

**Restricted Data Use Agreement
for Restricted Data in the Virtual Data Enclave (VDE)
from the Inter-university Consortium
for Political and Social Research (ICPSR)**

I. Definitions

“**Agreement**” means this Restricted Data Use Agreement by and among The Regents of the University of Michigan, on behalf of ICPSR on the one hand, and Investigator and Institution identified on the signature page hereof on the other hand, dated and effective as of the date on which the last signatory hereto signs below.

“**Confidentiality Pledge (VDE User)**” means the promise and agreement of each VDE User to maintain the confidentiality of all Restricted Data made available to such VDE User under the terms of this Agreement, which pledge appears on the VDE login screen and must be accepted by such VDE User in order to gain access to the Restricted Data. The Confidentiality Pledge (VDE User) may be amended or modified by ICPSR from time to time.

“**Data Security Plan**” means the permissible computer configurations for use of Restricted Data and the procedures and protocols Investigator and Research Staff commit to use in order to keep Restricted Data secure as set forth in Attachment A.

“**Deductive Disclosure**” is the discerning of a Private Person's identity or confidential information through the use of characteristics about that Private Person contained in the Restricted Data. Disclosure risk is present if an unacceptably narrow estimation of a Private Person's confidential information is possible or if determining the exact attributes of the Private Person is possible with a high level of confidence.

“**Derivative**” is a file or statistic derived from the Restricted Data that poses disclosure risk to any Private Person identified or identifiable in the Restricted Data obtained through this Agreement. Derivatives include copies of the Restricted Data provided through ICPSR's VDE, subsets of the Restricted Data, and analysis results that do not conform to the guidelines in Section VI.G.

“**ICPSR**” means the Inter-university Consortium for Political and Social Research and a center of The University of Michigan, and for Restricted Data under this Restricted Data Use Agreement, the data steward contracted by MCC.

“**Institution**” is the organization at which Investigator and Research Staff will conduct research using Restricted Data obtained through this Agreement.

“**Investigator**” is the person primarily responsible for conducting the research or statistical activities relative to the research description section of the Online Application or supervising the Research Staff conducting the research or statistical activities relative to the research description section of the Online Application, for which Restricted Data are obtained through this Agreement.

“**MCC**” means the Millennium Challenge Corporation, a United States government agency that makes foreign assistance grants to finance poverty-reducing and economic growth generating projects in some of the poorest countries of the world. For Restricted Data under this Restricted Data Use Agreement, MCC is the original data provider and sponsor.

“**Online Application**” means all information provided through the ICPSR web-based data access request system, including: (i) the name, contact information, and CV/Resume/Biosketch for each person (Investigator and Research Staff) that will access the Restricted Data, (ii) data selection specifying which files are requested, (iii) a research proposal describing the need for the data and how it will be used, (iv) documentation of Institutional Review Board approval or exemption of the research proposal, and (v) a signed Restricted Data Use Agreement.

“**Online Access**” means the process Investigator and Research Staff must follow to gain access to the VDE following approval of the Online Application, including: (i) completing the ICPSR VDE training video and quiz, (ii) obtaining VDE licenses for each approved person that will access the Restricted Data by assigning licenses within the ICPSR web-based data access request system after the Online Application has been approved, (iii) providing ICPSR with the information needed to create VDE user accounts, and (iv) installing the necessary VDE and two-factor authentication software.

“**Private Person**” means any individual (including an individual acting in an official capacity) and any private (i.e., non-government) partnership, corporation, association, organization, community, tribe, or entity (or any combination thereof), including family, household, school, neighborhood, health service, or institution from which the Restricted Data arise or were derived, or which is related to a Private Person from which the Restricted Data arise or were derived.

“**Representative of Institution**” is a person authorized to enter into binding legal agreements on behalf of Investigator's Institution.

“**Research Staff**” means all persons at Investigator's Institution, who will have access to Restricted Data obtained through this Agreement, including students, other faculty and researchers, staff, agents, or employees for whom Institution accepts responsibility.

“**Restricted Data**” means the research dataset(s) provided under this Agreement that include potentially identifiable information in the form of indirect identifiers that if used together within the dataset(s) or linked to other dataset(s) could lead to the re-identification of a specific Private Person, as well as information provided by a Private Person under the expectation that the information would be kept confidential and would not lead to harm to the Private Person. Restricted Data includes any Derivatives.

“**Secure Project Office**” means the secure office from which any VDE User will use the Restricted Data. Only other VDE Users who have been granted access to Restricted Data under this Agreement may be inside the Secure Project Office while a VDE User is using the Restricted Data. The Secure Project Office door must remain closed while the VDE User is using the Restricted Data and locked when the VDE User is not in the Secure Project Office but use of the Restricted

Data is active. The computer screen may not be visible from any doorways or windows. Each VDE User may have a different Secure Project Office.

“VDE” is the Virtual Data Enclave, which permits monitored access to Restricted Data that are not available to the general public. The VDE is isolated from the user's physical desktop computer, restricting the user from downloading files or parts of files to their physical computer. The VDE is also restricted in its external access, preventing users from emailing, copying, or otherwise moving files outside of the secure environment, either accidentally or intentionally.

“VDE User” means any of Investigator or any Research Staff who is granted access to Restricted Data under this Agreement.

“VDE User PII” means any and all personally identifiable information of any VDE User collected by ICPSR as part of or in connection with the Online Application or ICPSR’s monitoring of the VDE User’s utilization of the VDE.

II. Responsibility to Address Disclosure Risk

Deductive Disclosure of a Private Person's identity from research data is a major concern of federal agencies, researchers, and Institutional Review Boards. Investigator, Research Staff, and Institution are obligated to protect the Restricted Data from Deductive Disclosure risk, non-authorized use, and attempts to identify any Private Person by strictly adhering to the obligations set forth in this Agreement.

III. Requirements of Investigator

- A. Investigator assumes the responsibility of completing the Online Application and satisfying the requirements for Online Access, and providing any other required documents, reports, or amendments.
- B. Investigator agrees to manage and use Restricted Data in accordance with the Confidentiality Pledge (VDE User), implement all Restricted Data security procedures per the Data Security Plan, and ensure that all Research Staff understand their obligations under this Agreement (including the Data Security Plan) and the Confidentiality Pledge (VDE User).
- C. Investigator must demonstrate experience with using information of a sensitive, confidential, or private nature by providing information in the Online Application that summarizes their recent or relevant research, including references. If Investigator has no prior experience using information of a sensitive, confidential, or private nature, the Online Application should (i) reference the research of the sponsor that he or she has participated in if such activity is germane to show an understanding of how to use sensitive, confidential, or private information or (ii) provide recent or relevant research of the sponsor who has demonstrated experience.

IV. Requirements of Institution

Institution represents that:

- A. It is 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, 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-U.S. or foreign entity.
- B. It is not currently debarred or otherwise restricted in any manner from receiving information of a sensitive, confidential, or private nature under any applicable laws, regulations, or policies.
- C. It has a demonstrated record of using sensitive data according to commonly accepted standards of research ethics and applicable statutory requirements.
- D. To the extent permitted by law, it is liable for all actions or omissions of Institution, Investigator, and any Research Staff related to this Agreement or as a result of any access that may be granted to the VDE or the Restricted Data to Institution, Investigator, or any Research Staff.
- E. The Representative of Institution signing this Agreement has the right and authority to execute this Agreement on behalf of Institution and no further approvals are necessary to create a binding agreement.

V. Obligations of ICPSR

In consideration of the promises made in Section VI of this Agreement, and upon receipt of a complete and approved Online Application, ICPSR agrees to:

- A. Provide instructions to Investigator and Research Staff for completing the VDE training video and quiz, establishing VDE user accounts, assigning VDE user licenses, installing the software required for VDE access, and navigating the VDE within a reasonable amount of time after the execution of this Agreement. This will support establishing access to the VDE which requires proper authentication, including VDE user account login and password, and two-factor authentication.
- B. Provide the Restricted Data requested by Investigator in the Online Application within a reasonable time of execution of this Agreement by Institution and to make the Restricted Data available to Investigator and Research Staff via the VDE, a secure remote-access work space.
- C. Provide electronic documentation of the origins, form, and general content of the Restricted Data sent to Investigator, in the same time period and manner as the Restricted Data.
- D. Maintain the confidentiality of all VDE User PII in accordance with the ICPSR Privacy Policy and (i) maintain such VDE User PII securely, taking reasonable precautions to protect it to the

extent permitted by applicable law and (ii) not disclose, give, sell, or transfer any VDE User PII, unless required for law enforcement or by statute, or upon mutual agreement between and ICPSR and the applicable VDE User.

- E. Protect privacy information in accordance with the Privacy Act of 1974 (5 USC § 552a), the MCC Privacy Policy and related policies. Sensitive personal identifiable information can include, but is not limited to, social security numbers; health records or medical records; employment history; financial data; biometric data (including, but not limited to facial geometry, fingerprint, iris scan, or DNA); criminal history; name and mother's maiden name; driver's license number; or date and place of birth. ICPSR, as an MCC contractor, may disclose privacy information only in accordance with the routine uses described in the applicable System of Records Notice or as otherwise specifically permitted under 5 USC § 552a(b) of the Privacy Act. No information about an individual may be released except when pursuant to a written request by, or with written consent from, the individual to whom the information pertains (unless disclosure of this information would be for the purpose specified in United States Code (USC) – 5 USC § 552a). Submission of any information is voluntary.
- F. Use VDE User PII for the purposes set forth in the ICPSR Privacy Policy, including but not limited to: (i) to track data and documentation downloads for aggregated reporting purposes, (ii) to contact VDE Users for annual updates to MyData account information, (iii) to contact VDE Users regarding any changes to ICPSR access or confidentiality policies, and (iv) to contact VDE Users regarding any issues with accessed data. For the avoidance of doubt, the parties acknowledge and agree that ICPSR may retain all VDE User PII for these limited purposes indefinitely.

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 RESTRICTED DATA WILL NOT INFRINGE ANY PATENT, COPYRIGHT, TRADEMARK, OR OTHER PROPRIETARY RIGHTS.

VI. Obligations of Investigator, Research Staff, and Institution

Restricted Data access provided under this Agreement will be used or 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 Restricted Data from ICPSR, Institution agrees (on behalf of itself, Investigator and all Research Staff):

- A. That the Restricted Data will be used solely for statistical analysis and reporting of aggregated information relative to the project as identified in research description section of the Online Application, and for no other purpose whatsoever without the prior written consent of ICPSR. Further, no attempt will be made to identify Private Person(s), no Restricted Data of Private Person(s) will be published or otherwise distributed, the Restricted Data will be protected against Deductive Disclosure risk by strictly adhering to the obligations set forth in this

Agreement, and precautions will be taken to protect the Restricted Data from non-authorized use.

- B. With respect to the Restricted Data, to comply fully with all data security procedures set forth in the Data Security Plan.
- C. That no persons other than those identified in this Agreement or in subsequent amendments to this Agreement, as Investigator or Research Staff be permitted access to the contents of Restricted Data files or any Derivatives from the Restricted Data.
- D. That upon written request from ICPSR, Investigator and all Research Staff will provide proof of current training or certification in the protection of human subjects that aligns with current policies of Institution or the United States Policy or applicable regulation for Protection of Human Subjects.
- E. That within five (5) business days of becoming aware of any unauthorized access, use, or disclosure of Restricted Data, or access, use, or disclosure of Restricted Data that is inconsistent with the terms and conditions of this Agreement, the unauthorized or inconsistent access, use, or disclosure of Restricted Data will be reported in writing to ICPSR.
- F. That, unless prior specific, written approval is received from ICPSR, no attempt under any circumstances will be made to link the Restricted Data to any Private Person, whether living or deceased, or with any other dataset, including other datasets provided by ICPSR.
- G. To avoid inadvertent disclosure of the identity of Private Persons or their related Restricted Data by being knowledgeable about the factors that constitute disclosure risk and by using disclosure risk guidelines, such as but not limited to, the following guidelines¹ in the release of statistics or other content derived from the Restricted Data:²
 - 1. No release of a sample or sub-sample unique for which only one record in the Restricted Data provides a certain combination of values from key variables.
 - 2. No release of a sample statistic for which only a small number of records (e.g., 3, 5, or 10 depending on sample characteristics) in the Restricted 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 the statistic if the total, mean, or average is based on fewer cases than the appropriate threshold as determined from the sample characteristics.

¹ For more information, see the National Center for Health Statistics checklist, *NCHS Disclosure Potential Checklist* at http://www.cdc.gov/nchs/data/nchs_microdata_release_policy_4-02A.pdf; and *FCSM Statistical Policy Working Paper 22 (Second Version, 2005)* at <http://www.hhs.gov/sites/default/files/spwp22.pdf>.

² If disclosure review rules were established for a specific Restricted Dataset, they will be included in the dataset's documentation and are covered by this Agreement.

4. 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.
 5. 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 Restricted Data that are continuous and link to other data from ICPSR or elsewhere.
 6. 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 5th or 95th percentile, from a variable(s) representing highly skewed populations.
 7. 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 #6 above).
 8. In no instance should data on an identifiable case, or any of the kinds of data listed in preceding items 1-7, be derivable through subtraction or other calculation from the combination of tables released.
 9. No release of sample population information or characteristics in greater detail than released or published by the researchers who collected the Restricted Data. This includes but is not limited to publication of maps.
 10. No release of anecdotal information about a specific Private Person(s) or case study without prior written approval.
 11. The above guidelines also apply to charts and any other graphical representations that could reveal the prohibited statistics listed above.
- H. That if the identity of any Private Person should be discovered, then:
1. No use will be made of this knowledge;
 2. 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 ICPSR; and
 4. No one else will be informed of the discovered identity.
- I. Unless other provisions have been made with ICPSR, all access to the Restricted Data will be terminated on or before completion of this Agreement or within five (5) days of written notice from ICPSR. Investigators requiring access to the Restricted Data beyond completion of this Agreement should submit a request for continuation three (3) months prior to the end date of this Agreement.
- J. That any books, articles, conference papers, theses, dissertations, reports, or other publications that employed the Restricted Data or other resources provided by ICPSR reference the bibliographic citation provided by ICPSR and be reported to ICPSR for inclusion in its data-related bibliography.
- K. To provide reports to ICPSR staff upon written request from ICPSR (through ICPSR’s online data access request system), which include:

1. A copy of the annual IRB approval for the project described in the research description section of the Online Application;
 2. A listing of public presentations at professional meetings using results based on the Restricted Data or Derivatives or analyses thereof;
 3. A listing of papers accepted for publication using the Restricted Data, or Derivatives or analyses thereof, with complete citations;
 4. A listing of Research Staff using the Restricted Data, or Derivatives or analyses thereof, for dissertations or theses, the titles of these papers, and the date of completion; and
 5. Update on any change in scope of the project as described in the research description portion of the Online Application.
- L. To notify ICPSR of a change in institutional affiliation of Investigator, a change in institutional affiliation of any Research Staff, or the addition or removal of Research Staff on the research project. Notification with respect to a change in institutional affiliation must be in writing and must be received by ICPSR at least six (6) weeks prior to the last day of employment or enrollment with Institution, or as soon as reasonably possible. Notification of the addition or removal of Research Staff on the research project must be provided to ICPSR as soon as reasonably possible. Investigator's separation from Institution immediately terminates this Agreement and access to the Restricted Data.
- M. After separating from Institution, Investigator may reapply for access to Restricted Data as an employee of a new institution. In addition to the other components of the Online Application, re-application requires: (1) Execution of a new Restricted Data Use Agreement by both Investigator and the proposed new institution; and (2) Evidence of approval or exemption by the proposed new institution's IRB of the project identified in the research description section of the Online Application.

These materials must be approved by ICPSR before Restricted Data or any derivatives or analyses may be accessed at the new institution.

- N. That if Investigator separates from Institution and does not have a new Restricted Data Use Agreement executed by the time they leave Institution, ICPSR will temporarily deactivate Investigator's account but will maintain Investigator's profile to save their work during the transition. Upon approval of the new online application, ICPSR will reactivate Investigator's account. If a new Restricted Data Use Agreement is not executed within three (3) months, Investigator's account will be deleted.
- O. That use of the Restricted Data will be consistent with Institution's applicable policies and practices regarding scientific integrity and human subjects research so long as such policies and practices are consistent and do not conflict with the terms of this Agreement.
- P. To respond fully and in writing within ten (10) working days after receipt of any written inquiry from ICPSR regarding compliance with this Agreement.

VII. Violations of this Agreement

- A. Institution will investigate allegations by ICPSR or other parties of violations of this Agreement in accordance with its policies and procedures on scientific integrity and misconduct. If the allegations are confirmed, Institution will treat the violations as it would violations of the explicit terms of its policies on scientific integrity and misconduct.
- B. In the event of a breach of any provision of this Agreement by Institution, Investigator, or any Research Staff, Institution will be fully responsible for the same and will promptly cure the breach and mitigate any damages. Institution hereby acknowledges that any breach of the provisions of this Agreement by Institution, Investigator, or any Research Staff will result in irreparable harm to ICPSR that are not adequately compensable by money damages. Institution hereby agrees that ICPSR will be entitled to injunctive relief in the event of any breach of this Agreement, in addition to money damages. In addition, in the event of any breach of the terms of this Agreement by Institution, Investigator, or any Research Staff, ICPSR may, in its sole and absolute discretion:
1. Terminate this Agreement upon notice and/or immediately remove Institution's, Investigator's, and/or any Research Staff's access to Restricted Data and any derivatives thereof;
 2. Deny Institution, Investigator, and any Research Staff future access to Restricted Data;
 3. Report the inappropriate use or disclosure (including, but not limited to, the circumstances that led to the breach and any and all other information that ICPSR may deem advisable or necessary to report) by Institution, Investigator, or any Research Staff to Institution's IRB and/or the appropriate federal and private agencies or foundations that fund or regulate biomedical, behavioral, scientific and/or public policy research; and/or
 4. Pursue such other remedies that may be available to ICPSR under law or equity, including injunctive relief.
- C. Institution agrees, to the extent not prohibited under applicable law, to indemnify the Regents of the University of Michigan from any or all claims, losses, causes of action, judgments, damages, and expenses arising from Investigator's, Research Staff's, and/or Institution's use of the Restricted Data, except to the extent and in proportion such liability or damages arose from the negligence of the Regents of the University of Michigan. Nothing herein will be construed as a waiver of any immunities and protections available to Institution under applicable law.
- D. In the event of a violation of this Agreement, Investigator must:
1. Notify ICPSR within five (5) business days;
 2. Stop work with the Restricted Data immediately;
 3. Submit a notarized affidavit acknowledging the violation to ICPSR;
 4. Inform the Representative of Institution of the violation and review security protocols and disclosure protections with them.
 - i. The Representative of Institution must submit an acknowledgment of the violation and

security protocols and disclosure protections review to ICPSR; and

5. Reapply for access to the Restricted Data.
- E. Investigator and Institution acknowledge and agree that each is executing this Agreement for the benefit of MCC, and that MCC is a third-party beneficiary of this Agreement who, in addition to any other rights it may have, has the right of direct action against each of Investigator and Institution for any breach of this Agreement (including to seek any of the remedies granted to ICPSR under Section VII), and the right to otherwise enforce this Agreement.

VIII. Certificates of Confidentiality

To the extent the Restricted Data are subject to a Certificate of Confidentiality (within the meaning of §301(d) of the Public Health Service Act (42 U.S.C. 241(d)), as amended), Institution is considered to be a contractor or cooperating agency of ICPSR; as such, Institution, Investigator, and Research Staff are authorized to protect the privacy of the individuals who are the subjects of the Restricted Data by withholding their identifying characteristics from all persons not connected with the conduct of 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 information provided as part of the Online Application is incorporated into this Agreement by reference.

X. Miscellaneous

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

ICPSR
P.O. Box 1248
Ann Arbor, MI 48106-1248
-or-
help@icpsr.umich.edu

B. This Agreement will be effective for 24 months from execution or until the IRB approval related to the research project identified in the research description section of the Online Application expires, whichever occurs first.

C. The respective rights and obligations of ICPSR and Investigator, Research Staff, and Institution pursuant to this Agreement will survive termination of this Agreement.

D. This Agreement and any of the information and materials provided as part of the Online Application may be amended or modified only by the mutual written consent of the authorized representatives of 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.

The obligations of Investigator, Research Staff, and Institution set forth within this Agreement may not be assigned or otherwise transferred without the express written consent of ICPSR.

**Investigator and Institutional
Signatures**

Read and Acknowledged by:

Investigator

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 POSTCODE, COUNTRY

CITY, STATE, POSTCODE, COUNTRY

Attachment A: VDE Data Security Plan

All the following computer and data security requirements and procedures are required to be implemented and followed by all individuals (Investigator and Research Staff) using the VDE as part of this Agreement, unless otherwise specified in writing by ICPSR:

1. You³ must password protect the computer that is used to access the Restricted Data.
2. You must set the computer to activate a password protected screen saver after three minutes of inactivity.
3. 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 or your organization's information and technology (IT) staff.
4. Passwords must not be stored on a computer in electronic or written form. Software password storage programs may not be used.
5. Since the Restricted Data are administered by ICPSR, University of Michigan you should not contact the IT staff at your organization with questions about the Restricted Data. (You may contact your organization's IT staff if you need help installing the VDE client software to access the Restricted Data. Your organization's IT staff should never be allowed to access any Restricted Data.)
6. You must only use the Restricted Data on a computer in a Secure Project Office, for which
 - a. the computer or monitor screen is not visible from the doorway or windows
 - b. the office door is closed when a VDE User is logged into the VDE
 - c. only VDE Users approved to work with the Restricted Data are in the office when a VDE User is logged into the VDE
7. You will close and lock the Secure Project Office when access to the Restricted Data is active but you and any other VDE User is out of the office.
8. You will not allow under any circumstances any unauthorized person to access or view the Restricted Data.
9. You will not allow any unauthorized persons to be inside the Secure Project Office when any VDE User is logged into the VDE.
10. You must not allow the computer monitor to display Restricted Data content to any unauthorized person. The computer monitor display screen must not be visible from open doors or through windows.
11. 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.)
12. You will keep all Restricted Data and derivatives within the VDE:

³ As used in this Attachment A, "you" refers to any VDE User.

- a. 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).
 - b. You must not take screenshots, photographs, or videos of the displayed Restricted Data or statistical outputs.
 - c. You must not type or record the Restricted Data or results from the data onto your office or personal computer or onto some other device or media.
13. You must protect all hardcopy documents related to the Restricted 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.
 14. Prior to a disclosure review and approval by ICPSR, neither you nor any VDE User may talk about or discuss any Restricted Data or results from the Restricted Data in non-secure or public locations. These discussions cannot occur where an unauthorized person could eavesdrop.
 15. You must submit all statistical outputs/results/notes from the Restricted 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.
 16. You may only share aggregated information from the Restricted Data to unauthorized persons after you obtain clearance to do so through the ICPSR disclosure review process.