APPLICATION FOR DATA LICENSE

Name of Receiving Institution / Organization: **Anolinx, LLC**

Name & Title of Principal Project Officer (PPO): **Andrew Wilson, Lead Pharmacoepidemiologist**

PPO Address: **428 E Winchester, Salt lake City, UT 84107   Anolinx Office: Suite 202**
(*Provide street address, city, state, zip code, department and building name, and office / room number*)

PPO Phone Number: **888-968-5469**   PPO Email: **awilson@anolinx.com**

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

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 containing mental health variables from the Final Youth Survey

2. Briefly describe your research objective and how you will use the requested data. (*You may also attach a research proposal*.)
 Attached.

3. Explain why the public-use files cannot meet your research need.
 Publicly available datasets do not provide the data 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 other data linkage.

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 of a high-impact publication based on results of the survey data.

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? **9 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: <u>**428 E Winchester, Salt lake City, UT 84107   Anolinx Office: Suite 202**</u>
(*Provide street address, city, state, zip code, department and building name, and office / room number*)

Project Office Phone Number: <u>**888-968-5469**</u>

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.
 Data will be stored on a non-networked password-protected desktop PC housed in a locked room.
2. Describe the procedure for back-ups for this computer system. How will the requested data be excluded from routine back-ups?
  Folder housing dataset will be excluded from any regular disk backup.
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.*)
  Only Andrew Wilson has access to this computer.
4. Is this system used by other projects?
  Not until completion of this project.
5. Where will hard copy output be printed? Describe the storage and disposal methods for hard copy output.
 Summary statistics will be shared via local printout. Hard copy printouts will be shredded after use.
 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).

2. Describe the physical security of the location where data are to be stored and used.
Room housing computer is equipped with deadbolt lock with no other personnel access.
3. Describe the installed encryption software for directories containing secure data (i.e. Windows 2000 encryption).
Windows Encrypting File System (EFS) for Windows 7 will be used to encrypt files.
4. Describe the installed secure erasure program and the protocol for running it.
Piriform CCleaner v4.10 will be used with complex (7-pass) overwrite to delete data files when complete.
5. Will the network interface card (NIC) be removed or disabled so it cannot be used?

Yes.

File Access Management

1. Describe the number and location of copies of the data. **1 Copy stored onsite in secure office.**

2. Describe the rules for creation of and access to temporary (i.e., analytic) files. **All temporary files will be securely deleted at the end of every analytic session.**
3. How will hard copy data be handled, stored, and disposed of?
Any hard copies to be maintained will be kept in a locked filing cabinet in the locked office .
4. How will data access be restricted to the Principal Project Officers and authorized team members? **Data will not be made available except through the secure password-protected desktop.**

5. Describe the rules for passwords and screen saver activation.
Computer locks after 15 minutes of inactivity and requires complex password to unlock.

Communication of PII Data

1. Describe the rules for communication or transmission of detailed data tabulations.
Detailed data tabulations will only be shared when PII can be maintained, e.g., cell counts sufficiently high.
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 summarized statistics or tables will ever 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. **Employees have all taken HIPAA related CITI (data security) 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.

We will perform monthly internal data protocol audits to monitor data use.

OMB Control Number 2528-0297

End of Project Procedures

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

2. Please provide any additional information relevant to the security of the PII data.

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. **x**

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

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

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. x

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

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

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

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

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. x

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

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. x

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. x

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. x

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. x

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. x

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. x

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

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. x

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. x

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.

The primary purpose of this research which motivates the need for this dataset is to replicate the analysis and validate the findings published last year in the high-visibility, high-impact journal JAMA.

Citation:

> **Kessler R.C.**, Duncan G.J., Gennetian L.A., Katz L.F., Kling J.R., Sampson N.A., Sanbonmatsu L., Zaslavsky A.M., **Ludwig J.** (2014 Mar 5). "Associations of Housing Mobility Interventions for Children in High-Poverty Neighborhoods with Subsequent Mental Disorders during Adolescence." JAMA 311, no. 9 (March 5, 2014): 937–48. doi:10.1001/jama.2014.607.

Specifically, we will

1. Use SAS code (and random seed) shared by Ronald Kessler, to reproduce the imputation of 'PTSD' outcomes in the MTO Final Youth Evaluation, as reported in Kessler RC, Duncan GJ, Gennetian LA, et al. "Associations of Housing Mobility Interventions for Children in High-Poverty Neighborhoods with Subsequent Mental Disorders during Adolescence." *JAMA* 311, no. 9 (March 5, 2014): 937–48. doi:10.1001/jama.2014.607.
2. Verify that the PTSD counts for boys and girls in Table 5 of that article are faithfully reproduced.
3. Repeat Step 1 iteratively to generate an ensemble of imputed 'PTSD' outcomes that abstracts away the arbitrariness of single imputation.
4. Demonstrate that an analysis of the ensemble so generated coincides with a direct analysis of the logit probabilities that were generated in Step 1 as an intermediate of the imputation process (which employed a logistic regression).
5. If access can be obtained to the NCS-R data on which the abovementioned logistic imputation model was developed, a further step of abstraction will be undertaken: this model will be re-estimated with shrinkage to correct for overfitting, and used to repeat steps 3 and 4 above; the predictive performance of this model will also be characterized.
6. Every reasonable effort will be made to publish the results of these replication studies.