Data Security Plan Guidelines for use of NCERDC Data

The fundamental goal of the protections outlined in the Data Security Plan is to prevent persons who are not signatories to the Data Use Agreement or the Supplemental Agreement with Research Staff from gaining access to the data. When these agreements are executed, all members of the research team are obligated to follow all aspects of the Data Security Plan.

The Data Security Plan must be included in the research protocol submitted to the Institutional Review Board (IRB) by the Principal Investigator of each project.

The NCERDC requires that the original de-identified data files, and all resulting temporary and derived data files, must be stored on a secure network server with protections and restrictions appropriate for sensitive data. The data security plan must include a discussion of the computing environment in which the data will be managed, analyzed, stored, and transmitted among research team members. Investigators must provide details about the server on which data will be stored, how the networked system handles backups, and how long system backup copies of the data are kept. The security plan should include a description of the following:

- All locations where the data and paper files will be kept.
- The secure network server on which data will be stored, how the networked system handles backups, and how long system backup copies of the data are kept.
- The network's security protocols, including protections for original data sent by NCERDC and temporary analysis files.
- Information on how all files are tracked, accounted for, and schedule for deletion.
- The security system that would prevent unauthorized access to the data, and whether this system is used by other projects.

All data security plans must include the following statements:

ALL storage and analysis of NCERDC data will take place exclusively on the secure server. Data may not be downloaded to local workstations, or to any external devices, including laptops. Desktop and laptop workstations may be used only for remote access to the secure server.

Portable storage devices, including laptops, will not be used for downloading or storing data.

NCERDC data will NOT be shared with any other institution or any investigator not currently listed in the data use agreement. This restriction applies to source data as well as all derived data files. Project investigators, including the PI, do not have discretion to modify access to the NCERDC data. Any changes in access to the data on the secure server require explicit prior approval by the NCERDC.

All data security protections apply to the original NCERDC data, derived files, and temporary analysis files.