Preliminary Application Checklist for DNORS Restricted Data Version 3

Name: _____

Project title: _____

_____

☐ Research Proposal

- ☐ Specific aims of the project
- ☐ Scientific significance of the proposed research
- ☐ Types of variables from DNORS that the researcher intends to use for the proposed research
- ☐ Justification of the need for the Version 3 Restricted Data
- ☐ An analysis plan
- ☐ A proposed start date and end date for the project

☐ Data Access list

- ☐ A complete list of individuals who will have access to the data, including the names and responsibilities of the investigators and research staff (e.g., students, research assistants, and programmers)
- ☐ Current CV for each individual listed

☐ Data Protection Plan

- ☐ List and description of all locations where the original and all copies of the data will be kept
- ☐ Description of computing environment in which the data will be used, including:
  - ☐ Computing platform and operating system
  - ☐ Number of computers on which data will be stored or analyzed
  - ☐ Whether computers will be on a network (i.e., connected to the Internet) or will operate stand-alone (i.e., with no network and/or Internet connection)
  - ☐ Physical environment in which computer is kept
  - ☐ List and description of all device(s) on which data will be stored (e.g., network server, mainframe computer storage device, PC hard drive)
  - ☐ Data storage methods when data are not being used
  - ☐ Methods of data transmission between research team members (if applicable)
  - ☐ Methods of computer output storage in both electronic form and hard copy (on paper or other media)
  - ☐ Instruction in data protection policies to be provided to each staff member prior to data access, including frequency of instruction review and/or re-training of staff members

☐ Disclosure Rules; at minimum, researchers must agree to exclusion of the following from any type of publication or presentation:

- ☐ Listing of individual cases
- ☐ Description of individual cases
- ☐ Listing, description, or identification of any geographic unit smaller than a SPA (Service Planning Area) by number, by name, or by descriptive information, to include ZIP code areas, tracts, block groups, or blocks
- ☐ Maps with any features that allow tracts or smaller geographic units to be identified
- ☐ Summary statistics or tabulations by geographic level below SPA (Service Planning Area)

☐ Types of protection expected:

- ☐ Computers must be located in locked offices; access to the offices should be restricted to project personnel only, with the offices locked at all times when not occupied by project personnel
- ☐ Log of all acquired data files and dates files were received, returned, or destroyed
- ☐ Password-protected access to all computers storing the data, with automatic activation of password protection after 5 minutes
- ☐ All files containing data stored in password-protected, encrypted form (including log files)
- ☐ No storage of the data on laptop computers, unsecured network servers, etc.
- ☐ No automated backup copying of the data
- ☐ Removable devices holding the data (CDs, diskettes, zip drive disks, etc.) encrypted with strong password protection and stored in a locked compartment or room when not in active use
- ☐ Appropriate printout handling procedures (i.e., immediate pick up after printing, storage when not in use, and secure disposal by shredding when no longer needed)
- ☐ Reported results must not jeopardize respondent confidentiality
- ☐ No transmittal of data or detailed tabulations via e-mail or e-mail attachment
- ☐ Data can be hand-transferred or sent by tracked shipment (e.g., FedEx) using a removable device (CDs, diskettes, zip drive disks, etc.) or can transmitted by Secure FTP provided that the data files are not placed on a public server accessible without a password; data must be encrypted with strong password protection
- ☐ Use of e-mail, e-mail attachment, FTP, or any other means of electronic transfer to transmit only results from regression analyses and aggregate descriptive analyses
- ☐ Training procedures for staff members with data access regarding the Data Protection Plan, appropriate data use, and penalties for inappropriate use
- ☐ Destroying all sensitive data files upon completion of the project (specify the secure erase program to be used)
- ☐ Reporting any and all violations of the Data Safeguarding Plan in writing to the Restricted Data Investigator, to the local Institutional Review Board, and to RAND

☐ **Application Fee:** Check made payable to RAND in the amount of $650

<u>Please enclose a copy of this checklist with your application</u>