Preliminary Application Checklist for DNORS Restricted Data Version 4

Name: _____

Project title: _____

_____

Version 4 of the DNORS Restricted Data is only available to researchers who are Principal Investigators (PIs) of a federally-funded research project or researchers who working in a federally-funded research center (including, but not limited to, an NIH-funded Population Research Center or Center for the Demography of Aging). For those working in a federally-funded center, the Center Director (i.e., the PI of the center) must agree to take responsibility for data protection.

☐ Federally-Funded Project

- ☐ Title of grant or contract and name of PI
- ☐ Grant or contract number and federal agency
- ☐ Start date and end date of grant or contract
- ☐ Program officer name, title, address, telephone number, and e-mail address

☐ 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 4 Restricted Data
- ☐ An analysis plan
- ☐ A proposed start date and end date for the project (the end date cannot extend beyond end-date of the federally-funded contract or grant supporting 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:

- ☐ Physical environment in which computer is kept
- ☐ Computing platform and operating system
- ☐ Number of computers on which data will be stored or analyzed
- ☐ Indication that computers will be stand-alone (i.e., with no network connection) or on a secure, isolated network (i.e., with no local area or Internet connection)
- ☐ 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
- ☐ Indication that data will not be transmitted between research team members
- ☐ Procedures for reviewing and approving by the Restricted Data Investigator or Data Enclave Administrator all requests to print or remove on media any results or data
- ☐ 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:

- ☐ **Description of a secure physical or virtual data enclave**
- ☐ Computers must be located in a locked facility, with access to the facility restricted to project personnel only; the facility must be locked at all times when not occupied by project personnel
- ☐ All computers must have a separate BIOS password, known only to the Restricted Data Investigator or the Data Enclave Administrator
- ☐ Computers must be configured (through the password-protected BIOS) to prevent any devices from being installed—for example, users must not be able to set up their own network connections, including wireless network connections; other ports, such as the parallel, COM, and USB ports, should be disabled in the password-protected BIOS
- ☐ Only the Restricted Data Investigator or Data Enclave Administrator must be able to create user accounts on the computer
- ☐ Any device that can be used to copy data from the computer (e.g., CD or DVD writer, diskette drive, USB port) must be locked and unavailable (or set to read-only) to all users except for the Restricted Data Investigator or Data Enclave Administrator
- ☐ All permissions to create files and directories on the system hard drive outside the user's home directory should be locked (this is to prevent users from making any changes to the operating system)
- ☐ 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 **original** 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
- ☐ Original data storage devices destroyed or files deleted with a secure erase program (specify which one) when no longer needed or at end of project
- ☐ 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 by any means**
- ☐ 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 (and 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

Please enclose a copy of this checklist with your application