Attachment 17

PATH Study
ICPSR Data Use Agreement

Restricted Data Use Agreement
for Use of Confidential Data through the ICPSR Virtual Data Enclave ("VDE") from the National Addiction and HIV Data Archive Program ("NAHDAP")

I. Definitions

A. "Investigator" is the person primarily responsible for analysis and other use of Confidential Data obtained through this Agreement.

B. "Virtual Data Enclave Users (VDE Users)" are all persons at the Investigator's institution, including the Investigator, who will have access to Confidential Data obtained through this Agreement.

C. "Institution" is the university or institution meeting the criteria in Section IV at which the Investigator will conduct research using Confidential Data obtained through this Agreement.

D. "Representative of the Institution" is a person authorized to enter into legal agreements on behalf of Investigator's Institution.

E. "Confidential Data" consist of identifiable private information, linkable to a specific individual either directly or indirectly, for which the individual (whether a person or organization) has the expectation that the information will not be released in a manner that allows public identification of the individual or causes some harm to the individual.

F. "Private Person" means any individual (including an individual acting in his official capacity) and any private (i.e., non-government) partnership, corporation, association, organization, or entity (or any combination thereof), including family, household, school, neighborhood, health service, or institution.

G. "ICPSR" is the Inter-university Consortium for Political and Social Research, an international consortium of academic institutions and research organizations housed at the University of Michigan.

H. "ICPSR Virtual Data Enclave (VDE)" is an online secured facility using two-factor authentication for VDE users to access and analyze Confidential Data that are available from NAHDAP/ICPSR. The VDE simulates a non-Internet connected desktop computer.

I. "Data Security Plan" is a component of the Agreement, found as Attachment A, which specifies computer and data security requirements and procedures which must be implemented and adhered to for use of the Confidential Data in order to keep the Confidential Data secure.

J. "Deductive Disclosure" is the discerning of an individual's identity or confidential information through the use of known characteristics of that individual. Disclosure risk is present if an unacceptably narrow estimation of an individual's confidential information is possible or if determining the exact attributes of the individual is possible with a high level of confidence.

K. “Derivative” is a file or statistic derived from the Confidential Data that poses disclosure risk to any Private Person in the Confidential Data obtained through this Agreement. Derivatives include copies of the Confidential Data received from NAHDAP/ICPSR, subsets of the Confidential Data, and analysis results that do not conform to the guidelines in Section VI.G.

II. Description of Disclosure Risk Section

Deductive disclosure of an individual's identity from research data is a major concern of federal agencies, researchers, and Institutional Review Boards. If a person is known to have participated in ANY survey or study or whose information is known to be included in a database from which the Confidential Data were obtained, then a combination of his or her personal characteristics may allow someone to determine which record corresponds to that individual. Investigators and Institutions who receive any portion of Confidential Data are obligated to protect the individual’s confidential information from deductive disclosure risk by strictly adhering to the obligations set forth in this Agreement and otherwise taking precautions to protect the Confidential Data from non-authorized use.

III. Requirements of Investigator

A. The Investigator assumes the responsibility of completing the online access request and providing required documents, reports, and amendments.

B. The Investigator agrees to responsibly manage and use Confidential Data, implement all Confidential Data security procedures per the Data Security Plan, and ensure that all VDE Users understand their requirements per this Agreement and follow the Data Security Plan.

C. Investigator must demonstrate experience with using Confidential Data by providing information that summarizes their recent/relevant research, including references. An Investigator with no prior experience using Confidential Data should reference the research of the Sponsor that he or she has participated in if this activity is germane to show an understanding of how to use Confidential Data or provide recent/relevant research of the Sponsor who has demonstrated experience.

IV. Requirements of Institution

The Institution must meet the following criteria:

A. Be an institution of higher education; a research organization; a research arm of a government agency; a nongovernmental, not for profit, agency; a for-profit organization including a small business or for-profit organization other than small business; an Independent School District; a Public Housing Authority/Indian Housing Authority; a Native American Tribal Organization (other than a Federally recognized tribal government); a Faith-based or Community-based Organization; a Regional Organization; or a Non-domestic (non-U.S.) Entity (Foreign Institution).

B. The institution must not be currently debarred from receiving Confidential Data

V. Obligations of NAHDAP/ICPSR

In consideration of the promises made in Section VI of this Agreement, NAHDAP/ICPSR agrees to:

A. Provide the Confidential Data requested by the Investigator in the list of data files requested in the approved application within a reasonable time of execution of this Agreement by appropriate NAHDAP/ICPSR officials and to make the Confidential Data available to Investigator via the ICPSR Virtual Data Enclave (VDE). NAHDAP/ICPSR will provide instructions for user accounts and VDE access procedures within a reasonable amount of time after the execution of the Agreement.

B. Provide electronic documentation of the origins, form, and general content of the Confidential Data in the same time period and manner as the Confidential Data.

C. Provide telephone and/or email consultation to the VDE Users, to the extent that NAHDAP/ICPSR is able to respond to such inquiries.

NAHDAP/ICPSR MAKES NO REPRESENTATIONS NOR EXTENDS ANY WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED. THERE ARE NO EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE USE OF THE CONFIDENTIAL DATA WILL NOT INFRINGE ANY PATENT, COPYRIGHT, TRADEMARK, OR OTHER PROPRIETARY RIGHTS. Unless prohibited by law, Institution and Investigator assume all liability for claims for damages against them by third parties that may arise from the use or disclosure of the Confidential Data.

VI. Obligations of the Investigator, VDE Users, and Institution

Confidential Data provided under this Agreement shall be held by the Investigator, VDE Users, and Institution in strictest confidence and can be disclosed only in compliance with the terms of this Agreement. In consideration of the promises in Section V of this Agreement, and for use of Confidential Data from NAHDAP/ICPSR, the Institution, on behalf of the Investigator and VDE Users, agrees:

A. That the Confidential Data will be used solely for research or statistical purposes relative to the research project identified in the online application to obtain confidential data incorporated into this Agreement, and for no other purpose whatsoever without the prior consent of NAHDAP/ICPSR. Further, no attempt will be made to identify private persons, no Confidential Data of private person(s) will be published or otherwise distributed, and Confidential Data will be protected against deductive disclosure risk by strictly adhering to the obligations set forth in this Agreement and otherwise taking precautions to protect the Confidential Data from non-authorized use.

B. To supply NAHDAP/ICPSR with a completed online application to obtain access to the Confidential Data that will include the following:

1. Signed Restricted Data Use Agreement (this Agreement)
2. Information about the project and why the Confidential Data are needed
3. Investigator's contact information
4. List of data files requested
5. A copy of an Institutional Review Board (IRB) document approving or exempting the research project.
6. Information about the VDE Users and contact information
7. Data Security Plan (Attachment A to this Agreement and incorporated herein)
8. Curriculum Vitae (CV), résumé, or National Institutes of Health biosketch for each VDE User

C. To comply fully with the Data Security Plan at all times relevant to this Agreement.

D. That no persons other than those identified in this Agreement or in subsequent amendments to this Agreement, as VDE Users and who have executed this Agreement, be permitted access to the contents of Confidential Data files or any files derived from Confidential Data files.

E. That within one (1) business day of becoming aware of any unauthorized access, use, or disclosure of Confidential Data, or access, use, or disclosure of Confidential Data that is inconsistent with the terms and conditions of this Agreement, the unauthorized or inconsistent access, use, or disclosure of Confidential Data will be reported in writing to NAHDAP/ICPSR.

F. That, unless prior specific approval is received from NAHDAP/ICPSR, no attempt under any circumstances will be made to link the Confidential Data to any individual, whether living or deceased, or with any other dataset, including other datasets provided by NAHDAP/ICPSR.

G. To avoid inadvertent disclosure of private persons by being knowledgeable about what factors constitute disclosure risk and by using disclosure risk guidelines, such as but not limited to, the following guidelines[1] in the release of statistics or other content derived from the Confidential Data.[2]
   1. No release of a sample unique for which only one record in the Confidential Data obtained through sampling (e.g., not a census) provides a certain combination of values from key variables. For example, in no table should all cases in any row or column be found in a single cell.

---

[1] For more information, see the U.S. Bureau of the Census checklist. *Supporting Document Checklist on Disclosure Potential of Data, at* www.**census**.gov/srd/sdc/S14-1_v1.3_**Checklist**.doc; *NCHS Disclosure Potential Checklist* at http://www.cdc.gov/nchs/data/NCHS%20Micro-Data%20Release%20Policy%204-02A.pdf; and *FCSM Statistical Policy Working Paper 22 (Second Version, 2005)* at http://www.fcsm.gov/working-papers/SPWP22_rev.pdf.

[2] VI.G. can be customized with disclosure rules specific to the Confidential Data covered by the RDUA. Customized rules will be provided to the VDE Users.

2. No release of a sample rare for which only a small number of records (e.g., 3, 5, or 10 depending on sample characteristics) in the Confidential Data provide a certain combination of values from key variables. For example, in no instance should the cell frequency of a cross-tabulation, a total for a row or column of a cross-tabulation, or a quantity figure be fewer than the appropriate threshold as determined from the sample characteristics. In general, assess empty cells and full cells for disclosure risk stemming from sampled records of a defined group reporting the same characteristics.
3. No release of a population unique for which only one record in the Confidential Data that represents the entire population (e.g., from a census) provides a certain combination of values from key variables. For example, in no table should all cases in any row or column be found in a single cell.
4. No release of the statistic if the total, mean, or average is based on fewer cases than the appropriate threshold as determined from the sample characteristics.
5. No release of the statistic if the contribution of a few observations dominates the estimate of a particular cell. For example, in no instance should the quantity figures be released if one case contributes more than 60 percent of the quantity amount.
6. No release of data that permits disclosure when used in combination with other known data. For example, unique values or counts below the appropriate threshold for key variables in the Confidential Data that are continuous and link to other data from NAHDAP/ICPSR or elsewhere.
7. No release of minimum and maximum values of identifiable characteristics (e.g., income, age, household size, etc.) or reporting of values in the "tails," e.g., the 5^{th} or 95^{th} percentile, from a variable(s) representing highly skewed populations.
8. Release only weighted results if specified in the data documentation.
9. No release of ANOVAs and regression equations when the analytic model that includes categorical covariates is saturated or nearly saturated. In general, variables in analytic models should conform to disclosure rules for descriptive statistics (e.g., see #7 above) and appropriate weights should be applied.
10. In no instance should data on an identifiable case, or any of the kinds of data listed in preceding items 1-9, be derivable through subtraction or other calculation from the combination of tables released.
11. No release of sample population information or characteristics in greater detail than released or published by the researchers who collected the Confidential Data. This includes but is not limited to publication of maps.
12. No release of anecdotal information about a specific private person(s) or case study without prior approval.
13. The above guidelines also apply to charts as they are graphical representations of cross-tabulations. In addition, graphical outputs (e.g., scatterplots, box plots, plots of residuals) should adhere to the above guidelines.

H. That if the identity of any private person should be discovered, then:

1. No use will be made of this knowledge;

2. NAHDAP/ICPSR will be advised of the incident within five (5) business days of discovery of the incident;
3. The information that would identify the private person will be safeguarded or destroyed as requested by NAHDAP/ICPSR; and
4. No one else will be informed of the discovered identity.

I. Unless other provisions have been made with NAHDAP/ICPSR, all access will be terminated to the Confidential Data on or before completion of this Agreement or within 5 days of written notification from NAHDAP/ICPSR. Investigators requiring the Confidential Data beyond the completion of this Agreement should submit a request for continuation three months prior to the end date of the Agreement.

J. To ensure that the Confidential Data are managed and used only in compliance with the terms and conditions of this Agreement and with all applicable statutes and regulations. Noncompliance with this Agreement by any VDE Users hereto shall be deemed noncompliance and a breach by Investigator and Institution for purposes of Section VII below.

K. That any books, articles, conference papers, theses, dissertations, reports, or other publications that employed the Confidential Data or other resources provided by NAHDAP/ICPSR reference the bibliographic citation provided by NAHDAP/ICPSR.

L. To provide at the end of the Agreement period to NAHDP/ICPSR staff:
1. A listing of public presentations at professional meetings using results based on the Confidential Data or derivatives or analyses thereof;
2. A listing of papers accepted for publication using the Confidential Data, or derivatives or analyses thereof, with complete citations;
3. A listing of VDE Users using the Confidential Data, or derivatives or analyses thereof, for dissertations or theses, the titles of these papers, and the date of completion.

M. To notify NAHDAP/ICPSR of a change in institutional affiliation of the Investigator, a change in institutional affiliation of any VDE User, or the addition or removal of a VDE User on the research project and need to access the Confidential Data. Notification must be in writing and must be received by NAHDAP/ICPSR at least six (6) weeks prior to the last day of employment with Institution or as soon as possible for a change in membership on the research project. Investigator's separation from Institution terminates this Agreement.

N. To respond fully and in writing within ten (10) working days after receipt of any written inquiry from NAHDAP/ICPSR regarding compliance with this Agreement .

VII. Violations of this Agreement

A. In the event Investigator, VDE Users, or Institution breaches any provision of this Agreement, Institution shall be responsible to promptly cure the breach and mitigate any damages. The Institution hereby acknowledges that any breach of the confidentiality provisions herein may

result in irreparable harm to NAHDAP/ICPSR and the National Institute on Drug Abuse not adequately compensable by money damages. Institution hereby acknowledges the possibility of injunctive relief in the event of breach, in addition to any other remedies at law or in equity. In addition, NAHDAP/ICPSR may:

1. Terminate this Agreement upon notice and remove access to the Confidential Data;
2. Deny Investigator future access to Confidential Data; and/or
3. Report the inappropriate use or disclosure to the Secretary of Health and Human Services.

B. Institution agrees, to the extent permitted under the law, to indemnify, defend, and hold harmless The University of Michigan, NAHDAP/ICPSR, and the sources of Confidential Data from any or all claims and losses accruing to any person, organization, or other legal entity as a result of Investigator's, VDE User's, and/or Institution's acts, omissions, or breaches of this Agreement.

VIII. Confidentiality

To the extent the Confidential Data are subject to a Certificate of Confidentiality, the Institution is considered to be a contractor or cooperating agency of NAHDAP/ICPSR and, as such, the Institution, the Investigator, and VDE Users are authorized to protect the privacy of the individuals who are the subjects of the Confidential Data by withholding their identifying characteristics from all persons not connected with the conduct of the Investigator's research project. "Identifying characteristics" are considered to include those data defined as confidential under the terms of this Agreement.

IX. Incorporation by Reference

All parties agree that the following documents are incorporated into this Agreement by reference:

A. The application information entered in the online application system.

B. A copy of the Institution's IRB approval or exemption of the research project.

C. The Data Security Plan.

X. Miscellaneous

A. All notices and contractual correspondence under this Agreement on behalf of the Investigator shall be made in writing and delivered to the address below:

National Addiction and HIV Data Archive Program
ICPSR
P.O. Box 1248
Ann Arbor, MI 48106-1248
nahdap@icpsr.umich.edu

B. This agreement shall be effective for 24 months from execution, unless earlier terminated per section VII herein.

C. The respective rights and obligations of NAHDAP/ICPSR and Investigator, VDE Users, and Institution pursuant to this Agreement shall survive termination of the Agreement.

D. This Agreement, the Investigator's research project, and the Data Security Plan may be amended or modified only by the mutual written consent of the authorized representatives of NAHDAP/ICPSR and Investigator and Institution. Both parties agree to amend this Agreement to the extent necessary to comply with the requirements of any applicable regulatory authority.

E. The persons signing this Agreement have the right and authority to execute this Agreement, and no further approvals are necessary to create a binding agreement.

F. The obligations of Investigator, VDE Users, and Institution set forth within this Agreement may not be assigned or otherwise transferred without the express written consent of NAHDAP/ICPSR.

Investigator and Institutional Signatures

Investigator or Sponsor (not student)	**Institutional Representative**
SIGNATURE DATE	SIGNATURE DATE
NAME TYPED OR PRINTED	NAME TYPED OR PRINTED
TITLE	TITLE
INSTITUTION	INSTITUTION
BUILDING ADDRESS	BUILDING ADDRESS
STREET ADDRESS	STREET ADDRESS
CITY, STATE ZIP	CITY, STATE ZIP

Attachment A: Data Security Plan

All of the following computer and data security requirements and procedures are required to be implemented and followed by all VDE Users as part of this Agreement:

- You must password protect the computer that is used to access the Confidential Data.
- You must set the computer to activate a password protected screen saver after three minutes of inactivity.
- Under no circumstances may you share or give your login and password to the VDE to anyone, and this includes not sharing them with other members of your research project team not listed as a VDE User on the Agreement or your organization's information and technology (IT) staff. Passwords must not be stored on a computer in electronic or written form. Software password storage programs may not be used.
- Since the Confidential Data are administered by ICPSR, University of Michigan you should not contact the IT staff at your organization with questions about the Confidential Data. (You may contact your organization's IT staff if you need help installing the VDE client software to access the Confidential Data. Your organization's IT staff should never be allowed to access any Confidential Data.)
- You must only use the Confidential Data on a computer in a Secure Project Office, for which
    - the computer or monitor screen is not visible from the doorway or windows
    - the office door is closed when a VDE User is logged into the VDE
    - only VDE Users approved to work with the Confidential Data are in the office when a VDE User is logged into the VDE
- You will close and lock the Secure Project Office when access to the Confidential Data is active but you and any other VDE User is out of the office.
- You will not allow under any circumstances any unauthorized person to access or view the Confidential Data.
- You will not allow any unauthorized persons to be inside the Secure Project Office when any VDE User is logged into the VDE.
- You must not allow the computer monitor to display Confidential Data content to any unauthorized person. The computer monitor display screen must not be visible from open doors or through windows.
- If you are logged into the VDE and you leave your computer, you must "disconnect" or "logoff" from the VDE. (Disconnecting from the VDE will leave any open programs running, but closes the connection to the VDE. Logging off of the VDE closes the connection and terminates all programs that are running.)
- You will keep all Confidential Data and derivatives within the VDE:
    - You must not duplicate or copy the data (e.g., you must not retype and/or use non-technical ways of copying the data, such as handwritten notes).
    - You must not take screenshots, photographs, or videos of the displayed Confidential Data or statistical outputs.

  - You must not type or record the Confidential Data or results from the data onto your office or personal computer or onto some other device or media.

- You must protect all hardcopy documents related to the Confidential Data such as research notes. Such hardcopy documents must be kept in locked drawers or cabinets in the Secure Project Office when not in use.
- Prior to a disclosure review and approval by ICPSR, neither you nor any VDE User may talk about or discuss any Confidential Data or results from the Confidential Data in non-secure or public locations. These discussions cannot occur where an unauthorized person could eavesdrop.
- You must submit all statistical outputs/results/notes from the Confidential Data to ICPSR for a disclosure review prior to sharing or giving such outputs to unauthorized persons. You also agree to revise or alter such files as required by ICPSR in order to minimize disclosure risk prior to ICPSR approving these files for sharing with unauthorized persons.
- You may only share aggregated information from the Confidential Data to unauthorized persons after you obtain clearance to do so through the ICPSR disclosure review process.