governance review via ITS Help.*
4. *Any access to study data from individuals or systems must follow the Password, Pass-phrases, and Other Authentication Methods Standard.*

***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 staff.*

Additional IT Security Resources

- *ITS Security*
- *Data Governance*
- *SOM Information Security*
- *IT Research Computing*
- *Institutional Privacy Office*
- *Digital Accessibility Office*

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.

Level III Data Security Requirements:

Based on the information the PI provided in the IRB application, this study will be collecting sensitive (University Tier 2 or 3) data that require additional security measures to ensure that the data are adequately protected from 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 information technology support staff.

Required Measures for Level III Data Security

1. *It is strongly recommended that you consult with an IT Professional and/or the Information Security Liaison in your unit to understand your responsibilities and the secure technology resources that are available from UNC-CH.*
2. *Both individuals and devices working with study data must be in compliance with the Information Security Controls Standard and other applicable policies.*
3. *Study data either stored with or shared with an external organization such as another research organization or using a cloud-based platform must be approved and rated for working with sensitive data. Previously-approved applications can be found at the Information Security Office's Purchasing Guide. Unless the application on the guide is available for general use, please open a request for a risk assessment and data governance review via ITS Help.*
4. *Any access to study data from individuals or systems must follow the Password, Pass-phrases, and Other Authentication Methods Standard.*

***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 staff.*

Additional IT Security Resources

- *ITS Security*
- *Data Governance*
- *SOM Information Security*
- *IT Research Computing*
- *Institutional Privacy Office*

- Digital Accessibility Office

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.

1. Data Security Level Acknowledgement

   No Answer Provided