In consultation with the UNC Information Security Office and the Office of Research Information Systems, and based on the information you’ve provided your study will be collecting data that requires additional security measures to ensure they are adequately protected from inadvertent disclosure. Due to the nature of this data, you will be required to implement the following security measures on any computer(s) that will store or access information collected for this study. Additionally, as Level 2 data the University security policy does not allow for you to store the information at your place of employment as those servers are not owned or managed by the University. They are not authorized for storage via an appropriate contract that has been approved by the Office of University Counsel.

You can however use VPN to connect to the UNC MPA secure space where all your data should be stored. VPN will give you the ability to connect to this storage space from anywhere you have a network connection (work or home). For more information about VPN please see http://help.unc.edu/2502

**Required Measures for Level II Data Security**

- Access to study data **must** be protected by a username and password that meets the complexity and change management requirements of a UNC ONYEN.
- 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).
- Computers storing or accessing study data **must** have Symantec Endpoint Protection (AntiVirus/AntiSpyware) installed and updated regularly where technologically feasible.
- Patch management and system administration **best practices** should be followed at all times on systems storing or accessing your data.
- 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).

**Connecting to SOG Network Drives from Off-Campus**

1. Begin by opening ‘My Computer’ from your desktop or Start Menu.
2. Choose ‘Tools’ then select ‘Map a Network Drive’.
3. In the next window, select the ‘S’ Drive and in the box Labeled ‘Folder’, type \esmna1.isis.unc.edu\sog_secure
4. Click ‘Finish’.
5. For the first drive you map, click the option to ‘Connect using a different user name’. When prompted, type AD\<username> in the ‘User’ box, and AD Login Password in the ‘Password’ box.
6. Choose ‘OK’, and then click ‘Next’. The drive should automatically open.
7. If you wish to map additional drives, begin the process again.