Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice
Data Security Requirements for Accessing Restricted Data
OMB Control No. [1121-0377]

LIST OF ATTACHMENTS

Attachment A: Required Pre-Approval Documents

Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice
Data Security Requirements for Accessing Restricted Data:
Required Pre-Approval Documents

To gain access to BJS restricted microdata, applicants must apply for access through the standard application process (SAP) portal, ResearchDataGov. Applicants must complete all required fields in the application system. Additionally, applicants must complete all BJS data security requirements for accessing restricted data, which are described in two PDF documents that are available for download in the SAP:

- BJS Required Pre-Approval Documents
- BJS Required Post-Approval Documents

The **Required Pre-Approval Documents** must be completed and submitted before a conditional approval may be issued in the SAP. Following a conditional approval, applicants must complete all **Required Post-Approval Documents** before data access may be provided.

This document includes a summary of BJS's **Required Pre-Approval Documents**. Template documents are available starting on page 2.

Information about post-approval documents can be found in the **BJS Required Post-Approval Documents** PDF, downloadable as a separate PDF within the SAP.

Required Pre-Approval Documents:

BJS will collect some data security documentation related to confidentiality and privacy processes through the SAP to review an application for restricted microdata. Applicants must complete and upload the following required pre-approval documents through the SAP when an application for restricted data is submitted:

BJS Privacy Certificate – The Office of Justice Programs regulations at 28 C.F.R. Part 22 require that a Privacy Certificate be submitted as part of any application for a project in which information identifiable to a private person will be collected, analyzed, or otherwise used for research or statistical purposes. The Privacy Certificate describes the specific technical, administrative, and physical controls and procedures that will be used to protect data confidentiality and safeguard the data from misuse or unauthorized access. The Privacy Certificate is an applicant's certification to comply with BJS's confidentiality requirements. All individuals who will have access to the restricted BJS data are required to sign a Privacy Certificate to affirm their understanding of and agreement to comply with BJS's confidentiality requirements. See page 2 below for a clean copy of the BJS Privacy Certificate. A clean copy can also be found on the BJS website: https://bjs.ojp.gov/sites/g/files/xyckuh236/files/media/document/bjsmpc.pdf.

Institutional Review Board (IRB) documentation – Users of BJS restricted data must comply with Department of Justice regulations at 28 C.F.R. Part 46 (Protection of Human Subjects), including ensuring that adequate protections are in place to protect the confidentiality of information identifiable to a private person. Applicants must submit the appropriate documentation to demonstrate that an IRB has approved or exempted the proposed project using BJS restricted data. The documentation must specify that the project was reviewed in accordance with the requirements in 28 C.F.R. Part 46. Further information about BJS's requirements related to human subjects protections can be found on the BJS website: https://bjs.ojp.gov/funding/human-subjects-and-confidentiality-requirements. **Please append an IRB determination letter to the completed BJS Privacy Certificate when submitting an application through the SAP**.

BUREAU OF JUSTICE STATISTICS (BJS)
MODEL PRIVACY CERTIFICATE

U.S. Department of Justice regulations at 28 CFR §22.23 require that a Privacy Certificate be submitted as part of any application for a project in which information identifiable to a private person will be collected for research or statistical purposes. The following summarizes the requirements of 28 CFR Part 22 and may be used as a guide to complete the Privacy Certificate.

1. Data identifiable to a private person will not be used or revealed unless it is research or statistical information being used for research and statistical purposes.

2. Identifiable data will be used or revealed only on a need-to-know basis to (a) officers, employees, and subcontractors of the recipient of assistance; and (b) persons and organizations receiving transfers of information for research and statistical purposes only if an information transfer agreement is entered into in which the recipient is bound to use the information only for research and statistical purposes and to take adequate administrative and physical precautions to ensure the confidentiality of the information.

3. Employees with access to data on a need-to-know basis will be advised in writing of the confidentiality requirements and must agree in writing to abide by these requirements.

4. Subrecipients requiring access to identifiable data will only do so in accordance with an information transfer agreement which states that the confidentiality of the data must be maintained and that the information may only be used for research or statistical purposes.

5. Private persons from whom identifiable data are obtained or collected will be advised that the data will only be used for research and statistical purposes and that compliance with requests for information is not mandatory. That is, participation in the research is voluntary and may be withdrawn at any time. *Please note: If the notification requirement is to be waived, an explanation must be contained within or attached to the Privacy Certificate.*

6. Adequate precautions will be taken to ensure the administrative and physical security of the identifiable data.

7. A log indicating that identifiable data has been transferred to persons other than those in BJS or other OJP bureaus or to grantee, contractor, or subcontractor staff will be maintained and will indicate whether the data has been returned or if there is an alternative arrangement for the future maintenance of such data.

8. Project plans will be designed to preserve the anonymity of persons to whom the information relates, including where appropriate, name-stripping, coding of data, or other similar procedures.

9. Project findings and reports prepared for dissemination will not contain information which can reasonably be expected to be identifiable to a private person.

10. Upon completion of the project, the security of research or statistical information will be protected by either:

    a. the complete physical destruction of all copies of the materials or the identifiable portions of the materials after a three year required recipient retention period or as soon as authorized by law; or

    b. the removal of identifiers from the data and separate maintenance of a name-code index in a secure location. *Please note: If you choose to keep a name-code index, you must maintain procedures to secure such an index.*

PRIVACY CERTIFICATE

Organization Name:_____ Vendor Number: _____

Project Title: _____

Application Number: _____

I. Brief description of project:

II. Procedures to notify subjects, as required by 28 CFR §22.23(b)(4) or an explanation if notification is to be waived, pursuant to 28 CFR §22.27(c):

III. Procedures developed to preserve the anonymity of private persons to whom information relates, as required by 28 CFR §22.23(b)(7):

IV. Procedures for data collection and storage, as required by 28 CFR §22.23(b)(5):

V. Procedures for the final disposition of data, as required by 28 CFR §22.23(c) and §22.25:

VI. List of individuals having access to data, as required by 28 CFR 22.23(b)(2):

Principal Investigator(s)

_____

_____

Project staff

_____

_____

Information technology personnel

_____

_____

Subcontractors or consultants

_____

_____

Additional lines may be added, as needed. Staff signatures are required in the next section.

Grantee[1] certifies that --

- *data identifiable to a private person*[2] will not be used or revealed, except as authorized under 28 CFR Part 22, Sections 22.21 & 22.22.

- access to the data will be limited to those employees having a need for such data and that such employees shall be advised of and agree in writing to comply with the regulations in 28 CFR Part 22.

- all contractors, subcontractors, and consultants requiring access to identifiable data will agree, through conditions in their subcontract or consultant agreement, to comply with the requirements of 28 CFR §22.24 regarding information transfer agreements and that the Bureau of Justice Statistics (BJS) will be provided copies of all transfer agreements before they are executed as well as the name and title of the individuals with the authority to transfer data.

- if applicable, a log will be maintained indicating that (1) identifiable data have been transferred to persons other than employees of BJS and other Office of Justice Programs bureaus and offices, or grantee/contractor/subcontractor staff; and (2) such data have been returned or that alternative arrangements have been agreed upon for future maintenance of such data, in accordance with 28 CFR §22.23(b)(6).

- any private person from whom identifiable information is collected or obtained shall be notified, in accordance with 28 CFR §22.27, that such data will only be used or revealed for research or statistical purposes and that compliance with the request for information is not mandatory.

- project findings and reports prepared for dissemination will not contain information which can reasonably be expected to be identifiable to a private person, except as authorized by 28 CFR §22.22.

- adequate precautions will be taken to ensure administrative and physical security of identifiable data and to preserve the confidentiality of the personally identifiable information.

- all project personnel, including subcontractors, have been advised of and have agreed, in writing, to comply with all procedures to ensure the confidentiality of data identifiable to a private person.

- the procedures are accurately described above and will be adhered to by project staff, as well as subcontractors and BJS shall be notified of any material change in any of the information provided in this Privacy Certificate.

All project staff, including information technology personnel, subcontractors, and/or consultants, with access to BJS restricted data are required to sign this Privacy Certificate to affirm their understanding of and agreement to comply with the terms of access and privacy requirements.

The Principal Investigator (PI) is responsible for maintaining an updated staffing list of individuals with access to the restricted data. All individuals who are granted access to BJS restricted data during the project period are required to sign a Privacy Certificate. The PI must retain copies of all signed Privacy Certificates as an auditable requirement and must report staffing updates and provide copies of the certificates to the National Archive of Criminal Justice Data (NACJD) per their reporting requirements or upon request.

Signature(s):

Principal Investigator_____Date _____

Institutional Representative_____Date _____

Other project staff, including information technology personnel, subcontractors, and/or consultants, with access to identifiable data:

Name and title_____Date _____

Name and title_____Date _____

Name and title_____Date _____

Name and title_____Date _____

Name and title_____Date _____

Name and title_____Date _____

Additional signature lines may be added, as needed.

[1] The term “grantee” refers to the Principal Investigator and Institutional Representative.

[2] *Information identifiable to a private person* is defined in 28 CFR §22.2(e) as "Information which either (1) Is labelled by name or other personal identifiers, or (2) Can, by virtue of sample size or other factors, be reasonably interpreted as referring to a particular private person."

Updated for Standard Application Process use: February 09, 2023

Attachment B: Required Post-Approval Documents

Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice
Data Security Requirements for Accessing Restricted Data:
Required Post-Approval Documents

To gain access to BJS restricted microdata, applicants must apply for access through the standard application process (SAP) portal, ResearchDataGov. Applicants must complete all required fields in the application system. Additionally, applicants must complete all BJS data security requirements for accessing restricted data, which are described in two PDF documents that are available for download in the SAP:

- BJS Required Pre-Approval Documents
- BJS Required Post-Approval Documents

The **Required Pre-Approval Documents** must be completed and submitted before a conditional approval may be issued in the SAP. Following a conditional approval, applicants must complete all **Required Post-Approval Documents** before data access may be provided.

This document includes a summary of BJS's **Required Post-Approval Documents**. Template documents are available starting on page 3.

Information about pre-approval documents can be found in the **BJS Required Pre-Approval Documents** PDF, downloadable as a separate PDF within the SAP.

To expedite data access, applicants are encouraged to submit **Required Post-Approval Documents** at the time of the initial SAP application submission. However, if you do not wish to submit the **Required Post-Approval Documents** at the time of initial submission, please upload a blank/unfilled copy of this PDF to the SAP as a placeholder. If a conditional approval of your SAP application is issued, NACJD or BJS staff will then contact the applicant(s) to finalize any remaining requirements, which include completing all **Required Post-Approval Documents** described below, before gaining access to the restricted microdata.

Required Post-Approval Documents:

Applicants must complete additional requirements following a conditional approval before data access may be provided. A summary of the requirements is provided below.

NACJD Restricted Data Use Agreement – This document is an agreement between BJS's official archive (currently the National Archive of Criminal Justice Data [NACJD], located within the Inter-University Consortium for Political and Social Research [ICPSR] at the University of Michigan), or its successor, on behalf of BJS, and the user(s) who is approved to access BJS's restricted data assets exclusively for statistical purposes, including evidence-building, in accordance with the terms and conditions stated in the agreement and all applicable federal laws and regulations. An applicant must submit the appropriate data security plan information to describe how they will protect the data from misuse and unauthorized access. The agreement describes the penalties associated with the misuse or unauthorized access of the data. The agreement requires signature from the applicant(s) and any other representative who has the authority to enter into a legal agreement with NACJD, as applicable. See page 3 below for a clean copy of the NACJD Restricted Data Use Agreement.

ICPSR Data Security Plan – This document describes the data access modality (physical enclave, virtual enclave, or secure download) and the specific data security measures and technical, physical, and administrative controls that must be followed to protect data from unauthorized disclosure and misuse.

ICPSR supports three restricted data access modalities:

1. **Physical Data Enclave (PDE)**: The physical data enclave is located at ICPSR's offices in Ann Arbor, MI. Data sets in the physical enclave typically contain highly sensitive personal information or data from protected populations. To analyze data located in the PDE, researchers must travel to ICPSR. To receive output, researchers must request that ICPSR conduct a disclosure review on the desired files before removal from the PDE.
2. **Virtual Data Enclave (VDE)**: This method permits monitored access to data through a connection to a virtual machine. The virtual machine is isolated from the user's physical desktop computer, preventing the user from downloading files or parts of files to their physical computer. It is also restricted in its external access, preventing users from emailing, copying, or otherwise moving files outside of the secure environment. To remove output from the VDE, researchers must request that ICPSR conduct a disclosure review on the desired files.
3. **Secure Download (Requester Secure Site)**: Upon approval, researchers will receive a temporary link via email to an encrypted data file which they may then download to the secure location specified in their Data Security Plan. The researcher must destroy any copies of the data at the completion of their project and must certify in writing that all copies of the data have been destroyed.

The available access modality for a given dataset is determined by NACJD in consultation with BJS. If unsure whether the requested data may be accessed via PDE, VDE, or Secure Download, please review the "Access modality" listed on the "Data Access" tab from the ResearchDataGov data asset homepage or contact nacjd@umich.edu for assistance. For more information on ICPSR's restricted data access modalities, please visit the NACJD and ICPSR websites.

All researchers accessing BJS data via ICPSR's PDE must complete and submit the Physical Data Enclave Data Security Plan (Appendix A, page 14). All researchers accessing data made available via ICPSR's VDE must complete and submit the Virtual Data Enclave Data Security Plan (Appendix B, pages 15-16).

Data Security Plan options for Secure Download data include an encrypted external hard drive, a standalone computer, or a local or virtual enclave on an isolated network. Users of Secure Download (Requester Secure Site) data must select, complete, and submit one of the Secure Download Data Security Plan options (Appendices C-E, pages 17-22).

ICPSR Confidentiality Pledge – This document describes an applicant's responsibilities related to accessing restricted data and confidentiality protections that each applicant must uphold, including adhering to applicable federal laws and regulations. The assurance requires signature from the applicant(s) and certifies their understanding of and agreement to fulfill the terms in the data use agreement and data security plan. Included in Appendix F, page 23.

Certification of training – Users of BJS restricted data may be required to complete relevant data security, confidentiality, and/or privacy training when required by BJS, NACJD, or ICPSR. Failure to complete required training may result in a revocation of data access. All applicable training requirements will be communicated to applicant(s) by NACJD or BJS staff after a conditional approval has been issued in the SAP.

Restricted Data Use Agreement
for Restricted Data from
the Inter-university
Consortium
for Political and Social Research
(ICPSR)

I. Definitions

A. "Application" includes all information entered into the application system. This information may include Principal Investigator and Research Team information, Research Description, Data Selection specifying which files and documentation are requested, and all uploaded documentation.

B. "BJS" is the Bureau of Justice Statistics.

C. "Data Security Plan" is a component of the Agreement which specifies the precautions the Investigator and Research Team are required to take for use of Restricted Data and records what the Investigator and/or institution commits to do in order to keep Restricted Data secure.

D. "Deductive Disclosure" is the discerning of a Private Person's identity or confidential information through the use of characteristics about that Private Person 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.

E. "Derivative" is a file or statistic derived from the Restricted Data that poses disclosure risk to any Private Person in the Restricted Data accessed through this Agreement. Derivatives include copies of the Restricted Data received from ICPSR, subsets of the Restricted Data, and analysis results that do not conform to the guidelines in Section VI.F.

F. "ICPSR" is the Inter-university Consortium for Political and Social Research. For avoidance of doubt, ICPSR is not a party to this Agreement.

G. "Institution" is the organization at which the Investigator may conduct research using Restricted Data obtained through this Agreement.

H. "NACJD" is the National Archive of Criminal Justice Data at ICPSR.

I. "Physical Data Enclave" (PDE) is the physical space is located at ICSPR's facility in Ann Arbor, Michigan, and can be made available to researchers wishing to access data sets which contain highly sensitive personal information or data from protected populations. Data in the physical data enclave

typically contain highly sensitive personal information, data from protected populations, or data in which respondents can be identified.

J. "Principal Investigator" is the person primarily responsible for conducting or supervising the research or statistical activities relative to the Research Description of the Application for which Restricted Data are made accessible through this Agreement.

K. "Private Person" means any person as defined in 28 CFR § 22.2(a) other than an agency, or department of Federal, State, or local government, or any component or combination thereof. Included as a private person is an individual acting in his or her official capacity.

L. "Representative of the Institution" is a person authorized to enter into binding legal agreements on behalf of Investigator's Institution. Generally, this is a president, provost, or designated representative of the institution's office of sponsored programs, office of research, contracts office, or similar. IRB chairs, Professors, Deans, and Department Chairs typically do NOT have this authority.

M. "Research Team" are persons at the Principal Investigator's Institution, excluding the Principal Investigator, who will have access to Restricted Data through this Agreement, including co-principal investigators, students, other faculty and researchers, staff, agents, employees, consultants or contractors for which Institution accepts responsibility.

N. "Restricted Data" are 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.

O. "Secure Download" means that data files are encrypted and made available to the Principal Investigator. When the request is approved, for most studies the Principal Investigator receives a temporary link and password to download the restricted-use files. The Principal Investigator must destroy any copies of the data at the completion of the project.

P. "Virtual Data Enclave" (VDE) means that monitored access to Restricted Data Data is provided via a virtual desktop infrastructure managed by ICPSR. The virtual machine is isolated from the user's physical desktop computer, restricting the user from downloading files or parts of files to their physical computer. The virtual machine 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.

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. Investigators and Institutions who receive any portion of Restricted Data are obligated to adhere to all applicable confidentiality data use and provisions in federal law and 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 Principal Investigator**

A. The Principal Investigator agrees to complete the Application, ICPSR Confidentiality Pledge, BJS Privacy Certificate, and any other required documents, reports, and amendments for the selected restricted data access modality.

B. The Principal Investigator agrees to manage and use Restricted Data appropriately, implement all Restricted Data security procedures per the applicable Data Security Plan, and ensure that all members of the Research Team understand and affirm their agreement to follow the requirements per this Agreement and the applicable Data Security Plan.

C. Principal Investigators must meet each of the following criteria:

1. Demonstrate the capability to meet the requirements set forth in this Agreement, including the data use, security, and confidentiality requirements
2. Demonstrate the capability and appropriate expertise to fulfill the proposed research goals, e.g. have a PhD or hold a faculty appointment, or otherwise be in a position to use sensitive data to conduct research*
3. Have a demonstrated need for using sensitive data to complete the proposed research project and demonstrated ability to use and protect sensitive data according to commonly accepted standards and applicable statutory requirements

IV. **Requirements of Institution**

The Institution represents that it is:

A. An institution of higher education, a research organization, a research arm of a government agency, or a nongovernmental, not-for-profit, agency.*

B. 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. Have a demonstrated record of using sensitive data according to commonly accepted standards of research ethics and applicable statutory requirements.

* For questions or concerns regarding Principal Investigator eligibility or applicants without an institution affiliation, please contact **nacjd@icpsr.umich.edu** for assistance.

V. **Obligations of ICPSR**

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

A. Make the requested Restricted Data available in accordance with the Information Transfer Agreement requirements set forth in 28 C.F.R. Part 22.24 and terms of this Agreement.
B. Provide the Restricted Data requested by the Principal Investigator in the Application within a reasonable time of execution of this Agreement by Institution and to make the Restricted Data available to Principal Investigator via the selected Restricted Data access modality.
C. Provide electronic documentation of the origins, form, and general content of the Restricted Data sent to the Investigator, in the same time period and manner as the Restricted Data.
D. Conduct required disclosure risk reviews and assessments on output, findings, and other materials.
E. Adhere to applicable BJS requirements governing Restricted Data, including data confidentiality requirements in 28 C.F.R. Part 22.

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. Unless prohibited by law, Institution assumes all liability for claims for damages against them by third parties that may arise from the use, storage, disposal, or disclosure by the Institution of the Restricted Data, except to the extent and in proportion such liability or damages arise from the negligence of ICPSR.

VI. **Obligations of the Principal Investigator, Research Team, and Institution**

Restricted Data provided under this Agreement shall be held by the Investigator, Research Team, and Institution in strictest confidence and can be used or disclosed only for statistical or research purposes and in compliance with 28 C.F.R. Part 22 and the terms of this Agreement. In consideration of the promises in Section V of this Agreement, and for use of Restricted Data from NACJD, the Institution agrees:

A. That the Restricted Data will be used solely for research or statistical purposes relative to the project as identified in the Research Description of the Application (the "Research Description"), and for no other purpose whatsoever without the prior written consent of NACJD. 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. To comply fully with the confidentiality provisions outlined in 28 C.F.R. Part 22 and approved Data Security Plan at all times relevant to this Agreement.

C. To ensure that any individual who is granted access to Restricted Data during the Agreement period reviews and signs a copy of this Agreement, the BJS Privacy Certificate, and the ICPSR Confidentiality Pledge before being granted access to the Restricted Data.

D. That no persons other than those identified in this Agreement or in subsequent amendments to this Agreement, as Principal Investigator or a member of the Research Team, and who have signed this Agreement, the BJS Privacy Certificate, and the ICPSR Pledge of Confidentiality (Appendix F), be permitted access to the contents of Restricted Data files or any Derivatives from the Restricted Data.

E. To maintain a log of all individuals who have access to the Restricted Data covered under this agreement.

F. That any real or suspected security incident including Restricted Data covered under this agreement be reported to ICPSR in email or by phone within one hour of discovery. A security incident may involve real or suspected unauthorized access, use, loss of control, or disclosure of Restricted Data, or access, use, or disclosure of Restricted Data that is inconsistent with the terms and conditions of this Agreement.

G. That, unless prior specific, written approval is received from NACJD, 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.

H. To ensure project findings and reports prepared for dissemination will not contain information which can reasonably be expected to be identifiable to a private person.

I. 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 Restricted Data.[2]

1. No release of a 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 rare 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.

[1] For more information, see the *Federal Committee on Statistical Methodology Data Protection Toolkit* at https://www.fcsm.gov/resources/safe-guard-data/; *NCHS Disclosure Potential Checklist* at http:// 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:// 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.

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.
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 5^{th} or 95^{th} 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 from NACJD.
11. 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.

J. To abide by federal law and regulations that require that research data collected by the U.S. Department of Justice or by its grantees and contractors may only be used for research or statistical purposes. The applicable laws and regulations may be found in the United States Code, 34 USC Section 10231(a), (Confidentiality of Information), 28 CFR 22 (Confidentiality of Identifiable Information), 28 CFR Part 46 (Human Subjects Protections), and 62 F.R. 35044 (June 27, 1997) (The Federal Confidentiality Order). Accordingly, any identification or disclosure of a person or establishment – whether inadvertent or willful - may violate federal law as well as the assurances of confidentiality given to the providers of the information. Therefore, users of data collected by or with the support from the U.S. Department of Justice and distributed by NACJD or other ICPSR archives must agree to abide by these regulations and understand that NACJD and ICPSR may report any potential violation to the U.S. Department of Justice. Any person violating the provisions of 34 USC Section 10231(a), or of any rule, regulation, or order issued thereunder, shall be fined not to exceed $10,000, in addition to any other penalty imposed by law.

K. 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 one (1) hour of discovery of the actual or suspected incident;

3. The information that would identify the Private Person will be safeguarded or destroyed as requested by ICPSR; and

4. Unless required by applicable law or institutional policy/reporting, no one else will be informed of the discovered identity.

L. Unless other provisions have been made with NACJD, all originals and copies of the Restricted Data, if provided through the Secure Download System, shall be destroyed on or before completion of this Agreement or within (5) days of written request from NACJD or ICPSR. The Investigator must complete and notarize an Affidavit of Destruction, attesting to the destruction of the Restricted Data.

M. Unless other provisions have been made with NACJD, all originals and copies of the Restricted Data accessed through the Virtual Data Enclave, if applicable for the Restricted Data Access System selected, will be terminated on or before completion of this Agreement or within (5) days of written request from NACJD or ICPSR.

N. Upon acceptance by NACJD, the Principal Investigator and Research Team may have access to Restricted Data as defined herein until the completion of the applicable research project, or 24 months from the date this Agreement is accepted by NACJD, whichever comes first. If, at the end of 24 months, access to Restricted Data is still desired, the Principal Investigator must contact NACJD in writing requesting such continued access.

O. Principal Investigators requiring the Restricted Data beyond the completion of this Agreement should submit a request for continuation three months prior to the end date of the agreement. The obligation of destruction for data provided through the Secure Download System (if applicable), shall not apply to Investigator's scholarly work based upon or that incorporates the Restricted Data.

P. That any books, articles, conference papers, theses, dissertations, reports, or other publications that employed the Restricted Data or other resources provided by NACJD reference the bibliographic citation provided by NACJD and be reported to NACJD for inclusion in its data-related bibliography.

Q. To provide reports to NACJD staff as requested, which may include:

1. A copy of the annual IRB approval for the project described in the Research Description;
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 the Research Team 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.

R. To notify NACJD of a change in institutional affiliation of the Investigator, a change in institutional affiliation of any member of the Research Team, or the addition or removal of any member of the Research Team. Notification and must be received by NACJD at least six (6) weeks prior to the last day of employment with Institution. Notification of the addition or removal of Research Team shall be provided to NACJD as soon as reasonably possible. Principal Investigator's separation from Institution terminates this Agreement.

S. Upon Investigator's change in institutional affiliation, the Investigator must cease using the Restricted Data immediately and proceed with terminating their project as described in section I-K. For data access through the Virtual Data Enclave (VDE) or Physical Data Enclave (PDE), ICPSR will at the request and cost of the Investigator, maintain these files and reinstate data access to the Investigator upon submission and approval of a new Application by the new Institution. Although the Restricted Data will be stored in a secure location, ICPSR assumes no responsibility for the Restricted Data or associated files and the Institution and Investigator shall not be liable for any damages arising from any suits or claims arising from the storage of the Restricted Data or associated files by ICPSR. ICPSR makes no guarantees and provides no warranty that the exact same Restricted Data or associated files can be or will be provided to Investigator after such storage, or that any files or Restricted Data accessed by the Investigator after such storage will be free from defect or fit for any particular purpose.

T. Investigator may reapply for access to Restricted Data as an employee of the new institution. Re-application requires:

1. Completion of a new Application;
2. Execution of a new Agreement for the Use of Restricted Data by both the Principal Investigator and the proposed new institution;
3. Execution of ICPSR Pledge of Confidentiality by the Principal Investigator and Research Team at the proposed new institution;
4. Execution of BJS Privacy Certificate by the Principal Investigator and Research Team at the proposed new institution;
5. Preparation and approval of a new Data Security Plan; and
6. Evidence of approval or exemption by the proposed new institution's IRB.

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

U. That use of the Restricted Data will be consistent with the Institution's policies regarding scientific integrity and human subject's research.

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

VII. **Violations of this Agreement**

A. The Principal Investigator or Institution will investigate allegations by NACJD, ICPSR, or other parties of violations of this Agreement in accordance with its policies and procedures on scientific integrity and misconduct and applicable federal policies. If the allegations are confirmed, the Institution will treat the violations as it would violations of the explicit terms of its policies on scientific integrity and misconduct. Be aware that any person violating the provisions of 34 USC Section 10231(a), or of any rule, regulation, or order issued thereunder, shall if convicted be fined not to exceed $10,000, in addition to any other penalty imposed by law.

B. In the event of a breach of 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 ICPSR not adequately compensable by money damages. Institution hereby acknowledges the possibility of injunctive relief in the event of breach, in addition to money damages. In addition, ICPSR may:

1. Terminate this Agreement upon notice and immediately revoke access to the Restricted Data and any derivatives thereof;
2. Deny Principal Investigator future access to Restricted Data; and/or
3. Report the inappropriate use or disclosure to the appropriate federal and private agencies or foundations that fund scientific and public policy research.
4. Such other remedies that may be available to ICPSR under law or equity, including injunctive relief.

C. Principal Investigator or 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 Teams', 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 shall be construed as a waiver of any immunities and protections available to Institution under applicable law.

D. In the event of a violation, the Principal Investigator must:

1. Notify ICPSR within one (1) hour of discovery;
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 Investigator's Institution must submit an acknowledgment of the violation and security protocols and disclosure protections review to ICPSR;
5. Notify the appropriate IRB officials; and
6. Reapply for access to the Restricted Data.

VIII. **Confidentiality**

This Agreement is consistent with the requirements of the United States Code -- 31 USC Section 3729 et seq. (The False Claims Act), and 34 USC Section 10231(a), which authorizes the Department of Justice to collect confidential data while mandating strict protections -- and the Code of Federal Regulations -- 28 CFR 22 (Confidentiality of Identifiable Research and Statistical Information), 28 CFR 46 (Department of Justice version of the Common Rule), as well as 62 F.R. 35044 (June 27, 1997) (The Federal Confidentiality Order).

IX. **Incorporation by Reference**

All parties agree that the information entered into the Application, including all uploaded documents, are incorporated into this Agreement by reference.

X. **Miscellaneous**

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

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

Reporting Incidents
734-358-8875

B. This Agreement shall be effective for 24 months from execution, termination of the Agreement, or until the IRB expires, whichever occurs first.

C. The respective rights and obligations of ICPSR and Principal Investigator, Research Team, and Institution pursuant to this Agreement shall survive termination of the Agreement.

D. This Agreement and any of the information and materials entered into the Application may be amended or modified only by the mutual written consent of the authorized representatives of NACJD and Principal 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 Representative of the Institution signing this Agreement has the right and authority to execute this Agreement, and no further approvals are necessary to create a binding agreement.

F. The obligations of Principal Investigator, Research Team, 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
ADDRESS	ADDRESS
CITY, STATE ZIP	CITY, STATE ZIP
PHONE	PHONE
EMAIL	EMAIL

Appendix A
ICPSR Physical Data Enclave (PDE)
Data Security Plan

I agree to fulfill my responsibilities on this research project in accordance with the following guidelines:

1. No copies will be made by Researcher of any files, portions of files, or Enclave Data to which access is granted. This includes hard copies of materials and screenshots.

2. No paper, including written notes pertaining to the identification of any establishment, individual, or geographic area that may be revealed in the conduct of my research in the enclave, will be removed by Researcher from the Enclave.

3. No printouts, electronic files, documentation or media will be removed by Researcher from the enclave until they have been reviewed for disclosure risk by enclave staff after the researcher's visit.

4. No attempts will be made to bring any electronic recording devices, including cameras and cell phones, into the Enclave.

5. No unauthorized persons will be given access to the Enclave and the Enclave door will remain closed and locked at all times.

INVESTIGATOR NAME	INVESTIGATOR SIGNATURE DATE

Appendix B
ICPSR Virtual Data Enclave (VDE)
Data Security Plan

I agree to fulfill my responsibilities on this research project in accordance with the following guidelines:

I. Passwords and Login Sessions

A. Guest logins to the computer are disabled and only computer accounts for authorized VDE users are enabled.

B. The VDE user must password protect the computer that is used to access the Restricted data and set the computer to activate a password protected screen saver after 15 minutes or less of inactivity.

C. Under no circumstances may the VDE user share or give their VDE login and password to anyone, including other members of the research project team or their organization's information and technology (IT) staff personnel. In addition, the VDE user must never share their computer account credentials.

D. VDE passwords may only be electronically stored in software designed for secure password storage. Offline password manager software is preferred.

E. If the VDE user is logged into the VDE and they leave their computer, they must first "disconnect" or "log off" from the VDE. The VDE user must also manually lock the computer screen. (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.)

II. Physical Workspace Requirements

A. The VDE user's computer is located in a secure office space with a locked door. The secure office space must be closed and locked when unoccupied and no unauthorized persons are allowed inside the secure office when VDE users are logged into the VDE.

B. If a secure office space is not accessible to the VDE user, the user may request approval for an alternate workspace. (The alternate workspace must maintain the appropriate physical safeguards to protect the data and mitigate its exposure. Preference is given to private or low traffic areas, computer monitors equipped with privacy screens and laptops that can be securely stored in locked cabinets or drawers when not in use). You must email ICPSR-help@umich.edu to request approval for an alternative workspace and provide sufficient details to describe the specific controls and procedures that will be used to safeguard the data.

C. The VDE user will not allow any unauthorized person to access or view the Restricted Data under any circumstances. The computer monitor display screen must not be visible to unauthorized people while the user is accessing the data. For example, the computer screen should not be visible through doors or windows, or to high traffic areas. A privacy screen is recommended to restrict viewing angles.

D. VDE users may not discuss the Restricted Data or results from the Restricted Data in public or non-secure settings unless those results have received disclosure review and approval by ICPSR. VDE users may only discuss the data and results, prior to ICPSR approval, with other approved members of the Research Team in secure private settings.

III. Use of User IT Staff

A. The VDE user should not contact IT staff at their organization with questions about the Restricted Data. (They may contact their organization's IT staff if they need help installing the VDE client software to access the Restricted Data.) The Restricted Data is prohibited from being accessible to the organization's IT staff.

IV. Data Management and Statistical Output

A. The VDE user will keep all Restricted Data and derivatives within the VDE. Any documents which are related to the Restricted Data, such as research notes, must be maintained only in the VDE until ICPSR approval for release. One approved by ICPSR, the VDE user may only share aggregated information from the Restricted Data

B. The VDE user must not duplicate or copy any data, documentation, research output or statistics, or other VDE materials outside of the VDE unless and until such materials have been approved and removed from the VDE by ICPSR staff. This includes, but is not limited to:
    1. taking screenshots, photographs, or videos of these materials
    2. sharing any of these materials via email, chat, or any other online program, even to ICPSR staff or to other authorized users
    3. typing, writing, or otherwise recording these materials onto an office or personal computer, or onto some other device or media
    4. creation of hardcopy documents containing these materials

C. The VDE user must submit all statistical outputs/results/notes from the Restricted Data to ICPSR at ICPSR-help@umich.edu for disclosure review. All materials must be reviewed, approved, and removed from the VDE by ICPSR staff only. The VDE user also agrees to revise or alter files, as requested by ICPSR, in order to minimize disclosure risk before the materials are removed from the VDE by ICPSR.

INVESTIGATOR NAME	INVESTIGATOR SIGNATURE DATE

Appendix C
ICPSR Secure Download – Local Virtual or Physical Enclave on an Isolated Network
Data Security Plan

To access these data via the Secure Download access modality, please review all Secure Download Data Security Plans and select the plan that best meets your project's needs.

Local Virtual or Physical Enclave on an Isolated Network Data Security Plan
This Investigator will store and work with Restricted Data in a secure environment managed by their institution. Security requirements include a secure datacenter, full encryption at rest and in transit, and strong technical controls to prevent Restricted Data from leaving or being shared outside the secure environment. A Virtual Desktop Environment is a common method for providing a secure environment. ICPSR does not permit Restricted Data to be stored and used on a shared file server without strong data flow controls, nor does ICPSR allow Restricted Data to be stored, used, or transferred using third-party cloud-based tools.

I agree to fulfill my responsibilities on this research project in accordance with the following guidelines:

1. Data will remain stored in a secure, locked location and will only be accessed by approved researchers from a private room or office. Computer monitor(s) will be oriented to prevent eavesdropping. The computer screen will be set to auto-lock after 15 minutes (or less) of inactivity and all users agree to manually lock the screen or log off from the desktop when stepping away. All users will utilize all applicable security features available within their local computer's operating system to prevent unauthorized data access, including password-protected user accounts and NTFS permissions. Login credentials will not be shared with others.

2. Should any actual or suspected security incidents or breaches of this plan occur, the Principal Investigator will notify ICPSR within the time frame specified in the Restricted Data Use Agreement by contacting ICPSR-help@umich.edu or 734-358-8875.

3. The Principal Investigator will either renew this Restricted Data Use Agreement or destroy all data at or prior to the conclusion of the Restricted Data Use Agreement. The Principal Investigator will certify in writing at the end of the access period that all copies of the restricted data have been destroyed.

4. Restricted data will be completely removed from all storage and backups at or prior to the conclusion of the Restricted Data Use Agreement. Use of secure multi-pass erasure software meeting or exceeding DoD 5220.22 M standards is recommended.

5. Any printed copies of the data will be destroyed appropriately (e.g., shredded rather than recycled or placed intact in a waste receptacle) at or prior to the conclusion of the Restricted Data Use Agreement.

6. Data will be stored directly on a private, secure server that is maintained by the Institution's IT department. Restricted data files may not be removed from this system for any reason. This system has technical controls in place to prevent and/or log any attempts to move or copy data off of the secure directory, and access to the directory containing these data will be restricted to only the Principal Investigator and Research Team listed within the Application.

7. Any IT system's infrastructure that maintains Restricted Data meets or exceeds compliance with FISMA Moderate standards (or equivalent). Appropriate documentation of security controls must be provided to ICPSR (e.g., System Security Plan).

8. The operating system of the local computer will remain current and kept up-to-date with system and application security patches.

9. During all backups of the computer(s), the restricted data will be excluded from backups or fully encrypted with the chain-of-custody documented and secured.

10. IT personnel at the Principal Investigator's institution who will have access to the Restricted Data must have existing contracts or non-disclosure agreements (to be provided to ICPSR upon request) in place with the Investigator's institution and be informed of and certify in writing their agreement to comply with the terms of this Agreement.

11. FIPS 140-compliant encryption software must be used for full-disk encryption of the local computer used to access the data. The connection between the storage server and the local computer will be fully encrypted. Note: Folder- or file-level encryption is not sufficient. ICPSR recommends the use of Windows BitLocker or Mac OSX Disk Utility.

12. Please describe the secure location for data access and procedures for data security:

13. Should there be a need to change or modify this security plan, the Principal Investigator will contact ICPSR-help@umich.edu for assistance. Note that all requests to modify existing security plans must be reviewed and approved by ICPSR prior to any restricted data files being moved or transferred to a new location.

INVESTIGATOR NAME	INVESTIGATOR SIGNATURE DATE

Appendix D
ICPSR Secure Download – Standalone Computer
Data Security Plan

To access these data via the Secure Download access modality, please review all Secure Download Data Security Plans and select the plan that best meets your project's needs.

Standalone Computer Data Security Plan
The Investigator will store and work with the Restricted Data on a dedicated standalone computer that will not be used for activity other than the storage and analysis of Restricted Data for the duration of the Restricted Data Use Agreement.

I agree to fulfill my responsibilities on this research project in accordance with the following guidelines:

1. Data will remain stored in a secure, locked location and will only be accessed by approved researchers from a private room or office. Computer monitor(s) will be oriented to prevent eavesdropping. The computer screen will be set to auto-lock after 15 minutes (or less) of inactivity and all users agree to manually lock the screen or log off from the desktop when stepping away. All users will utilize all applicable security features available within their local computer's operating system to prevent unauthorized data access, including password-protected user accounts and NTFS permissions. Login credentials will not be shared with others.

2. Should any actual or suspected security incidents or breaches of this plan occur, the Principal Investigator will notify ICPSR within the time frame specified in the Restricted Data Use Agreement by contacting ICPSR-help@umich.edu or 734-358-8875.

3. The Principal Investigator will either renew this Restricted Data Use Agreement or destroy all data at or prior to the conclusion of the Restricted Data Use Agreement. The Principal Investigator will certify in writing at the end of the access period that all copies of the restricted data have been destroyed.

4. Restricted data will be completely removed from all storage and backups at or prior to the conclusion of the Restricted Data Use Agreement. Use of secure multi-pass erasure software meeting or exceeding DoD 5220.22 M standards is recommended.

5. Any printed copies of the data will be destroyed appropriately (e.g., shredded rather than recycled or placed intact in a waste receptacle) at or prior to the conclusion of the Restricted Data Use Agreement.

6. Data will be stored directly on a standalone, non-networked computer. All network cables will be physically disconnected from the computer, wireless network access will be disabled, and computer network ports will be disabled. The computer will not be connected to any networks nor the Internet for the duration of this research project.

7. Restricted data files will not be copied or moved out of the secured directory on the computer's internal hard drive for any reason.

8. FIPS 140-compliant encryption software will be used for full-disk encryption of the computer used to

store and access the data. Note: Folder- or file-level encryption is not sufficient. ICPSR recommends the use of Windows BitLocker or Mac OSX Disk Utility.

9. Please describe the secure location for data access and procedures for data security:

10. Should there be a need to change or modify this security plan, the Principal Investigator will contact ICPSR-help@umich.edu for assistance. Note that all requests to modify existing security plans must be reviewed and approved by ICPSR prior to any restricted data files being moved or transferred to a new location.

INVESTIGATOR NAME	INVESTIGATOR SIGNATURE	DATE

Appendix E
ICPSR Secure Download – External Hard Drive
Data Security Plan

To access these data via the Secure Download access modality, please review all Secure Download Data Security Plans and select the plan that best meets your project's needs.

External Hard Drive Data Security Plan
The Investigator intends to work with Restricted Data on their personal or institutional computer that may also be used for activity other than the storage and analysis of Restricted Data for the duration of the Restricted Data Use Agreement.

I agree to fulfill my responsibilities on this research project in accordance with the following guidelines:

1. Data will remain stored in a secure, locked location and will only be accessed by approved researchers from a private room or office. Computer monitor(s) will be oriented to prevent eavesdropping. The computer screen will be set to auto-lock after 15 minutes (or less) of inactivity and all users agree to manually lock the screen or log off from the desktop when stepping away. All users will utilize all applicable security features available within their local computer's operating system to prevent unauthorized data access, including password-protected user accounts and NTFS permissions. Login credentials will not be shared with others.

2. Should any actual or suspected security incidents or breaches of this plan occur, the Principal Investigator will notify ICPSR within the time frame specified in the Restricted Data Use Agreement by contacting ICPSR-help@umich.edu or 734-358-8875.

3. The Principal Investigator will either renew this Restricted Data Use Agreement or destroy all data at or prior to the conclusion of the Restricted Data Use Agreement. The Principal Investigator will certify in writing at the end of the access period that all copies of the restricted data have been destroyed.

4. Restricted data will be completely removed from all storage and backups at or prior to the conclusion of the Restricted Data Use Agreement. Use of secure multi-pass erasure software meeting or exceeding DoD 5220.22 M standards is recommended.

5. Any printed copies of the data will be destroyed appropriately (e.g., shredded rather than recycled or placed intact in a waste receptacle) at or prior to the conclusion of the Restricted Data Use Agreement.

6. Data will be stored directly on an encrypted external hard drive, and will not be copied or moved out of the secured directory on the external hard drive for any reason. FIPS 140-compliant encryption software will be used for full-disk encryption of the local computer used to access the data, as well as for full-disk encryption of the external drive used to store the data. Note: Folder- or file-level encryption is not sufficient. ICPSR recommends the use of Windows BitLocker or Mac OSX Disk Utility.

7. The local computer used to access the hard drive containing restricted data will be disconnected from the Internet and all other networks during any time that the external drive is physically connected to the

machine.

8. During all backups of the computer(s), the restricted data will be excluded. This also applies to any cloud-based storage and/or backups (e.g., Box, DropBox, OneDrive, iCloud).

9. The operating system of the local computer will remain current and kept up-to-date with system and application security patches.

10. Please describe the secure location for data access and procedures for data security:

11. Should there be a need to change or modify this security plan, the Investigator will contact ICPSR-help@umich.edu for assistance. Note that all requests to modify existing security plans must be reviewed and approved by ICPSR prior to any restricted data files being moved or transferred to a new location.

INVESTIGATOR NAME | INVESTIGATOR SIGNATURE | DATE

Appendix F
ICPSR Pledge of Confidentiality

By virtue of my affiliation with this research project I have access to Restricted Data identified in this Agreement. I understand that access to this Restricted Data is subject to applicable federal laws that protect data confidentiality and the exclusive statistical or research use of the data and carries with it a responsibility to guard against unauthorized use and to abide by the Data Security Plan. To treat information as restricted means to not divulge it (willfully or inadvertently) to anyone who is not a party to the Agreement for the Use of Restricted Data or cause it to be accessible to anyone who is not a party to that Agreement.

I agree to fulfill my responsibilities on this research project in accordance with the following guidelines:

- I have read the associated Agreement for the use of Restricted Data.
- I am a "Principal Investigator" or member of the "Research Team " within the meaning of the Agreement.
- I will comply fully with the terms of the Agreement, including the legal requirements to protect confidentiality of identifiable information (34 U.S.C. § 10231 and 28 C.F.R. Part 22), the legal requirement to use the data for only statistical or research purposes (34 U.S.C. § 10134), and the Data Security Plan.
- I agree not to permit Restricted Data access to anyone not a party to the Agreement for the use of Restricted Data, in either electronic or paper copy.
- I agree to not attempt to identify private persons as defined in the Agreement for the use of Restricted Data.
- I agree that in the event an identity of any private person is discovered inadvertently, I will (a) make no use of this knowledge, (b) report the incident to ICPSR, (c) safeguard or destroy the information after consultation with ICPSR, and (d) not inform any other person of the discovered identity.

NAME SIGNATURE DATE