APPLICATION FOR DATA LICENSE

Name of Receiving Institution / Organization: David Norris Consulting, LLC

Name & Title of Principal Project Officer (PPO): David C. Norris, MD

PPO Address: 523 Broadway E, Suite 348, Seattle WA 98102-5384

(*Provide street address, city, state, zip code, department and building name, and office / room number)*

PPO Phone Number: 206-327-9280 PPO Email: david@dnc-llc.com

Title of Research Project: Housing Mobility and Adolescent Mental Health (Reproduction)

To be completed by HUD:

Circle one: Approved Denied Returned for modification

Date data must be destroyed unless written extension provided by HUD: _____

PROPOSED RESEARCH PROJECT

1. List the survey name, year and wave description (if any) of the data file(s) you wish to access.
mental_health_yt_20101004.sas7bdat mental health variables from Final Youth Survey

2. Briefly describe your research objective and how you will use the requested data. (*You may also attach a research proposal*.)
As previously described in connection with abovenamed study.

3. Explain why the public-use files cannot meet your research need.
Public use files do not provide the resolution needed to reproduce previous study.

4. If you plan to link the requested data to any other data, list these other dataset names and describe how linking the data will allow you to achieve your research objectives.
No linkage will be done.

5. What is the scientific and/or policy value of your proposed research? Which sector(s) of the housing and urban development community will be served by your work?
Reproduction and re-analysis of published study; integral to the scientific process.

6. Do you agree that the requested data will not be used for any administrative or regulatory purpose?
Yes.

7. How long will you need access to this data?
6 months.

SECURITY PLAN

Please describe your security plan by providing specific information to answer each of the questions below. You may attach or insert additional materials as needed.

Physical Location of Data

Project Office Address: 107 Spring Street #3007, Seattle WA 98104

(*Provide street address, city, state, zip code, department and building name, and office / room number)*

Project Office Phone Number: 508-561-2617

Note: The PII data and computer must be secured and used **only** at this location. When the data are not being used, the data must be stored under lock and key at this location. Only authorized users of the data, as listed on the License, may have key access to the secure project office/room.

Computer System Information

1. Provide a detailed description of the **physical computing environment** where the PII will be stored and analyzed, including precise physical location(s) of the computer and original data CD.
Non-networked, encrypted-disk Linux workstation in locked office #3007 as above.

2. Describe the procedure for back-ups for this computer system. How will the requested data be excluded from routine back-ups?
No backups will be performed during the period of this study.

3. Who has physical access to the equipment? Who has permission to use the equipment?
(*As a general matter, only authorized users who have signed affidavits agreeing to data confidentiality procedures should have access to the room with the secure computer and hard copy data. If you propose an alternate arrangement, please describe in detail.)*

4. Is this system used by other projects?
No.

5. Where will hard copy output be printed? Describe the storage and disposal methods for hard copy output.
No printouts will be made or utilized.

Note: Receiving institutions must provide a secure computing environment. In general, this means a physically secure PC(s) *not attached* to the institutional network or to the Internet, a local printer using easily identified paper not to leave the secure facility, and a local shredder for discarded paper. Back-up of processing programs is permitted, but back-up of data files is not. *Use of a laptop computer, external hard drive, or USB memory stick is strictly prohibited. Absolutely no PII data may be copied onto a server or computer that is attached to the Internet or an institutional network.* Researchers may propose an alternative computing set-up, but the stand-alone PC in a secure environment accessible only to authorized users is the accepted method and the standard against which alternatives will be evaluated.

Security System Information

1. Describe the BIOS configuration (e.g., boot the computer from the hard drive only, plus password protection of BIOS so changes cannot be made to the BIOS without authorization).
Password-protected BIOS allowing boot only from hard drive.

2. Describe the physical security of the location where data are to be stored and used.
Office building with keyed main entry, and separately keyed entry to private office itself.

3. Describe the installed encryption software for directories containing secure data (i.e. Windows 2000 encryption).
LVM encryption by AES-256 algorithm

4. Describe the installed secure erasure program and the protocol for running it.
'shred' and 'wipe' utilities; hdparm / ATA Secure Erase (Seagate 7200.12 - 500 GB)

5. Will the network interface card (NIC) be removed or disabled so it cannot be used?
The NIC on the motherboard will be disabled in BIOS.

File Access Management

1. Describe the number and location of copies of the data.
A single copy of the data will be maintained on an encrypted hard drive partition.

2. Describe the rules for creation of and access to temporary (i.e., analytic) files.
To be created on an AES-256 encrypted partition; swap partition is encrypted likewise.

3. How will hard copy data be handled, stored, and disposed of?
Hard copies will not be produced.

4. How will data access be restricted to the Principal Project Officers and authorized team members?
Keyed office door; double authentication with password and Yubico physical token.

5. Describe the rules for passwords and screen saver activation.
Screensaver activates on removal of leashed Yubico token, ensuring physical proximity.

Communication of PII Data

1. Describe the rules for communication or transmission of detailed data tabulations.
Tabulations inspected to ensure PII maintained confidential; e.g., no low cell counts.

2. Describe any circumstances under which analytic output from the MTO data will be transferred electronically (e.g., what are the restrictions on the content of electronic transfers?).
Only summary stats, e.g. reproductions/re-analyses of published tables, will be shared.

Research Team Training and Monitoring

1. Describe the plan for training research team members in the restrictions and security provisions of this agreement.
David Norris has completed CITI training.

2. Describe the plan for monitoring the periodic aspects of this plan, such as back-ups, password changes, and erasure of temporary directories and files.
Password change at 3 months. Routine backups only for code + outputs.

End of Project Procedures

1. Describe the steps to be taken at the completion of the research project.
Secure erasure of HDD.

2. Please provide any additional information relevant to the security of the PII data.
The body-leashed Yubico encryption token adds 1 extra layer of security.

In submitting this application, the researcher agrees to comply with the security protocols outlined above. Additionally, the following physical location and computer security procedures must be implemented when in possession of PII data. By checking the box next to each security procedure, you signify that these procedures will be implemented for the duration of the project and License period:

Only authorized users listed on the License will have access to the PII data, files derived from the PII data, and the secure room in which the data is housed. Access will be limited to the secure room/project office by locking office when away from the office. ☑

Data will only be secured, accessed and used within the secure project room/office ☑

A password will be required as part of the computer login process. ☑

The password for computer access will be unique and at least 8 characters with at least one non-alphanumeric character and a mix of upper- and lower-case characters. ☑

The computer password will change at least every 3 months or when project staff leave. ☑

Read-only access will be initiated for the original data. ☑

An automatic password protected screensaver will enable after 3 minutes of inactivity. ☑

No routine backups of the PII data will be made. ☑

Project office room keys will be returned and computer login will be disabled within 24 hours for any user who leaves the project. The PPO will notify HUD of staff changes. ☑

PII data will not be placed on a server (network), laptop computer, USB memory stick, or external hard drive. ☑

The Receiving Institution must make available for inspection, at reasonable hours, by HUD the physical housing and handling of all data files and any other information, written or electronic, relating to this agreement. ☑

The data will removed from the project computer and overwritten, whether at the end of the project, or when reattaching a modem or LAN connection. ☑

The receiving institution will, at the conclusion of the license period or completion of the research, whichever comes first, return the original data transfer medium to HUD and to destroy all copies made of the data. ☑

The Receiving Institution and researcher further agree:

The Receiving Institution will not add to the list of authorized users of the data nor reduce any security arrangements without first notifying HUD. ☑

The Receiving Institution agrees that it has no interest in the identity of individuals in the data file and will make no attempt to determine, through computer matching or other means, the identity of individuals in the file. ☑

No cell describing 10 or fewer cases (small cell) can be released, or be obtainable by subtraction to people not on the list of authorized users of the data, unless agreed to by HUD. ☑

The Receiving Institution will immediately inform HUD in case of suspected breach. ☑

In the event that HUD determines that confidentiality has been breached, the Organization will return all copies of the data to HUD and will be denied further access to the data until the Organization provides sufficient assurance, acceptable to HUD, that the data disclosure will not be repeated. ☑

The Organization will attribute HUD as the source of these data in all reports and other data products produced with these data. The Organization agrees to provide HUD with copies of the relevant portions of all documents that present these data. ☑

HUD will review annually the Organization's ability to maintain the confidentiality of the data and may revoke the Organization's access to the data if there is sufficient evidence that the Organization has not maintained adequate safeguards.