Data Portal Confidentiality Procedures Manual

September 2013

U.S. Department of Health and Human Services (DHHS)
Substance Abuse and Mental Health Services Administration (SAMHSA)
Center for Behavioral Health Statistics and Quality (CBHSQ)

1 Choke Cherry Road
Rockville, MD 20857

Table of Contents

1. Introduction

This *Data Portal Confidentiality Procedures Manual* is provided to assist organization(s) interested in obtaining access to Center for Behavioral Health Statistics and Quality (CBHSQ), Substance Abuse and Mental Health Services Administration (SAMHSA) Confidential Data.

Confidential Data can only be accessed remotely through a secure Data Portal. This virtual computing environment has been designed with the specific purpose of providing access for authorized researchers to conduct approved research using Confidential Data that would not otherwise be available. Data Portal access is only provided through approved computer location(s) and IP address(es) at the researcher's organization. Users are required to maintain the confidentiality of the data utilized within the Data Portal. Researchers cannot transfer data into or out of the secure Data Portal.

The goal of the Data Portal is to maximize the use of CBHSQ data for important research and policy analyses, while conforming to Federal law and protecting identifiable data from disclosure. This manual describes the application process and the computer and data security requirements that must be followed if the application is approved and the organization is granted access to the data through the Data Portal.

This Manual was created as a guide to the process for applying for access to CBHSQ Confidential Data, as well as to explain the laws and regulations and security requirements governing the use of these data. It serves as a procedures guide and does not replace the provisions of the actual Confidential Data Use and Nondisclosure Agreement (i.e., data use agreement).

2. Legal Background

CBHSQ data are collected pursuant to SAMHSA's authority under Section 505[1] of the Public Health Service Act (PHS Act). Access to most CBHSQ Confidential Data is covered by a Federal law called the Confidential Information Protection and Statistical Efficiency Act (CIPSEA) of 2002 (see P.L. 107-347, Title V) and the Public Health Services (PHS) Act[2], as well as several other Federal laws. CIPSEA restricts the use of information to statistical purposes only.

In "public-use data" files, individually identifiable information has been recoded or deleted to protect the confidentiality of survey respondents. Access to public-use data does not require a license or other contract and is available online to the general public. However, access to Confidential Data requires a data use agreement (contract) between CBHSQ and the researcher's organization. CBHSQ Confidential Data do not include direct identifiers such as name or address.

There is demand for additional data that is not included in public-use data files. For example, analysts and policy makers have been interested in estimates at the state and local level, as well as for certain subpopulations. CBHSQ is required to comply with the confidentiality provisions of both the PHS Act and CIPSEA. Under the provisions of 501(n) [3] of the PHS Act, information that is individually identifiable may only be used and released for the purpose for which it was supplied unless consent was given to use the information for some other purposes. Requesting access to Confidential Data requires following the requirements of CIPSEA. If a researcher is granted access to the data, all legal and security requirements for using the data must be met and implemented.

CIPSEA was enacted as part of the E-Government Act of 2002[4] and is intended to facilitate data protection and sharing. In November 2006, the Office of Management and Budget (OMB) designated CBHSQ as a federal statistical unit. Statistical agencies or units, such as CBHSQ, may designate agents with whom Confidential Data may be shared, so long as the agent uses the data for a statistical purpose and the agent agrees to implement security protections as established by the statistical unit. Violations of the provisions of CIPSEA are subject to five years imprisonment and/or a fine of up to $250,000.

---

[1] http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&docid=Cite:+42USC290aa-4

[2] See 42 U.S.C. 290aa(n)

[3] Section 501(n) states "No information, if an establishment or person supplying the information or described in it is identifiable, obtained in the course of activities undertaken or supported under section 290aa–4 of this title may be used for any purpose other than the purpose for which it was supplied unless such establishment or person has consented (as determined under regulations of the Secretary) to its use for such other purpose. Such information may not be published or released in other form if the person who supplied the information or who is described in it is identifiable unless such person has consented (as determined under regulations of the Secretary) to its publication or release in other form."
http://frwebgate3.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=54521924645+13+0+0&WAISaction=retrieve

[4] P.L. 107-347, Title V.

Under CIPSEA, the following provisions apply when CBHSQ shares data for research purposes:

- Data can only be made available to "agents" designated by the statistical unit (CBHSQ). Each agent is an "individual data recipient".
- The data can be used only for statistical purposes.
- CBHSQ decides whether individual data recipient's analysis is safe to release (through a disclosure review) once disclosure risks in the analysis are minimized.
- Data are shared only on an as-needed basis; CBHSQ decides what data are available to share and when access is appropriate.
- Each individual data recipient has to undergo annual CIPSEA training.
- Each individual data recipient has to sign a certificate of Designation of Agent and Affidavit of Nondisclosure form.
- CBHSQ is responsible for monitoring individual data recipients and conducting site inspections for data security compliance.

The CBHSQ Confidential Data access program is designed to comply with the requirements of both 501(n) and CIPSEA. In addition to 501(n) and CIPSEA, the protection of data with individually identifiable information is found in other Federal laws such as the Privacy Act of 1974[5] and the Federal Information Security Management Act of 2002[6].

The Privacy Act of 1974 (5 U.S.C. 552a) protects the privacy of personal data maintained by the Federal Government. It imposes numerous requirements upon Federal agencies to safeguard the confidentiality and integrity of personal data and limits the uses to which one may use the data. Under the direction of the Office of Management and Budget, Federal agencies issue policies, standards, and guidelines for protecting personal data. A key standard is the Federal Information Processing Standard Publication (FIPSPUB) 41, *Computer Security Guidelines for Implementing the Privacy Act of 1974*. FIPSPUB 41 provides guidance to ensure that government-provided individually identifiable information is adequately protected in accordance with Federal statutes and regulations.

The Federal Information Security Management Act (FISMA) of 2002 (P.L. 107-347, Title III) requires that each federal agency develop, document, and implement an agency-wide program to provide security for the information and the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Under FISMA, information security means protecting information and the systems it resides on from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality and availability.

[5] 5 U.S.C. 552a.
[6] P.L. 107-347, Title III.

3. The Application Process

Overview

Who Can Apply for Access to Confidential Data?

CBHSQ provides Confidential Data only to qualified organizations in the United States. Individual researchers must apply through a recognized organization (e.g., a government agency, university, or research organization). An Application for Access will only be considered if it is submitted by the Call for Application deadline.

The Principal Project Officer (PPO) will serve as the project contact person at a Receiving Organization. The Receiving Organization Representative (ROP) is an individual who has the legal authority to bind the organization to a contract. A ROP must sign the legally binding contract (i.e., data use agreement) prior to access to CBHSQ Confidential Data.

The PPO must be directly employed at the Receiving Organization (i.e., they cannot be a contractor, temporary employee, visiting professor or outside consultant to the Receiving Organization). Research Staff must be directly employed by or students currently enrolled at the Receiving Organization. At institutions of higher education, the PPO must have an advanced degree (e.g., Ph.D., J.D., M.D. or Ed.D.). Usually PPOs serve as principal investigators of research projects or sponsor Ph.D. students conducting dissertation research. Graduate students may not apply for access and must find a qualified faculty member to apply on their behalf.

The Receiving Organization headquarters, related business offices and/or research site locations must be located in the 50 United States or District of Columbia. An Application will not be approved if the Receiving Organization's place of business is within a private residence.

If there are multiple Receiving Organizations, then a PPO at one of the Receiving Organizations must be designated on the Application for Access as the Primary Contact for the overall project.

The maximum number of persons who may have access to the Confidential Data during the project is limited to ten (10). This includes the PPO and Research Staff combined and for projects that span across multiple organizations.

The Application must clearly outline the nature of the proposed research project as well as the specific information and categories of variables needed and how this information will be used. Only the data requested in your application and approved as part of the signed Agreement will be provided for your use in the Data Portal. Any additional data must be requested and approved through a formal, signed amendment to the Agreement. Such an amendment would be required for *any* data other than that originally requested under the Agreement—including *any additional* CBHSQ data files or data from sources.

As part of the Agreement, the PPO and each Project team member must confirm and implement the physical security requirements for computer set-up and locations as well as behavioral security requirements regarding the action of project team members. Section 3 discusses the security requirements.

To better understand the data, security requirements, and restrictions, please review all of the documents in the Appendices prior to the submission of your Application form. Also, please see Appendix 3 for a list of some conditions that must be met for an application to be approved. The Appendices include copies of the forms for reference but you should download the forms from the website to ensure that you have the current versions.

If you have any questions, please contact dataportal@icpsr.umich.edu.

Confidential Data Request

As part of the Application for Access, the PPO must determine which surveys and survey years are needed for the proposed project. The data currently available are for the National Survey on Drug Use and Health and the Drug Awareness and Warning Network. The survey years that are available are listed on the Application for Access. Much of the information on variables is available through the codebooks for the public-use files. Additionally, a complete listing of all variables in the Confidential NSDUH Data files is available on the Data Portal website. The combined examination of the public-use data codebook, the questionnaires, and the Confidential Data variable lists, may help analysts decide whether the public-use file meets their research purposes or whether the Confidential Data are needed. You can also contact CBHSQ for more information on approximate sample sizes (exact sample sizes are confidential).

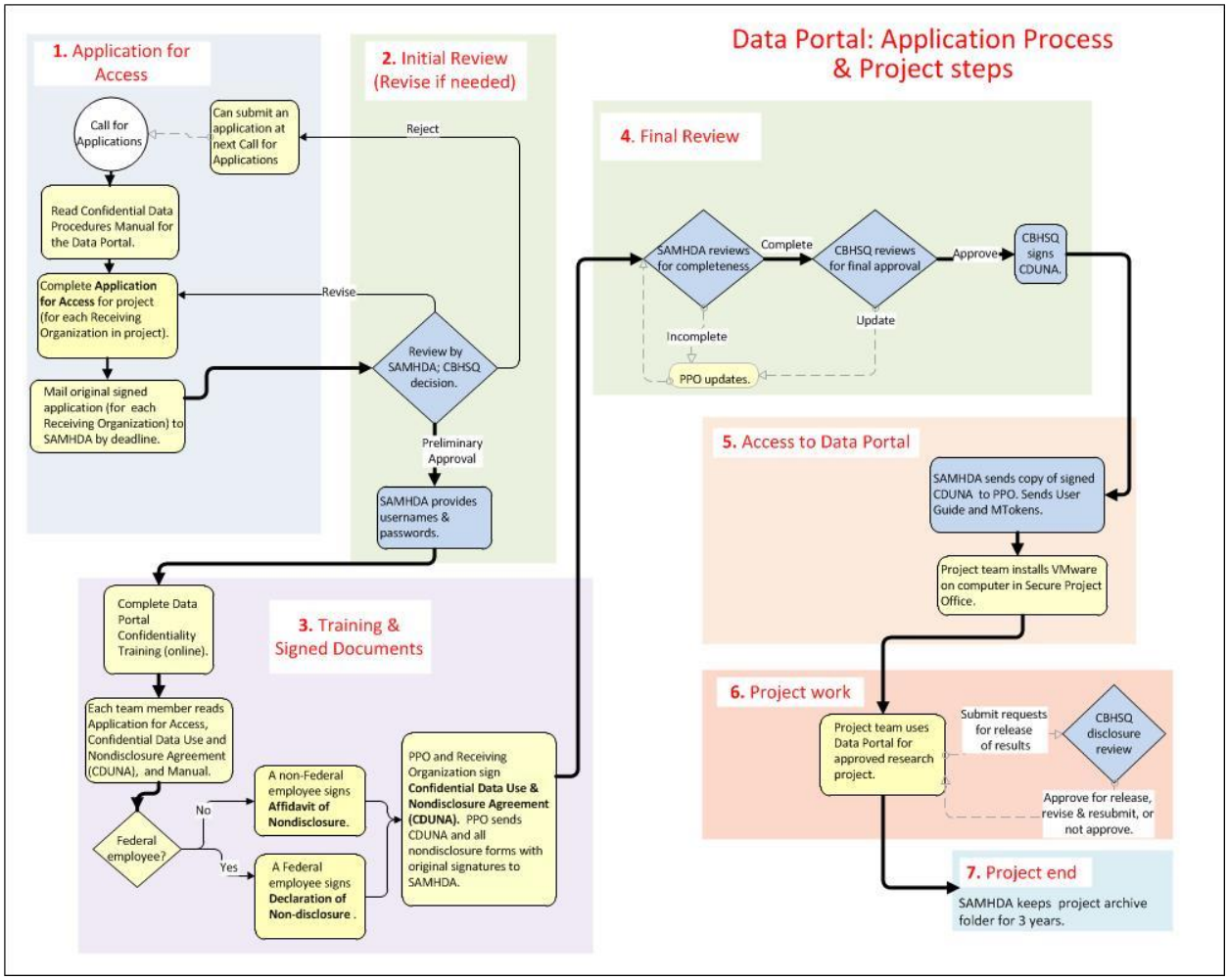
Other Data Requests

Any request for additional non-CBHSQ data to be used in your research should be requested as part of your original Application. You will have to make the case for why the data are needed for your research.

If additional data are requested after the Agreement is signed, then this request is an amendment to your Application and must also go through an approval process, including a consideration of potential disclosure issues that arise from combining data sources. If CBHSQ approves, then the data would be provided through the Data Portal.

Steps in the Application Process

The application process and main project steps are summarized in the flowchart on the next page, and are described in this section. The names of the documents are in bold italics in the list of steps. The forms that are needed are available on the SAMHDA website: www.icpsr.umich.edu/icpsrweb/content/SAMHDA/dataportal.html



STEP 1 - SUBMIT APPLICATION FOR ACCESS

(i) Complete the ***Application for Access to Confidential Data*** which has three sections and a signature page:

Section A.

- Information for your Receiving Organization: name, title, and contact information for the Principal Project Officer and all project team members (including all who will have access to the data), and organization information
- Summary of Experience and Curriculum Vitae
- Description of the Secure Project Office(s) where the data will be accessed

Section B.

- Information for all Receiving Organizations participating in the project

Section C.

- Description of the proposed research project

- Data requested and why the public-use data file(s) and the Restricted-use Data Access System (R-DAS) are not adequate for the research project
- Survey years requested
- Request for restricted variables

Original Signature Page.

- Signed by PPO

- Important: For more information on Receiving Organizations, how to complete the Application for Access for projects involving more than one Receiving Organization, or how a PPO submits multiple research projects, see the section on "Receiving Organizations" and "Multiple Project Research Topics, as well as the instructions for the Application for Access form in the Appendix.

(ii) Send the completed Application to SAMHDA by mail or courier to the address below by the deadline for the Call for Applications. This must be the original paper copy (with original signatures in blue ink):

For United States Postal Service:

ICPSR/SAMHDA
University of Michigan
Institute for Social Research
P.O. Box 1248
Ann Arbor, MI 48106-1248

For Courier (UPS, Fed EX, DHL, etc.) delivery:

ICPSR/SAMHDA
330 Packard Street
Ann Arbor, MI 48104

(iii) Send a Word version of the Application to SAMHDA. (This does not need to be signed and does not need to include CVs.)

STEP 2 - REVIEW OF APPLICATION BY SAMHDA AND CBHSQ.

Review Criteria

Since CBHSQ can only approve a limited number of applications, application evaluation criteria will be used. The primary evaluation criteria are:

- The behavioral health impact of the proposed project and its potential contribution and alignment with Department of Health & Human Services and SAMHSA missions,
- How well the research is aligned with the purpose[7] for which the data were collected, and

[7] The Data Portal will initially make Drug Abuse Warning Network (DAWN) and National Survey on Drug Use and Health (NSDUH) data sets available. For descriptions of these data sets, see DAWN (http://www.samhsa.gov/data/DAWN.aspx) and NSDUH (http://www.samhsa.gov/data/NSDUH.aspx) resources.

- Whether the data requested is suitable for the proposed research project given data limitations (available sample size or survey content).

CBHSQ will also consider secondary evaluation criteria as:

- Available resources needed by CBHSQ to prepare the data file and the cost of site inspection.
- The experience and capabilities of the research team.

Review Process

SAMHDA reviews each Application for Access to check that it is complete. If not, SAMHDA requests that the PPO provide the missing information for Application for Access.

It is possible that additional information may be requested by CBHSQ to clarify the information provided in the Application. If needed, CBHSQ may contact the applicants to discuss aspects of the Application.

CBHSQ staff will determine if there are enough cases for the proposed analysis and if the proposed dissemination plan can protect respondent identity from disclosures.

Reasons for non-approval may include confidentiality concerns, inability of data to support planned analyses (e.g., requested variables not collected or too sensitive or inadequate sample size), or other reasons, such as incomplete application or unresolved security issues.

Once all Applications have been received from all Receiving Organizations and each is complete, SAMHDA forwards the Application to CBHSQ for final approval. If CBHSQ approves the Application, SAMHDA will contact the research team to start the process of confidentiality training.

Overview of Review Outcomes

SAMHSA/CBHSQ reviews the Application and decides whether to give preliminary approval, require revisions, or reject the application:

- *Preliminary Approval.* CBHSQ will verify that only eligible individuals will have access to the data. When a project has received preliminary approval, SAMHDA provides usernames and passwords and instructions for the online Data Portal Confidentiality Training.
- *Revise.* If revisions are required, SAMHDA notifies the PPO and the PPO revises the Application and emails it to SAMHDA. (Revisions should be summarized in a cover note and changes in the Application should be indicated in bold, underline text, in blue font. The revised application does not require original signatures.)

- *Reject.* If the application is rejected (e.g., it is submitted after the deadline), then another application can be submitted during the next Call for Applications.

STEP 3 - COMPLETE TRAINING AND SIGN DOCUMENTS

(i) **Data Portal Confidentiality Training.** Each team member (including PPO) must complete the online Data Portal Confidentiality Training course and read the approved *Application for Access, Confidential Data Use and Nondisclosure Agreement* (CDUNA), and the *Data Portal Confidentiality Procedures Manual*.

(ii) The PPO and each team member must sign either an Affidavit of Nondisclosure or a Declaration of Nondisclosure:

- Each team member who is ***not*** a Federal employee must sign a ***Designation of Agent and Affidavit of Nondisclosure*** form where he/she agrees to abide by CIPSEA requirements and the Confidential Data Use and Nondisclosure Agreement. This Affidavit must be notarized. (A copy of the form is in Appendix D.)
- If the research team member is a Federal government employee, the team member must sign the ***Designation of Agent and Declaration of Nondisclosure*** form after completing the confidentiality training. (A copy of the form is in Appendix C.)

Note: All project team members must complete confidentiality training on an annual basis. The signed nondisclosure form serves to designate a person as an 'agent' under CIPSEA.

(iii) The Principal Project Officer (PPO) and the Receiving Organization Representative (who has the authority to sign legally binding contracts for the Organization) both sign the ***Confidential Data Use and Nondisclosure Agreement*** **(CDUNA).**

(iv) The PPO sends the original signed, notarized Affidavit(s) or signed Declaration(s) and the original signed CDUNA to SAMHDA by United States Postal Service or by Courier to an address listed in Step 1.

STEP 4 - FINAL REVIEW

Step 4 is the final step in the Application and approval process.

Once the original signed CDUNA and Affidavits are received by CBHSQ, CBHSQ review for completeness. If the CDUNA is complete, then CBHSQ will process it for signature. A copy of the signed and approved CDUNA will be sent to the PPO. At this point, the PPO and project team will be authorized to access the Data Portal.

PROJECT BEGINS

STEP 5 - ACCESS TO DATA PORTAL

SAMHDA forwards a copy of the signed CDUNA, *Data Portal User Guide* and MTokens to the PPO.

The project team members follow instructions in the *Data Portal User Guide* to set up access to the Data Portal. (Access may only be set up on the computer(s) in Secure Project Office(s) as listed and approved Application for Access.)

SAMHDA will load the data into the project folders within the Data Portal. Access to these data is allowed only for approved project members who have signed Affidavits within the last year.

STEP 6 - PROJECT WORK

The project team carries out the approved research.

Disclosure Review and Release of Results. Results can only be released outside of the Data Portal as approved by CBHSQ. The PPO for the project submits request for disclosure review to SAMHDA. The results submitted for disclosure review should be in near-final form as would be needed for publication or presentation. Results that include many results from analytic runs or a large number of tables or computer outputs are not near-final form and are discouraged. The review process is covered in Section 5 of this Manual and in the *Data Portal User Guide*.
All project team members must complete confidentiality training on an annual basis.

STEP 7 - PROJECT END

At the end of the project, SAMHDA stores an archive project folder provided by the Primary Contact for three years (unless an extension for a longer period of time has been requested and approved by CBHSQ/SAMHSA prior to expiration date). Also, see Section 8 of this Manual on "Closing out a Project".

Receiving Organizations

The Receiving Organization must be an institution of higher education, a research organization, or a government agency. The Receiving Organization headquarters, related business offices and/or research site locations must be located in the 50 United States or District of Columbia. An Application will not be approved if the Receiving Organization's place of business is within a private residence.

The Principal Project Officer (PPO) will serve as the contact person for the project at an individual Receiving Organization and signs the Application for Access and CDUNA. The Receiving Organization Representative (ROP) is an individual who has the legal authority to bind the organization to a contract. Only the ROP, as the legal representative for Receiving

Organization, may sign the legally binding contract required for access to CBHSQ Confidential Data.

A project may involve one organization with multiple locations or multiple Receiving Organizations. Each situation is described below:

- Single Receiving Organization. If your project involves one organization with researchers at one or more locations, and the organization is represented by a single Receiving Organization Representative, then there is one PPO and one Receiving Organization for your project. You will need to complete only one Application for Access, which lists the researchers for each location. Each location must also be identified and described.

- Multiple Receiving Organizations. If your project involves multiple collaborators at different Receiving Organizations:

    - Each Receiving Organization will need to have a separate PPO and a separate Application for Access.

    - For the Application process, one of the PPOs must be designated as the Primary Contact with SAMHDA and CBHSQ. The Primary Contact coordinates the Applications from the Receiving Organizations, including the content of Section B (which lists all the Receiving Organizations involved in the project) and Section C (which contains the research proposal and data request).

    - Responses for Sections B and C must be identical for applications from all of the Receiving Organizations. So either…
        - Applications for all the Receiving Organizations are sent to SAMHDA in one package, including (i) Application sections for each Receiving Organization that are specific to the Organization (i.e., Section A, signature page, and curriculum vitae) and (ii) one copy of Section B and C.
          This option is preferred as it facilitates review and processing of the Application.
          Or
        - Each Receiving Organization submits its own application separately. The PPO of each Receiving Organization inserts the same Section B and Section C content as coordinated and provided by the Primary Contact. This information must be included in each Application since this completed Application for Access document will become part of the contract agreement with the individual Receiving Organization.
          Applications are processed as they are received, but the set of Applications and project proposal is not reviewed until Applications have been received from all the Receiving Organizations).

Multiple Research Project Topics

In response to a single Call for Applications, a PPO can only submit one Application for Access. However, that Application can encompass several, separate topics of research. All of the research topics should be covered in Section C. There should be one overall research project title and responses to questions should encompass all the research topics for all questions except for Question 11 in Section C. Question 11 describes the proposed research and should be completed by answering the set of items for an individual topic, and then doing this for each topic in turn. For example, if a PPO is overseeing several students' doctoral research work, the students' research projects should all be covered in one application.

If there are Multiple Receiving Organizations, as discussed above, Sections B and C must be identical for all the Organizations.

4. Security

Overview

This section reviews security requirements that cover access control to the Data Portal, secure locations, and secure use of the data within the Data Portal. Users are required to maintain the confidentiality of all data within the Data Portal and to scrupulously follow all security protocols and policies. Users of the Data Portal must follow all the requirements of CIPSEA to protect the data and prevent disclosure of the identity of individual respondents. A disclosure review of statistical results must occur before any data or results are permitted to leave the Data Portal.

Only those persons (project team members) listed on the Application for Access to Confidential Data, who have completed confidentiality training and have a Designation of Agent and Affidavit of Nondisclosure form on file with CBHSQ or who are approved later through a formal approved amendment to the Agreement, are authorized to use the Data Portal. Only the data requested in your Application and approved as part of the signed Confidential Data Use and Nondisclosure Agreement can be used in your analysis.

As part of each Application, applicants must confirm that their computers and project offices meet the physical security requirements for computer set-up and locations as required in the Application and Agreement. All project team members must follow all security requirements for the duration of the project. In addition, confidentiality requirements for the data do not end at the completion of the project, but must continually be observed.

Data and Software in the Secure Data Portal

The Data Portal is a system that provides secure access to CBHSQ Confidential Data.

When a researcher logs onto the Data Portal, a separate Windows desktop opens within the researcher's own computer desktop. The Data Portal is connected to a server at ICPSR. The Data Portal is virtually isolated from the user's local, physical desktop computer. For each project team, there is a workspace with the directory of folders for the project. The workspace will contain the Confidential Data required for the user's specific research project. The project team may create their own folder sub-structure as needed within the overall project folder. A user will not be able access the content of any other researcher's project folders.

Providing access through the Data Portal minimizes the possibility that a researcher could inadvertently or purposefully release Confidential Data to unauthorized persons. The Data Portal prevents users from emailing, ftp'ing, copying, or otherwise moving files or information outside of the Data Portal or moving files or other data into the Data Portal, either accidentally or intentionally. It also blocks unauthorized access to the data from unauthorized persons.

Within the Data Portal, users can analyze data, write papers, and produce reports using their own computer, but it won't be possible to share information between the user's local computer and the Data Portal virtual computer.

The following software is provided in the Data Portal:

- SAS 9.3 including the Education Analytical Suite, SAS Enterprise Miner Client, SAS/GIS, and SAS/SPECTRAVIEW;
- SPSS 19 including the add-ons for Regression Models and Advanced Models;
- STATA 12;
- SAS-Callable SUDAAN 11.0.0;
- Stat Transfer 9;
- R (programming language only; no modules); and
- Microsoft Office 2010 (Access, Excel, InfoPath, OneNote, PowerPoint, Publisher, and Word).

Users can write their own programs within the Data Portal using the software available. Users will not be able to import programs into the Data Portal. If a project team needs to use their own previously developed analysis program, the program will need to be submitted to the Data Portal user support group with a request to move it into the project team's Data Portal folder. However, this needs to be described in the Application along with any other software needed which is not provided in the Data Portal.

Security Requirements

Access Control

Under no circumstances, can any unauthorized person be allowed to access the Data Portal.

Login. The access control procedures at login verify the IP address, username, and password. Only the desktop computer at the approved IP address (or within approved range of addresses for organization) can be used to login to the Data Portal. (Other IP addresses are blocked by a firewall protecting the Data Portal.) Only strong passwords[8] are allowed. The Data Portal will time out and lock after a few minutes of user inactivity. The user will be required to enter the password to unlock the Data Portal desktop. SAMHDA maintains audit logs for monitoring researcher behavior during data access and use.

Passwords. *Protect passwords.* Login credentials must be used correctly and not given to any person. A user's Data Portal password must not be shared with anyone else, either intentionally or through lack of security (such as using a saved password list outside the Data Portal in electronic or written form). Passwords cannot be shared with your IT support people. (You may

[8] When you change your password, your new password will be checked for strength by the ICPSR/University of Michigan IT system. The password must use nine or more characters, with characters in at least three of the following categories: lowercase letters, uppercase letters, numerals, and punctuation. It must not be a word or simple phrase or use parts of your name. For example, the user can make a strong, easy to remember password by using the first letters of the words in a phrase and converting some words to number as in "Four score and seven years ago our forefathers brought forth" is 4S&7yaofb4th. The user should also select a unique password for Data Portal use. Do not use a password that you currently use or one that was used for other past computing accounts.

contact your institution's IT staff if you need help installing the VMware client software before you access the Data Portal, but IT staff should never be allowed to access the Data Portal or view content within the Data Portal.)

MToken. An approved user will be issued an MToken. The MToken generates a random number that is used to login along with the user's login ID and password. This MToken must not be shared with anyone. If the MToken is lost, you must report it to dataportal@icpsr.umich.edu. When a team member leaves the project, the **MToken must be returned to SAMHDA**, ICPSR, University of Michigan, P.O. Box 1248, Ann Arbor, MI 48106-1248

Logoff or disconnect. If you are logged into the Data Portal and you leave your computer, you must "disconnect" or "logoff" from the Data Portal. (Disconnecting from the Data Portal will leave any open programs running, but closes the connection to the Data Portal. Logging off of the Data Portal closes the connection and terminates all programs that are running.)

Password-protected screensaver. The approved computer must have a password-protected screensaver installed and set to activate within 3 to 5 minutes of inactivity. However, automatic time outs or screensavers are <u>not</u> sufficient access control, as they leave the Data Portal open to access by others.

Security patches. The desktop computer must be maintained with security patches and up-to-date anti-virus software enabled.

Data cannot be moved in or out of the Data Portal. The Data Portal prevents users from emailing, ftp'ing, copying, or otherwise moving files outside of the secure environment, either accidentally or intentionally. The Data Portal prevents unauthorized access to data from outside persons by using secure access controls and firewalls.

If you become aware of any unauthorized access, use, or disclosure of Confidential Data, whether suspected or actual, this unauthorized access, use, or disclosure of Confidential Data must be reported <u>immediately</u> to CBHSQ and SAMHDA/ICPSR via phone call to CBHSQ (240-276-1273 and 240-276-1364) and SAMHDA (888-741-7242) followed-up with an email to CBHSQ (neil.russell@samhsa.gov and marna.hoard@samhsa.gov) and SAMHDA (dataportal@icpsr.umich.edu).

Secure Project Office and Computers

Only computers at the authorized IP addresses can access the Data Portal. These computers must be secure from access by unauthorized persons by being placed in a designated and approved Secure Project Office. The computer must be a desktop model and the internet connection must be hard wired. A wireless connection is not allowed for connecting to the Data Portal.

As part of the security Data Portal protocol, only computers using Windows can be used to access the Data Portal. (If Macs are allowed in the future, you can submit a request to modify your approved computer to include a Mac computer.)

The computer must be placed inside a Secure Project Office where only authorized persons can view the computer screen when data are displayed. You may add a second screen for your computer so that results are more easily viewed by one or more authorized persons at the same time. The screens must not be visible from outside the office by anyone.

The computer location must be within a walled office and be secured with a lockable door. No unauthorized persons are allowed inside the office when the data are in use. The office should be locked and the Data Portal should be locked when team members temporarily leave and do not logoff or disconnect from the Data Portal.

Use of a cubicle as a Secure Project Office is not allowed. (A project team can have more than one Secure Project Office, e.g., team members may work in separate Secure Project Offices.)

No telecommuting or remote access from unauthorized locations is allowed. Attempts to access the Data Portal through remote connection using an authorized computer, but from an unauthorized location is a serious violation and may result in penalties or denial of access for the person and/or the project team.

All conversations about the Confidential Data, analyses, and results must only be conducted among authorized project team members in a secure location. These discussions should only take place within the confines of the Secure Project Office where unauthorized persons cannot overhear the discussions. In general, these kinds of conversations must not be conducted in public locations where unauthorized persons could overhear such discussions.

Secure Use of Data

Analysis and use of data can only be done within the Data Portal. Recording data or results and then moving them outside of the Data Portal is not allowed. This means that no screenshots, photographs, or videos may be made of the displayed data or output. No copies of data may be made (e.g., no retyping or copying data, such as handwritten notes). In addition, cameras and other video equipment are not allowed to be present inside the Secure Project Office when the Data Portal is in use. Recording data or results and then moving them outside of the Data Portal is a serious violation and may result in penalties or denial of access for the person and/or the project.

Disclosure review and approval is required before any analysis results or findings can be released in any form or discussed outside the authorized project team. Without a disclosure review and approval from SAMHDA/ICPSR and CBHSQ, you cannot share or discuss the data or results with unauthorized persons.

You can discuss the type of research you are doing, e.g., the hypotheses you are testing, with others outside your authorized project team, but you cannot discuss any data or results, due to potential disclosure risk.

Authorized persons can discuss general questions with the SAMHDA user support team at SAMHDA/ICPSR or the SAMHDA COR if requested to do so as part of user support or to report a disclosure issue. However, never send any information with Confidential Data through email, even if reporting a disclosure issue.

5. Disclosure Review Process: Safeguarding Confidentiality

Overview

Analysis results must go through the disclosure review process at SAMHDA/ICPSR and CBHSQ before they can be discussed or viewed by anyone who is not on the project team as listed in the Application. After analysis is completed, the program results, report, or presentation files created within the Data Portal must undergo a disclosure review to assess output for disclosure risk. The purpose of the disclosure review is to protect respondent confidentiality. It is not a review of research quality or findings.

Only near-final results intended for publication or presentation should be submitted for disclosure review. Analysis results remain in the Data Portal until the disclosure review process has been completed. Since, users cannot export any files or documents out of the Data Portal, SAMHDA will deliver results (cleared during the disclosure review process) to the project team for use outside the Data Portal. Only after disclosure review approval has been obtained can results be discussed, reviewed, presented, or released to persons outside of the authorized project team.

Disclosure

Disclosure occurs if it is possible from the analysis or results to determine the value of some characteristic of an individual entity. Identification may occur when data are combined with other data sources. Identification may also occur in aggregated statistics. For example, a table cell that includes only one respondent in combination with other knowledge could make identification possible.

Key rule: Do not attempt to identify an individual respondent (e.g., whether person, organization, or establishment.) You must immediately report inadvertent identification or disclosure of Confidential Data to SAMHDA and CBHSQ.

In addition to the penalties associated with CIPSEA, any violation of Federal law or the terms in the Agreement may be reported to the Research Integrity Officer, Institutional Review Board, or Human Subjects Review Committee of the user's institution. A range of sanctions are available to institutions including revocation of tenure and termination. If the confidentiality of human subjects has been violated, the case may be reported to the Federal Office for Human Research Protections. This may result in an investigation of the user's institution, which can result in institution-wide sanctions including the suspension of all research grants.

Guidelines for Researchers to Avoid Disclosure

- Limit analyses to those proposed and approved in your Application.
- Avoid analyses involving small sample sizes (e.g., cells with less than 5 respondents). It is better to combine small groups rather than eliminating records from an analysis.
- Avoid creating tables that are very similar but with very small differences in categories used in the analysis.

- Do not report any unweighted sample size numbers except a limited number of overall sample size numbers rounded to the nearest 100.
- Do not report any unweighted percent distributions.

Preparing Your Analyses for Disclosure Review

- Use titles for each analysis being presented for disclosure review.
- Specify the dataset(s), variables, and sample/sub-sample from which the outputs have been derived. Describe how the output will be used (e.g., presentation, publication).
- Avoid submitting peripheral or interim output or documents for disclosure review, i.e., output or documents that will not appear in publication or be disseminated. While these kinds of output and documents can be produced, their use should be within the Data Portal. Also, release of these items may create complementary disclosure risks through the combination of information from different sources or sub-samples. Exploratory descriptive analysis, preliminary regression models, or draft papers are examples of peripheral output or documents which should not be submitting for a disclosure review.

Important note: The project team must consider the analyses and release of results in the context of the work of the entire project. The team may want to delay asking for disclosure review for results until a later date. For example, an early result that has been reviewed and cleared for release could cause a disclosure risk for subsequent results if both results were combined. Once analyses are approved for release, SAMHDA and CBHSQ assume approved results will be disseminated by the project team. So results approved for release could impact what else can be approved for later release.

Initiating Disclosure Review. If any project team members want to release results outside the project team, these results (whether a report or presentation files) are placed into the "FOR SAMHDA REVIEW" folder for disclosure review. These files are then reviewed by SAMHDA staff, a Disclosure Review Board, and CBHSQ staff. The PPO sends an email to dataportal@icpsr.umich.edu requesting a disclosure review for the file named in the review folder.

Release of Results from the Data Portal. Once the results are approved, the files and/or edited version of files are deposited into the folder "SAMHDA REVIEW COMPLETED." Since users cannot export from the Data Portal, SAMHDA will deliver approved results to the PPO usually via email.

Disclosure review. SAMHDA will work with CBHSQ to identify any disclosure risks in the results or documents. CBHSQ will make the final determination regarding final approval for release. The determination of the presence of disclosure risks will not focus on scientific merit or policy relevance of the analyses. If CBHSQ determines there are disclosure risks, the researcher is not authorized to publish or disseminate the results. CBHSQ's decision is final.

Researchers who avoid the disclosure review process and use or publish data outside of the Data Portal without CBHSQ approval commit a serious violation of the Agreement. Such violations may result in penalties or denial of data access for the person and/or the project.

6. Site Inspection

Based on CIPSEA requirements, CBHSQ will conduct announced or unannounced site inspections during the period that project researchers have access to the data. A site inspection of the project team members' site(s) is to assess and ensure compliance with the provisions of the Agreement. This also includes an assessment of the current status of the project.

The site investigator will review the project operations and security procedures with the Principal Project Officer, or other senior project team member (as listed in the Application).

The inspector will review the names and status of all project team members. All project team members must have a signed, notarized Designation of Agent and Affidavit of Nondisclosure form on file with SAMHDA (see Checklist for Application in Section 3.) This review is to confirm that SAMHDA and CBHSQ have the most current information on file for those individuals who are authorized to access the data.

The investigator will check to ensure that the Application, Agreement, Affidavits and training materials have been reviewed by all project team members. All project team members must know and understand all of the security procedures required for accessing Confidential Data.

Violations

Statement of Warning. If the investigator finds the site to be noncompliant where an unauthorized disclosure could occur, CBHSQ will send a Statement of Warning to the PPO within two weeks (10 working days) of the site inspection. (More serious violations may result in immediate revocation of Data Portal access and/or criminal prosecution.) The PPO and project team has one week (5 working days) from receipt of the Statement of Warning to remedy the violations, and to send a response to the CBHSQ describing the remedies and results.

Any violation found through the site inspection may subject the PPO and project team members to immediate denial of Data Portal access or a report of the violation to the U.S. Attorney. Penalties, fines and imprisonment, may be enforced for each occurrence of such violations.

Revocation of access. Any violation of the terms and conditions contained in the Agreement (and documents included by referral) may subject the project and research team members to immediate revocation of access to the Data Portal. If violations are discovered, CBHSQ will notify the PPO in writing of the factual basis and grounds for revocation. CBHSQ shall provide written notice of a decision to the PPO after receipt of the PPO's written argument.

Most Common Violations

- No three to five minute shutdown through use of a password protected screensaver
- Attempting to access Confidential Data from an unauthorized location
- PPO not maintaining control over access to the Confidential Data
- PPO neglecting to inform CBHSQ of any project personnel changes

- Making use of or copying the Confidential Data and taking it outside of the Data Portal before a disclosure review is conducted
- Discussing Confidential Data in non-secure locations
- Not locking the Secure Project Office when project team members temporarily leave the office
- Allowing unauthorized persons to view any information displayed in the Data Portal when it is in use

Prosecution and Penalties. Alleged violations of the Privacy Act of 1974 or CIPSEA are subject to prosecution by the United States Attorney after first making reasonable efforts to achieve compliance.

Any violation of the terms of the Agreement and Affidavits (and other documents included by referral) may also be a violation of Federal law under the Privacy Act of 1974 (5 U.S.C. 552a) and may result in a misdemeanor and a penalty of up to $5,000.

Anyone violating the confidentiality provisions of CIPSEA by making an unauthorized disclosure of the Confidential Data could be found guilty of a class E felony and be imprisoned for up to five years, and/or fined up to $250,000.

7. Modifications to the Application

The PPO shall keep CBHSQ informed of any modifications in project operations, conditions, or location that would alter what was described in the Application throughout the span of the Agreement period. Requests for modifications to the original Application must be submitted by the PPO to CBHSQ. All correspondence with CBHSQ and SAMHDA must be initiated by the PPO.

MODIFICATIONS AT ONE RECEIVING ORGANIZATION

Adding Team Members to the Project

A PPO may request the addition of new project team members by submitting the name and contact information to SAMHDA. CBHSQ will determine if the person is eligible. If the person is eligible, SAMHDA will then conduct training, and obtain the signed and notarized Designation of Agent and Affidavit of Non-disclosure from the new team member. SAMHDA will notify the PPO if the new team member is authorized for access to the data.

Departing Team Members

The PPO will notify SAMHDA and CBHSQ in writing of changes in the Research Staff. CBHSQ shall be informed 6 weeks prior to a team member's departure when a person will no longer be working on the project. Research Staff separation from the Receiving Organization will lead to the termination of their access to the Data Portal.

Change in PPO

The PPO will notify CBHSQ in writing in the event the PPO plans to separate from the Receiving Organization during the Contract Period, at least 4 weeks prior to the last day on the project. PPO separation from the Receiving Organization will lead to the termination of access to the data for the entire research team at that Receiving Organization, unless the Receiving Organization identifies and obtains CBHSQ approval of a new PPO.

The Receiving Organization will obtain approval from CBHSQ prior to transferring the Agreement to another PPO at the same Receiving Organization. In order to obtain such approval, the PPO must inform CBHSQ in writing 6 weeks prior to the proposed date of transfer, submit a complete copy of the Agreement signed by the Receiving Organization Representative and the new PPO, and maintain responsibility for the Computer and Data Security requirements until the transfer Agreement has been approved by CBHSQ.

MODIFICATIONS FOR OVERALL PROJECT

Agreement Extension

If an extension of time is needed, the Primary Contact from the Application process must submit a written request to CBHSQ and SAMHDA 3 months prior to the end of Agreement time period

with a justification for the additional time. Any modifications in the scope of the original project must be explicitly described in the extension justification.

Change in Research Plan or Computer Environment

If during the course of research there are needed changes to research plans or in the computer environment that is different from the information originally submitted in the Application, different from that which is required in the Agreement, and/or is different from that the Computer and Data Security Requirements in Appendix B of the Agreement, then the PPO must send CBHSQ a copy of the revised materials and a memorandum describing the changes. These revisions will be considered amendments to the Agreement and may not be implemented until written approval is obtained from CBHSQ.

8. Closing out a Project

Project Archive

Prior to the end of the project, SAMHDA will send an e-mail to the PPO (or Primary Contact if multiple Receiving Organizations) notifying the project team to create an archive folder. The email will have the instructions for the required format for items in the archive folder (e.g., syntax/code, output, notes, and minimal data due to space limitations). The e-mail will request acknowledgement by the PPO of the receipt of the e-mail.

The PPO then prepares the archive folder and then sends an email to dataportal@icpsr.umich.edu that the archive folder is ready.

The archive folder is moved to the Archive location. The project folder on the Data Portal is deleted. Access to the Data Portal is removed for all members of the project team.
After three years, a courtesy e-mail is sent to the PPO prior to permanently deleting the archived folder.

If access is required by the project team to the material in the archive folder during the archive period, the PPO or other team member sends a request to dataportal@icpsr.umich.edu.

If the PPO and project team find that they need access to their Archive for longer than three years, they will need to submit a request prior to the end of the three year archive period and the reason for the extension. If the request is approved, access will be allowed for the additional approved period.

Confidentiality

Confidentiality requirements for the data do not end at the completion of the project, but must continually be observed.

Publications

Any publications based on the Confidential Data must cite the data source. The citation or the actual final publication must be sent to dataportal@icpsr.umich.edu.

Only material or results that have been approved for release by CBHSQ (after a disclosure review and approval) can be used or referenced outside the Data Portal.

9. Responsibilities

The PPO, research team members, CBHSQ, and SAMHDA have separate and shared responsibilities for project support, communication, and ensuring that all security and confidentiality requirements are met and implemented.

Primary Contact Responsibilities (in addition to being a PPO)

- Responsible for the Application process phase with SAMHDA and CBHSQ.
- At the end of the project, the Primary Contact prepares the archive folder and notifies dataportal@icpsr.umich.edu that the archive folder is ready.

PPO Responsibilities (in addition to being team member)

- Serve as a liaison between CBHSQ and all project team members at the PPO's Receiving Organization.
- Follow all security procedures as outlined in the *Data Portal Confidentiality Procedures Manual*, Training Materials, Affidavits, and the Agreement.
- Inform CBHSQ and Primary Contact of any willful or inadvertent violations of the provisions set forth in the above stated documents.
- Ensure that all team members included in the Application follow the guidelines established by CBHSQ for access to the Confidential Data.
- Serve as a liaison between the Primary Contact and all project team members.
- Inform CBHSQ and Primary Contact if he/she (PPO) will be moving to another organization 6 weeks prior to the move.
- Inform Primary Contact and CBHSQ as soon as possible when staff are to join the project. The new project staff will need to be approved by CBHSQ prior to their access to the data.
- Notify CBHSQ and SAMHDA immediately of any legal, investigatory or other demand for the Confidential Data.
- Make sure all project work is compliant with the requirements established in the Agreement (including other documents by referral).
- Provide all publications, presentations, and reports that use Confidential Data to CBHSQ for a disclosure review prior to disseminating them outside of the Data Portal.
- Report loss of a MToken to dataportal@icpsr.umich.edu.
- At the end of the project, the Primary Contact prepares the archive folder and notifies dataportal@icpsr.umich.edu that the archive folder is ready.
- At the end of the project, all MTokens issued to project team members must be returned to SAMHDA, ICPSR, University of Michigan, P.O. Box 1248, Ann Arbor, MI 48106-1248.

Project Team Member Responsibilities

- Follow all security procedures as outlined in the *Data Portal Confidentiality Procedures Manual*, Training Materials, Affidavits, and the Agreement.

- Inform the PPO and CBHSQ of any willful or inadvertent violations of the provisions set forth in the above stated documents.
- Inform the PPO of any plans to depart the project team at least 6 weeks before leaving the project.
- Report loss of a MToken to dataportal@icpsr.umich.edu.
- Return the MToken to SAMHDA, ICPSR, University of Michigan, P.O. Box 1248, Ann Arbor, MI 48106-1248 when team member leaves project.

CBHSQ Responsibilities

- Accept, review, and approve or disapprove all Applications for data access. Communicate with requestor to clarify any issues as needed.
- Help to determine scope of project-specific Confidential Data files. CBHSQ will work with requestor to determine the content of a limited set of variables that are within the scope of the project as described in the Application.
- Help to evaluate Application materials related to access to the Confidential Data.
- Develop annual confidentiality training for all agents.
- Maintain Affidavits, track new and departing staff on all projects, and monitor data access expirations and renewals.
- Conduct or delegate site inspections.

SAMHDA Responsibilities

- Maintain the Data Portal.
- Manage user Data Portal accounts.
- Provide user support for the Data Portal.
- Provide annual confidentiality training for all agents.
- Retain Archive folder of project files provided by Primary Contact for 3 years after the end of the Agreement.

Glossary

Agent: An agent is a person designated by CBHSQ to perform statistical activities authorized by law (e.g.: CIPSEA) as specified in a written legal agreement under the supervision or control of CBHSQ staff. Agents agree in writing to comply with all provisions of law that affect the activities conducted on behalf of the agency. Agents are a PPO and all other project team members.

Center for Behavioral Health Statistics and Quality (CBHSQ): The Substance Abuse and Mental Health Services Administration (SAMHSA), Center for Behavioral Health Statistics and Quality collects and reports on national and State data to assist policymakers, treatment providers and patients to make informed decisions regarding the prevention and treatment of mental and substance use disorders. More information can be found at http://www.samhsa.gov/about/cbhsq.aspx.

Confidential Data: CBHSQ Confidential Data do not contain direct identifiers, but the data likely contains information that might lead to respondent identification. Thus, the data are confidential and are not released to any person outside CBHSQ without appropriate legal agreements and other documents in place. Confidential data files may contain more variables, such as demographic and geographic variables, and larger samples than the public-use files. Confidential data are only accessed through the Data Portal. All security requirements for accessing the Data Portal and use of the data must be followed. No data, analyses, or results based on the Confidential Data can be released in any form without a disclosure review and approval by CBHSQ/SAMHDA. Releasing results before a disclosure review is completed is a violation of the terms of the Agreement and as such is subject to penalties.

Confidential Data Use and Nondisclosure Agreement: This is the legally binding contract used by CBHSQ to authorize access to Confidential Data through the Data Portal. The Agreement specifies the obligations imposed on the signatories and the procedures and security requirements that must be followed to protect the data.

Confidentiality and Information Protection and Statistical Efficiency Act (CIPSEA): CIPSEA is Title V of the E-Government Act (P.L. 107-347) and provides strong confidentiality protections for statistical information.

Contracting Officer's Representative (COR): A Federal employee appointed in writing and delegated limited responsibilities by a Contracting Officer (CO) to perform specified contract management duties related to technical oversight and administration of a specific contract.

Data Portal: The secure computer environment used by authorized users for remote access to Confidential Data. The Data Portal is part of SAMHDA/ICPSR and was developed under the contract with CBHSQ/SAMHSA.

Designation of Agent and Affidavit of Non-disclosure: A form that is completed by a person who will have access to Confidential Data. This form contains: (1) the wording of an oath not to disclose such information to persons not similarly sworn, (2) a description of the penalties for such disclosure, and (3) a section for signature and imprint of a notary public.

Direct identifiers: Direct identifiers include information such as names, addresses, social security numbers and phone numbers that can be used to specifically identify a responding entity.

Disclosure: The release of confidential information to any unauthorized person.

ICPSR: The Interuniversity Consortium for Political and Social Research. It is a center within the Institute for Social Research at the University of Michigan.

Indirect Identifiers: Indirect identifiers include data such as local geography, detailed racial-ethnic characteristics, or other characteristics, when used together could potentially lead to the disclosure of a responding entity's identity.

Individually Identifiable Information: Identifiable information refers to information that can be used to establish individual or establishment identity, whether directly—using items such as name, address, or unique identifying number—or indirectly—by linking data about respondents with external information that directly identifies them.

Nonstatistical Use of Data: Using the data in identifiable form in a way that would affect the rights, privileges, or benefits of a responding entity. Examples of a nonstatistical use of the data include using the data for an administrative, regulatory, law enforcement, or judicial purpose; and releasing the data through a Freedom of Information Act (FOIA) request.

Principal Project Officer (PPO): The PPO is the researcher in charge of the day-to-day operations at a Receiving Organization involving the use of the Confidential Data. This person will be the point of contact for the Receiving Organization to coordinate with CBHSQ and SAMHDA. The PPO signs the Confidential Data Use and Nondisclosure Agreement.

Primary Contact: The Primary Contact is the PPO who coordinates and is the main point of contact for the Application process. The Primary Contact is responsible for the liaison with CBHSQ.

Public-use File (PUF): Public-use data files are data files prepared by CBHSQ with the intent of making them available to the public without restrictions. CBHSQ public-use data files may not contain all variables, cases or any direct identifiers, and may have undergone other procedures to limit the risk of disclosing a respondent's identity.

Recertification: The process of annual confidentiality training and signing a Designation of Agent and Affidavit of Nondisclosure to ensure agent's continued understanding and implementation of security procedures as required by the Agreement.

Receiving Organization Representative (ROP): The ROP is the individual who has the legal authority to bind the organization to a contract or data use agreement. The ROP is responsible for signing the legally binding documents required for approval to access Confidential Data. With his/her signature, the ROP certifies that: (1) the organization has the authority to undertake the commitments in the Confidential Data Use and Nondisclosure Agreement and (2) *he/she has the authority to legally bind the organization to the provisions of the Agreement.*

SAMHDA: the Substance Abuse and Mental Health Data Archive that is housed at ICPSR under contract with CBHSQ.

Statistical Use of Data: Using data for statistical purpose includes the description, estimation, or analysis of the characteristics of groups, without identifying the individuals or organizations that comprise such groups. It includes development, implementation, or maintenance of methods or procedures to support these purposes. Making policy- or program evaluation-related decisions based on aggregated data that do not identify or specifically target the individual respondents is a statistical use.

APPENDICES

Appendix 1

Application for Access to Confidential Data

The Center for Behavioral Health and Statistical Quality (CBHSQ), Substance Abuse and Mental Health Services Administration (SAMHSA) has developed the Data Portal for accessing CBHSQ Confidential Data. The Data Portal is accessed via the web through the Substance Abuse and Mental Health Data Archive (SAMHDA). SAMHDA is located at the Inter-university Consortium for Political and Social Research (ICPSR), Institute for Social Research, University of Michigan (UM).

INSTRUCTIONS: Please use this application to apply for access to CBHSQ Confidential Data. You will need to describe your research project, specify the data you need, list all members of your project team, and describe the Secure Project Office(s) where the data will be accessed. Please see the *Data Portal Confidentiality Procedures Manual* for more information and requirements. Applications must be submitted on paper as original signatures are required. The *Manual* and other information about the Data Portal is available at www.icpsr.umich.edu/icpsrweb/content/SAMHDA/dataportal.html

WHO CAN APPLY FOR ACCESS TO CONFIDENTIAL DATA?

CBHSQ provides Confidential Data only to qualified organizations in the United States. Individual researchers must apply through a recognized organization (e.g., a government agency, university, or research organization). An Application for Access will only be considered if it is submitted by the Call for Application deadline.

The Principal Project Officer (PPO) will serve as the primary project contact person at the Receiving Organization. The Receiving Organization Representative (ROP) is an individual who has the legal authority to bind the organization to a contract. A ROP must sign the legally binding contract (i.e., data use agreement) prior to access to CBHSQ Confidential Data.

The PPO must be directly employed at the Receiving Organization (i.e., they cannot be a contractor, temporary employee, visiting professor or outside consultant to the Receiving Organization). Research Staff must be directly employed by or students currently enrolled at the Receiving Organization. At institutions of higher education, the PPO must have an advanced degree (e.g., Ph.D., J.D., M.D. or Ed.D.). Usually PPOs serve as principal investigators of research projects or sponsor Ph.D. students conducting dissertation research. Graduate students may not apply for access and must find a qualified faculty member to apply on their behalf.

The Receiving Organization headquarters, related business offices, and/or research site locations must be located in the 50 United States or District of Columbia. An Application will not be approved if the Receiving Organization's place of business is within a private residence.

If there are multiple Receiving Organizations, then a PPO at one of the Receiving Organizations must be designated on the Application for Access as the Primary Contact for the overall project.

The maximum number of persons who may have access to the Confidential Data during the project is limited to ten (10). This includes the PPO and Research Staff combined and for projects that span across multiple organizations.

The Application must clearly outline the nature of the proposed research project as well as the specific information and categories of variables needed and how this information will be used. Only the data requested in your application and approved as part of the signed Agreement will be provided for your use in the Data Portal.

RECEIVING ORGANIZATIONS

The Principal Project Officer (PPO) will serve as the contact person for the project at an individual Receiving Organization and signs the Application for Access for that Receiving Organization. The Receiving Organization Representative (ROP) is an individual who has the legal authority to bind the organization to a contract. As the legal representative of the Receiving Organization, only the ROP may sign the contract required for access to CBHSQ Confidential Data. A project may involve one organization with multiple locations or multiple Receiving Organizations. Each situation is described below with instructions on how to complete the Application for Access.

- Single Receiving Organization. If your project involves one organization with researchers at one or more locations, and the organization is represented by a single Receiving Organization Representative, then there is one PPO and one Receiving Organization for your project. The PPO is also the Primary Contact with SAMHDA and CBHSQ for the project. You will need to complete only one Application for Access, which lists the researchers for each location. Each location must also be identified and described.

- Multiple Receiving Organizations. If your project involves multiple collaborators at different Receiving Organizations:

    - Each Receiving Organization will need to have a separate PPO and a separate Application for Access.

    - One of the PPOs must be designated as the Primary Contact with SAMHDA and CBHSQ for the overall project. The Primary Contact coordinates the Applications from the Receiving Organizations, including the content of Section B (which lists all the Receiving Organizations involved in the project) and Section C (which contains the research proposal and data request).

- Responses for Sections B and C must be identical for applications from all of the Receiving Organizations. So either…
    - Applications for all the Receiving Organizations are sent to SAMHDA in one package, including (i) Application sections for each Receiving Organization that are specific to the Organization (i.e., Section A, signature page, and curriculum vitae) and (ii) one copy of Section B and C.
      This option is preferred as it facilitates processing and review of the Application, but is not required.
      Or
    - Each Receiving Organization submits its own application separately. The PPO of each Receiving Organization inserts the same Section B and Section C content as coordinated and provided by the Primary Contact. This information must be included in each Application since this completed Application for Access document will become part of the contract agreement with the individual Receiving Organization.
      Applications are processed as they are received, but the set of Applications and project proposal is not reviewed until Applications have been received from all the Receiving Organizations.

Multiple Research Project Topics

In response to a single Call for Applications, a Primary Contact can only submit one Application for Access. However, that Application can encompass several, separate topics of research. All the research topics should be covered in Section C. There should be one overall research project title and responses to questions should encompass all the research topics for all questions except for Question 11 in Section C. Question 11 describes the proposed research and should be completed by answering the set of items for an individual topic, and then doing this for each topic in turn. If there are Multiple Receiving Organizations, as discussed above, Sections B and C must be identical for all the Organizations.

SECTION A. Information for Your Receiving Organization

Name of Receiving Organization	

PROJECT TEAM

1. **Principal Project Officer (PPO) Contact Information**

Name of PPO	
Title	
Department (if applicable)	
Organization Name	
Organization URL	
Phone	
Fax	
Email	
Work Site Street Address	*(physical location—also include building name, room number)*
Mail Address	*(for mail/package delivery by USPS)*
Courier Address	*(for package delivery by courier)*
Federal Employee?	☐ Yes ☐ No

2. **Contact Information for Project Team Members**:

Please complete the following information for each additional project team member.

Note: The maximum number of researchers for the project (including all Receiving Organizations) is limited to 10.

(i) Team Member

Name of Team Member	
Title	
Department (if applicable)	
Organization Name	
Organization URL	
Phone	
Fax	
Email	
Work Site Street Address	*(physical location—also include building name, room number)*
Mail Address	*(for mail/package delivery by USPS*
Courier Address	*(for package delivery by courier)*
Describe the person's role on the Project Team:	
Is this person a Federal Employee? □ Yes □ No	

Additional Team Members: Copy all items from the table above into the space below and fill in for each additional team member.

Receiving Organization Representative (ROP)

3. **Contact Information for the Receiving Organization Representative** (only those persons who are authorized to sign contracts on behalf of the organization should be listed here):

Name	
Title	
Department (if applicable)	
Receiving Organization Name	
Organization URL	
Phone	
Fax	
Email	
Work Site Street Address	*(physical location—also include building name, room number)*
Mail Address	*(for mail/package delivery by USPS)*
Courier Address	*(for package delivery by courier)*
Federal Employee?	□ Yes □ No

Organization Certification Number

4. If you are employed at an organization that has a current NIH Multiple Project Assurances (MPA) Certification Number or Federal Wide Assurances (FWA) Certification Number, please provide this number and expiration date. (Once you provide this number and date, you do not need to respond to question number 5 below.)

MPA Number:

FWA Number: Expiration Date of MPA/FWA Certification Number:

5. If your organization does NOT have an NIH Multiple Project Assurances (MPA) Certification Number or Federal Wide Assurances (FWA) Certification Number, please answer the following questions:

a. Please describe your organization in detail. Include the type of organization, profit/non-profit status, and primary sources of revenue.

b. What is (are) the source(s) of funding for the specific research (described above) that will use these Confidential Data? (List name of funding organization, whether funds are provided as a grant, contract, or other mechanism.)

c. Does your organization have policies regarding scientific integrity and misconduct or human subject research that cover the secondary analysis of data? If so, please describe these policies and provide any applicable website.

NOTE: Any required IRB approvals for your project must have been received by the time this application may be approved.

Summary of Experience and Curriculum Vitae

6. (i) Please summarize the experience that team members at your Receiving Organization have in using Confidential Data on other projects.

(ii) Also, please attach **current curriculum vitae** at the end of the Application for each project team member listed in question 1 and question 2 above.

Security: Software, Secure Project Offices, Locations, and Computers

7. Required software. To be able to connect to the Data Portal you will need to use VMware software. You can download and install free VMware View Client software from the University of Michigan (UM) website. Please check with your IT group that your organization either has VMware View Client available or will allow the download of VMware View Client from the UM site. Please check the appropriate answer:

☐ Your Receiving Organization has VMware View Client available for your Secure Project Office computer(s). You will need VMware View Client version 5.3.

☐ Your Receiving Organization will allow the download for your Secure Project Office computer(s).

8. Secure Project Office. Please describe the Secure Project Office location(s) and computer(s) at your Receiving Organization using Tables 8A and 8B below.

Users cannot access data from off-site locations such as a home office. The Data Portal can only be accessed from desktop computers within approved Secure Project Office(s). These locations will be verified as part of a site inspection if your application is approved.

As part of the security protocol for the Data Portal, currently only computers using Windows can be used to access the Data Portal. (If Macs are allowed in the future, you can submit a request to modify your approved computer list to include a Mac computer.)

Note: Secure Project Office requirements are covered in the *Data Portal Confidentiality Procedures Manual*. Also, in Appendix B in the Manual is a list of computer and data security requirements and procedures that are required to be implemented as part of the Confidential Data Use and Nondisclosure Agreement (CDUNA). A Secure Project Office must meet all the requirements listed in the *Manual* and the CDUNA.

Table 8A. Secure Project Office Location(s). List all office locations where users will access the Data Portal. Provide exact locations including street address, building names and room numbers. (Add more rows as needed.)

Table 8A. SECURE PROJECT LOCATIONS		
Location	**Street Address Building name Room number**	**Please describe the overall building and the office area(s) security where the Secure Project Office(s) are located (e.g., are employees required to swipe ID cards or show ID upon entering the building?)**
Location 1		
Location 2		
Location 3		

Table 8B. Computers and team member access. List all computers to be used during the project for access to the Data Portal. (Add more rows as needed.)

NOTE:
Column 4 and last row. TEAM MEMBER ACCESS
All team members (including PPO) must be listed in Table 8B.

- *Access is needed.* If a person will need to login in to the Data Portal (e.g., to analyze, create, read, or review data or reports in the Data Portal) then a Secure Project Location and computer information must be provided for the person in Table 8B so that access can be set up to the Data Portal for that individual.
- *Access is not needed*. If a person will not require access, then list the person in the row labeled "Access to Data Portal is not needed for team members listed at right."

When determining whether access is needed for a team member, keep in mind that…

All data and results remain in the Data Portal unless they have been cleared for release by CBHSQ as the result of a disclosure review.

- When an authorized team member is logged in, other project team members also in the Secure Project Office can view results on the computer screen--but a team member will not be able to login directly to see results unless they have their own Data Portal user account.
- You must not take notes on data or results from Confidential Data within the Data Portal, whether handwritten or otherwise, unless that information has been cleared for release by CBHSQ.

Column 5. IP ADDRESSES.
Every computer connecting to the Internet has a unique IP (Internet Protocol) address assigned to it.

Your computer may connect through a fixed IP or your organization may assign an IP address from a fixed range of IP addresses. The IP addresses listed in Table B must be provided in the form of a public facing IP addresses. Commonly used forms of IP addresses that are not public facing but rather are internal organizational addresses begin with "192.168.", "172.", or "10.".

Please contact your IT group to verify what your public facing IP address or range of addresses is for the computers you will use. Ask them the following questions:
1. Are you using NAT [network address translation]? If so what is the public-facing IP?
2. If not, are you using a static IP? If so, what is the static IP?
3. If not, are you using DHCP (Dynamic handling)? If so, what is the full range (subnet) for this computer)? (However, we prefer fixed IP addresses rather than ranges. Please also ask your IT group whether the project computers can each be assigned a fixed IP address.)

Table 8B. COMPUTERS TO BE USED BY TEAM MEMBERS TO ACCESS DATA PORTAL				
1. Secure Project Location: (Enter the line number from Table A.)	**2. Computer Brand, Model Number, and Serial Number.** (Must be a desktop computer.)	**3. Operating system: enter version of 'Windows'**	**4. Team member(s) who will use this computer to login to Data Portal**	**5. IP Address for computer (or range of addresses)**

ACCESS TO DATA PORTAL IS NOT NEEDED FOR TEAM MEMBERS LISTED AT RIGHT:	

SECTION B. Receiving Organizations

If there is only one Receiving Organization involved in this project, skip to Section C.

If there are multiple Receiving Organizations, the Primary Contact should respond to item 9, and send the completed version of Section B to PPOs at other Receiving Organizations, who will then include that completed Section B version in the Application for the individual Receiving Organization.

9. If there are multiple Receiving Organizations involved in this project, which PPO will serve as the Primary Contact for the project overall?

Name of Primary Contact	
Receiving Organization of Primary Contact	

For **each** Receiving Organization, please list the name of the organization and the contact information for the PPO at all the organization(s). List the Receiving Organization of the Primary Contact first. Then please copy the table as needed and fill in the PPO contact information for each additional Receiving Organization.

Receiving Organization(s):

Name of PPO	
Title	
Department (if applicable)	
Organization Name	
Organization URL	
Phone	
Fax	
Email	

Section C. Proposed Research Project Information

Note: If there is more than one Receiving Organization involved in a project, the content of Section C must be identical for all Applications from Receiving Organizations involved in the project. So the Primary Contact coordinates with all the Receiving Organizations to create the content of Section C. The Primary Contact sends the completed Section C to PPOs at the other Receiving Organizations so they can include it in their individual Applications for the project.

10. Title of research project.

Project title:	

11. Research Project Description. Please describe the research project including the research questions and analysis/statistical methodology to be used for the project. In your description, please answer each item below separately labeled by item letter and topic.
If you are proposing separate, multiple research topics, you will need to describe each research topic by answering the set of items below for each individual topic.

a) research or policy questions being addressed;
b) research plan--hypotheses, analyses, and statistical models;
c) potential significance and application of the results;
d) relevance of the research to DHHS and SAMHSA missions to reduce the impact of substance abuse and mental illness on America's communities;
e) feasibility of the research given the data and resources available;
f) approximate sample sizes you will need for your analyses;
g) disclosure considerations and how the project will address them;
h) related experience of the PPO and project team members; and
i) relationship of past work and publications by the project team to the proposed research

12. Time Period. What is the proposed period of time you will need access to the Data Portal for your project? Please respond to all questions.

(i) What is the expected start date for the project?
(ii) What is the expected period of time you will need access to the Data Portal?
(iii) Do the project, and/or the start and end dates, depend on other approvals that the Receiving Organization(s) will need (e.g., contract or grant approvals)?

13. Software availability. While working with the Confidential Data you can only use software that is provided within the Data Portal. Note: **All the software listed below in the table is automatically provided in the Data Portal.**

a. For our information, please put an X in front of each software package you plan to use, and put an X in second column to indicate in which format(s) you would like the data files:

Plan to Use?	Data format needed	Software Package
		SAS 9.3 which includes the Education Analytical Suite; SAS Enterprise Miner Client, SAS/GIS, and SAS/SPECTRAVIEW
		SPSS 19 with add-ons for (a) Regression Models and (b) Advanced Models
		Stata 12
		SAS-Callable SUDAAN 10.0.1
		R 2.11.1
		StatTransfer 9
		Microsoft Office 2010 (Access, Excel, InfoPath, OneNote, PowerPoint, Publisher, and Word).

b) If you need software that is not listed above, please describe the software (title and version) and describe why it is needed and how it will be used:

14. Use of results. D**esc**ribe how you intend to use the results of the research, including plans for public dissemination (e.g., journal publication, conference paper presentations). Note that results can only be publicly disseminated after they undergo a disclosure review and are cleared for release by CBHSQ.

Data Request

The data requested must encompass the research across all organizations involved in the project.

- If there is only one Receiving Organization for the project, the PPO submits the data request as part of the Application for Access.

- If there are several PPOs (each from a different Receiving Organization) working on the project, then the PPO listed in item 9 as the Primary Contact coordinates the creation of an overall, combined data request for all the Receiving Organizations.

15. Need for Confidential Data. State the reasons why the NSDUH and/or DAWN data in the public-use data file(s) and the Restricted-use Data Access System (R-DAS) are not adequate for conducting your research. Also, state why your research project can only be conducted using the Confidential Data.

For those requesting NSDUH data. In addition to your reasons for needing the confidential data, there are several birthdate and geographic variables that are not automatically provided to approved data portal applicants. These variables are listed in Q16(ii)(b), and you can use the table in Q16 to explain why those specific variable(s) are needed for your research.

Note: For information on the public-use files and R-DAS go to www.datafiles.samhsa.gov.

16. Data Request for **National Survey on Drug Use and Health (NSDUH)**

(i) ☐ 2008-2012 NSDUH Adult Clinical Interview Data

(ii) **Survey Years.**

(a) Check the box for the survey years you are requesting:

☐ 2004 National Survey on Drug Use and Health
☐ 2005 National Survey on Drug Use and Health
☐ 2006 National Survey on Drug Use and Health
☐ 2007 National Survey on Drug Use and Health
☐ 2008 National Survey on Drug Use and Health
☐ 2009 National Survey on Drug Use and Health
☐ 2010 National Survey on Drug Use and Health
☐ 2011 National Survey on Drug Use and Health
☐ 2012 National Survey on Drug Use and Health

(b) **Restricted variables**. The NSDUH files for the Data Portal include data and variables not in the Public Use files. The following additional variables are not automatically provided within the Data Portal and must be requested specifically for your project. These additional variable requests are approved by CBHSQ separately based on your stated justification for research use.

Put an X in the first column for each variable you are requesting, and in the last column explain why the variable is needed for your research.

X	**Name of NSDUH Restricted Variable**	**Definition**	**Why is the variable needed for proposed research?**
	PXBMONTH	Birth month of child under 18, reported by the parent when parent and child were both surveyed.	
	PXBDAY	Birth day of child under 18, reported by the parent when parent and child were both surveyed.	

	PXBYR	Birth year of child under 18, reported by the parent when parent and child were both surveyed.	
	BRTHDATE	Exact birthday variable, long form string variable format (month, day, year	
	BIRMONTH	Exact birth month broken out into three numeric variables for month, day, and year.	
	BIRDAY	Exact birth day broken out into three numeric variables for month, day, and year.	
	BIRYEAR	Exact birth year broken out into three numeric variables for month, day, and year.	
	EIBDATE	An indicator variable to show which cases have birthday (BIRMONTH, BIRDAY, and BIRYEAR) edited via a computation or randomly assigned day based on respondents age and the interview date.	
	MTRACT	Majority census tract. In other words, the census tract that contains the majority of the sampling segment. In most cases, the entire sampling segment is entirely within a single tract, but not all.	
	TRACTIND	An indicator variable	

		identifying when the segment matches 1 tract only, and when a segment had to be assigned to a tract based on the tract containing the majority of the segment.	
	SEGID	Segment ID	
	LAT	Latitude of the centroid of the segment.	
	LONG	Longitude of the centroid of the segment.	
	ZIPCODE	Zipcode	

17. Survey Data Request for **Drug Abuse Warning Network (DAWN)**. Please check each survey year needed.

☐ 2004 Drug Abuse Warning Network
☐ 2005 Drug Abuse Warning Network
☐ 2006 Drug Abuse Warning Network
☐ 2007 Drug Abuse Warning Network
☐ 2008 Drug Abuse Warning Network
☐ 2009 Drug Abuse Warning Network
☐ 2010 Drug Abuse Warning Network
☐ 2011 Drug Abuse Warning Network

Note: Unlike NSDUH, there is not an additional set of restricted variables that you need to request and justify why they are needed.

18. **Other data.** Please describe other non-CBHSQ data you plan to merge with the Confidential Data within the Data Portal and the source of the data.
Provide an explanation for why these "external" data are necessary for the proposed research project.

Signature Page (Please sign in blue ink)

I attest that the information provided in this Application for Access to Confidential Data for the project (insert project title) _____ is accurate to the best of my knowledge:

_____ _____

Principal Project Officer (print name) Principal Project Officer (signature)

_____

Date signed

Please submit original of the completed Application for Access to Confidential Data to ICPSR/SAMHDA:

For United States Postal Service:

ICPSR/SAMHDA
University of Michigan
Institute for Social Research
P.O. Box 1248
Ann Arbor, MI 48106-1248

For Courier:
(UPS, Fed EX, DHL, etc.):

ICPSR/SAMHDA
330 Packard Street
Ann Arbor, MI 48104

Attach Curriculum Vitae

Please attach here at the end of this Application, the current curriculum vitae for the PPO and each project team member for **your** Receiving organization as listed in Section A.

Appendix 2

Substance Abuse and Mental Health Services Administration (SAMHSA)
Center for Behavioral Health Statistics and Quality (CBHSQ)
Substance Abuse and Mental Health Data Archive (SAMHDA)

Confidential Data Use and Nondisclosure Agreement

This Confidential Data Use and Nondisclosure Agreement ("Agreement") governs the access to and use of Confidential Data in the Substance Abuse & Mental Health Data Archive (SAMHDA) Data Portal under the auspices of the Substance Abuse and Mental Health Services Administration (SAMHSA), Center for Behavioral Health Statistics and Quality (CHBSQ).

SAMHSA/CBHSQ collects data related to substance abuse and mental health under the authority of section 505 of the Public Health Service (PHS) Act, as amended. These data are maintained in the Substance Abuse & Mental Health Data Archive (SAMHDA). SAMHDA is maintained by the Inter-university Consortium for Political and Social Research (ICPSR), Institute for Social Research, University of Michigan (UM) under contract with SAMHSA.

Section 501(n) of the Public Health Service Act (42 U.S.C. 299aa(n)) ("the SAMHSA Confidentiality Statute") requires that data collected by SAMHSA that identify individuals or establishments be used only for the purpose for which they were supplied.

The Confidential Information Protection and Statistical Efficiency Act (CIPSEA) of 2002 (hereinafter "CIPSEA"; see P.L. 107-347, Title V, subtitle A) establishes strong confidentiality protections for statistical information collections. Information protected under CIPSEA must be used only for statistical purposes.

Accordingly, any person or entity seeking permission from SAMHSA/CBHSQ to access and use Confidential Data must sign and submit this Agreement and accompanying Nondisclosure Form or Affidavit to SAMHSA/CBHSQ or designated representative for SAMHDA prior to the granting of such permission.

The Principal Project Officer and Receiving Organization (collectively "data recipients/agents") listed below that sign and enter into this Agreement have submitted to CBHSQ an Application for Access to Confidential Data ("Application") to use the Confidential Data and agree to adhere to the terms of this Confidential Data Use and Nondisclosure Agreement and its Attachments, and applicable federal laws and regulations.

By executing this Agreement, the data recipient understands and affirms that Confidential Data will only be used for statistical purposes consistent with the research described in the Application, the terms of this Agreement, and applicable federal laws, regulations, and SAMHSA/CBHSQ policies.

I. Requirements for Data Use

A. No Identification of Persons

The SAMHSA Confidentiality Statute prohibits the use of Confidential Data to identify any person (including but not limited to patients and health care providers). The use of Confidential Data to identify any person constitutes a violation of this Agreement and may constitute a violation of the SAMHSA Confidentiality Statute and CIPSEA. This Agreement prohibits data recipients/agents from releasing, disclosing, publishing, or presenting any individually identifying information obtained under this Agreement. SAMHSA and the data recipient(s)/agent(s) acknowledge that it may be possible for a data recipient, through deliberate technical analysis of the data sets and with outside information, to ascertain the identity of particular persons. This Agreement expressly prohibits any attempt to identify individuals, and information that could be used to identify individuals directly or indirectly shall not be disclosed, released, or published. Data recipients/agents shall not attempt to contact individuals for any purpose whatsoever, including verifying information supplied in the data set. Any questions about the data must be referred exclusively to SAMHSA/CBHSQ.

By executing this Agreement, the data recipient/agent understands and agrees that actual and considerable harm will ensue if he or she attempts to identify individuals. The data recipient/agent also understands and agrees that actual and considerable harm will ensue if he or she intentionally or negligently discloses, releases, or publishes information that identifies individuals or can be used to identify individuals. Misuse of Confidential Data about persons constitutes a violation of this Agreement and may constitute a violation of the SAMHSA Confidentiality Statute and CIPSEA.

B. No Identification of Establishments

The SAMHSA Confidentiality Statute and CIPSEA prohibit the use of Confidential Data to identify establishments (e.g.: hospital or treatment facility) unless the individual establishment has consented. Data recipients/agents are prohibited from identifying establishments directly or by inference in publicly disseminated material. In addition, users of the data are prohibiting from contacting establishments for the purpose of verifying information supplied in the data set. Any questions about the data must be referred exclusively to SAMHSA/CBHSQ. Misuse of Confidential Data about hospitals or any other establishment constitutes a violation of this Agreement and may constitute a violation of the SAMHSA Confidentiality Statute and CIPSEA.

II. Requirements of Principal Project Officers

The Principal Project Officer (PPO) must meet the following criteria:

A. Be directly employed by the Receiving Organization (i.e., the PPO cannot be a visiting faculty member, temporary employee, contractor or outside consultant), and

B. For institutions of higher education, must have an advanced degree (e.g., Ph.D., J.D., M.D. or Ed.D.).

III. Requirements of Receiving Organization

The Receiving Organization must be an institution of higher education, a research organization, or a government agency. The Receiving Organization headquarters, related business offices and/or research site locations must be located in the 50 United States or District of Columbia.

IV. Obligations of the Principal Project Officer, Research Staff, and Receiving Organization

Confidential Data for which access is provided under this Agreement via the Data Portal shall be limited to, and held in strictest confidence by the Principal Project Officer and Research Staff of the Receiving Organization.

In consideration of the requirements contained in this Section of this Agreement, the Principal Project Officer, Research Staff, and Receiving Organization agree that:

A. The Confidential Data will be used solely for statistical purposes and not for any non-statistical purposes, as defined in section 502 of the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA).

B. The Confidential Data and any other data files used in combination with the Confidential Data will only be viewed, accessed and analyzed for the research project that is described in the Application.

C. The Confidential Data will only be viewed, accessed and analyzed in the approved secure project office as listed in the Application.

D. The Confidential Data will be used to generate only statistical summary information that does not allow any individual, family, household, or establishment to be identified, and that no attempt will be made to identify individuals, families, households, or establishments.

E. Where applicable, if an individual person, family, household, or establishment is inadvertently identified in a data set or if a technique for doing so is discovered (unless specifically the objective of the project), then:
    1. No use will be made of this knowledge;
    2. A summary of this identification or technique, but not including any Confidential Data, will be reported to dataportal@icpsr.umich.edu immediately upon discovery by the Principal Project Officer; and
    3. This identification or technique will not be revealed to any other person.

F. When becoming aware of any suspected or actual unauthorized access, use, or disclosure of Confidential Data, this event will be immediately reported to CBHSQ via a telephone

call and then a follow-up report in writing as an attachment to an email to CBHSQ and SAMHDA.

G. No attempt will be made to link this Confidential Data with any other dataset, unless specifically identified in the approved Application for Access to Confidential Data.

H. Analyses or results derived from the Confidential Data will not be provided to any other individual or organization without the written consent of CBHSQ. Approval for disseminating information or results based on analysis derived from the Confidential Data can only be obtained through CBHSQ's disclosure review and approval process. The scope of the disclosure review and approval process will only be for determining compliance with CIPSEA, the Privacy Act and the Public Health Services Act, and to ensure adherence to the confidentiality and security provisions established under this Agreement. Notwithstanding the above, no restriction shall be placed on the ability of the Receiving Organization to publish work or other information products (e.g., dissertations or theses) developed hereunder, except that such work or other information products shall not include Confidential Data.

I. If the Receiving Organization requires a review of research proposals by an Institutional Review Board/Human Subjects Review Committee or equivalent body, then this review must take place and all approvals granted prior to submitting the Application for Access to Confidential Data.

J. The Principal Project Officer certifies that all aspects of the Computer and Data Security Requirements (Appendix B), as stated in the Attachment to this Agreement, will be strictly followed and implemented.

K. During the period of data access, the Receiving Organization will participate in announced and unannounced site inspection(s) conducted by CBHSQ-designated staff or contractor during normal business hours. These site visits will inspect the physical location and security measures in place for the use of the Data Portal and Confidential Data along with review of relevant records pertaining to the data covered under this Agreement.

L. The PPO will notify CBHSQ in writing, in the event the PPO plans to separate from the Receiving Organization during the Contract Period, at least two (2) weeks prior to the last day on the project. PPO separation from the Receiving Organization will lead to the termination of access to the data for the PPO and Research Staff. The PPO's separation from the Receiving Organization terminates this Agreement, unless the Receiving Organization identifies and obtains CBHSQ approval of a new PPO, pursuant to section IV.M of this Agreement.

M. The Receiving Organization will obtain approval from CBHSQ prior to transferring this Agreement to another Principal Project Officer at the same Receiving Organization. In order to obtain such approval, the Principal Project Officer must:

1. Inform CBHSQ in writing six (6) weeks prior to the proposed date of transfer;

2. Submit a complete copy of this Agreement signed by an official representative of the Receiving Organization and the new PPO; and
3. Maintain responsibility for the Computer and Data Security requirements until the transfer Agreement has been approved by CBHSQ.

N. Research Staff must be directly employed by or students currently enrolled at the Receiving Organization (i.e., they cannot be a contractor, visiting professor, temporary employee or outside consultant). The PPO will notify CBHSQ, in writing, of changes in the Research Staff. Research Staff separation from the Receiving Organization will lead to the termination of their access to the Data Portal.

O. The maximum number of persons who may have access to the Confidential Data under this Agreement is ten (10). This includes the PPO and Research Staff combined.

P. If during the course of research there are changes in research plans or in the computer environment that is different from (a) the information originally submitted in the Application, (b) different from that which is required by this Agreement, and/or (c) is different from that which in the Computer and Data Security Requirements (Appendix B), then the Principal Project Officer shall provide CBHSQ with a copy of the revised materials and a memorandum describing the changes. These revisions will be considered amendments to this Agreement and may not be implemented until written approval is obtained from CBHSQ.

Q. If the Principal Project Officer desires to extend this Agreement beyond the Contract Period, the Principal Project Officer must submit a written request to CBHSQ three (3) months prior to the end of the Agreement time period requesting CBHSQ approval of such continued access. If continued access is denied by CBHSQ, then this Agreement will terminate at the end of the Contract Period.

R. Should the Principal Project Officer, Research Staff, or Receiving Organization commit a material breach of this Agreement that is not cured within ten (10) working days after Principal Project Officer or Receiving Organization receives notice of such breach from SAMHDA or CBHSQ, then CBHSQ reserves the right to terminate this Agreement. In the event of a breach of any of the confidentiality provisions of this Agreement, CBHSQ reserves the right to immediately terminate this Agreement. In the event of termination of this Agreement, access to the Confidential Data and the Data Portal will be revoked. The Principal Project Officer, Research Staff, and Receiving Organization understand and agree that a violation of any of the terms and conditions of this Agreement may constitute a violation of state and federal statutes, including the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA), and may subject the Principal Project Officer, Research Staff, and/or Receiving Organization to criminal, civil, and administrative penalties associated with violations of those statutes, in addition to constituting a material breach of this Agreement with attendant legal liabilities.

S. The Receiving Organization will treat allegations of violations of this Agreement, by SAMHDA or CBHSQ, as allegations of violations of the Receiving Organization's policies and procedures on scientific integrity and misconduct. If the allegations are

confirmed, the Receiving Organization will treat the violations as it would violations of the explicit terms of its policies on scientific integrity and misconduct.

V. Miscellaneous

A. The respective rights and obligations of the Principal Project Officer, Research Staff, and Receiving Organization pursuant to this Agreement shall survive termination of this agreement.

B. This Agreement contains all of the terms and conditions agreed upon by the parties regarding the subject matter of this Agreement and supersedes any prior agreements, oral or written, and all other communications between the parties relating to such subject matters.

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

D. The obligations of Principal Project Officer, Research Staff, and Receiving Organization set forth within this Agreement may not be assigned or otherwise transferred without the express written consent of CBHSQ.

E. Ownership of the Confidential Data will be retained by CBHSQ. Permission to use the Confidential Data and to use the Data Portal by the Receiving Organization may be revoked by CBHSQ through SAMHDA at any time, at CBHSQ's discretion.

F. The Principal Project Officer and Research Staff must return MTokens to SAMHDA upon completion of the project or when requested by CBHSQ or SAMHDA.

G. This Agreement may be amended or modified only by the mutual written consent of the authorized representatives of CBHSQ and Receiving Organization. Both parties agree to amend this Agreement to the extent amendment is necessary to comply with the requirements of any applicable regulatory authority, including Federal law and policy, and as changes in the research plan or computer environment alter the information originally submitted as part of the Application.

H. This Agreement may be executed in one or more counterparts (facsimile transmission or otherwise), each of which counterpart shall be deemed an original Agreement and all of which shall constitute but one Agreement.

I. If used, the parties' electronic signatures shall be the legally binding equivalent of a handwritten signature.

J. Attachments incorporated into this Agreement are:
   1. Appendix A: Definitions,
   2. Appendix B: SAMHSA/CBHSQ Computer and Data Requirements,

3. Appendix C: The Designation of Agent and Affidavit of Non-disclosure for the Use of Confidential Data, or
4. Appendix D: Designation of Agent and Declaration of Nondisclosure (for Federal employee use only).

K. The parties agree that the following documents are incorporated into this Agreement by reference:
   1. The Application for Access to Confidential Data.
   2. Applicable federal laws.

VI. Signature Page

Principal Project Officer		**Receiving Organization Representative**	
Signature	Date	Signature	Date
Name (type or print)		Name (type or print)	
Title		Title	
Organization		Organization	
Building Address		Building Address	
Street Address		Street Address	
City, State, Zip		City, State, Zip	

Representative for SAMHSA\CBHSQ

Peter J. Delany, PhD, LCSW-C
RADM U.S. Public Health Service
Director, Center for Behavioral Health Statistics and Quality
Substance Abuse & Mental Health Services Administration

CBHSQ Director Signature Date

Appendix A: Definitions

"Substance Abuse and Mental Health Services Administration" is a federal government agency within the United States Department of Health and Human Services (DHHS). http://www.samhsa.gov

"Center for Behavior Health Statistics and Quality" is a Center within the Substance Abuse and Mental Health Services Administration, located at One Choke Cherry Rd., Rockville, Maryland, 20857. http://www.samhsa.gov/data/

"Substance Abuse & Mental Health Data Archive" is CBHSQ's data repository. SAMHDA houses CBHSQ public-use and restricted-use confidential databases. SAMHDA is administered by the Inter-university Consortium for Political and Social Research (ICPSR), Institute for Social Research, University of Michigan (UM), Ann Arbor, under contract with SAMHSA. http://www.datafiles.samhsa.gov

"Confidential Data" refers to CBHSQ restricted-use data or individually identifiable information that are accessible via a web portal (see Data Portal) at SAMHDA pursuant to this Agreement, and any other external data files merged with the Confidential Data within the Data Portal. The Confidential Data is protected under the Privacy Act of 1974 (5 U.S.C. 552a); Confidential Information Protection and Statistical Efficiency Act (CIPSEA) of 2002 (P.L. 107-347, Title V, subtitle A); and section 501(n) of the Public Health Services Act (42 U.S.C. 290aa(n)).

"Agent" is defined under CIPSEA as: "[A]n individual— (A)(i) who is an employee of a private organization or a researcher affiliated with an institution of higher learning … and with whom a contract or other agreement is executed, on a temporary basis, by an executive agency to perform exclusively statistical activities under the control and supervision of an officer or employee of that agency; (ii) who is working under the authority of a government entity with which a contract or other agreement is executed by an executive agency to perform exclusively statistical activities under the control of an officer or employee of that agency; (iii) who is a self-employed researcher, a consultant, a contractor, or an employee of a contractor, and with whom a contract or other agreement is executed by an executive agency to perform a statistical activity under the control of an officer or employee of that agency; or (iv) who is a contractor or an employee of a contractor, and who is engaged by the agency to design or maintain the systems for handling or storage of data received under this title; and (B) who agrees in writing to comply with all provisions of law that affect information acquired by that agency.

"Data Portal" is a virtual confidential data storage and statistical computing environment. The Data Portal is administered by ICPSR at the University of Michigan (UM). Approved users are provided with remote access to the Data Portal and can view and analyze confidential data using statistical software. Users can also produce research reports and documents within the Data Portal.

"Principal Project Officer" refers to the person who has the lead role on the project at the Receiving Organization. This person will serve as the primary point of contact for all communications involving this Agreement and for the Receiving Organization. The Principal

Project Officer must be a senior staff member on the project. The Principal Project Officer assumes all responsibility for compliance with all terms of this agreement and for the research staff of their own organization. Under this Agreement, the PPO is a CIPSEA agent.

"Receiving Organization" refers to the organization employing the Principal Project Officer.

"Research Staff" refers to any individuals other than the Principal Project Officer with access to the Confidential Data via the Data Portal. These persons are also known as Project Team Members and become CIPSEA agents under this Agreement

"Representative of the Receiving Organization" is an individual that represents the Receiving Organization and is legally authorized to enter into and sign a contract (this Agreement) on behalf of the Receiving Organization.

"Contract Period" is the time period beginning on the date of the last signature affixed on the signature page that executes this Agreement and ending upon completion of the research project, as noted in the Application for Access to Confidential Data or twelve (12) months from the date this Agreement is executed, whichever comes first.

Appendix B: SAMHSA/CBHSQ Computer and Data Requirements

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

- You must password protect the computer that is used to access the Data Portal.
- Under no circumstances may you share or give your Data Portal username, password or MToken to anyone, and this includes not sharing them with other members of your project team or your organization's IT staff. Passwords must not be stored on a computer in electronic or written form. Software password storage programs may not be used.
- Since the Data Portal is administered by ICPSR, University of Michigan (under contract SAMHSA/CBHSQ), you should not contact the IT staff at your organization with questions about the Data Portal. (You may contact your organization's IT staff if you need help installing the VMware client software to access the Data Portal. Your organization's IT staff should never be allowed to access the Data Portal or any Confidential Data.)
- Under no circumstances can any unauthorized person be allowed to access or view Confidential Data within the Data Portal.
- You must only access the Data Portal from within the authorized Secure Project Office (as listed in the Application) using only the approved desktop computer and assigned IP address.
- Unauthorized persons are not allowed to be inside the Secure Project Office when an authorized project team member is logged into the Data Portal.
- You must not allow the computer monitor to display Data Portal content to any unauthorized person. The computer monitor display screen must not be visible from open doors or through windows.
- You must set the computer to activate a password protected screen saver after three minutes of inactivity.
- If you are logged into the Data Portal and you leave your computer, you must "disconnect" or "logoff" from the Data Portal. (Disconnecting from the Data Portal will leave any open programs running, but closes the connection to the Data Portal. Logging off of the Data Portal closes the connection and terminates all programs that are running.)
- All Confidential Data must be kept within the Data Portal:
    - You must not duplicate or copy the data (e.g., you must not retype and/or use non-technical ways of copying the data, such as handwritten notes).
    - You must not take screenshots, photographs, or videos of the displayed Confidential Data or statistical outputs.
    - You must not type or record the Confidential Data or results from the data onto your PC or onto some other device or media.
- You must protect all hardcopy documents related to the Confidential Data such as research notes. Such hardcopy documents must be kept in locked drawers or cabinets when not in use.
- Prior to a disclosure review and approval by SAMHSA/CBHSQ, neither you nor any project team member may talk about or discuss any Confidential Data or results from the Data Portal in non-secure or public locations. These discussions cannot occur where an unauthorized person could eavesdrop.

- You must submit all statistical outputs/results from the Data Portal to CHBSQ for a disclosure review prior to sharing or giving such outputs to unauthorized persons. You also agree to revise or alter such outputs as required by CBHSQ in order to minimize disclosure risk prior to CBHSQ approving these outputs for dissemination to unauthorized persons.
- You may only disseminate aggregated information from the Confidential Data to unauthorized persons after you obtain clearance to do so through the CBHSQ disclosure review process.

Substance Abuse and Mental Health Services Administration (SAMHSA)
Center for Behavioral Health Statistics and Quality (CBHSQ)

Appendix C: Confidential Data Use and Nondisclosure Agreement

Designation of Agent and Affidavit of Nondisclosure Form

I, _____ (print name), in consideration of access to and use of SAMHSA/CBHSQ Confidential Data agree that:

A. I have read and will follow the requirements stated in the SAMHSA/CBHSQ Confidential Data Use and Nondisclosure Agreement and the Confidential Data Procedures Manual for the SAMHSA/CBHSQ Data Portal.

B. I have completed the required SAMHSA/CBHSQ confidentiality training that covered applicable federal laws (including CIPSEA, the Public Health Service Act, and the Privacy Act), security requirements, and disclosure review of researcher results within the last year and understand these requirements and penalties associated with unauthorized disclosures of Confidential Data.

C. I will only use the Confidential Data obtained under the Confidential Data Use and Nondisclosure Agreement for statistical purposes as defined by the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA).

D. I will not share, release, disclose or redistribute any Confidential Data. I further understand that I am subject to the penalties of federal law for unauthorized disclosures of any Confidential Data.

E. I will not make any disclosures or publication of the data where a responding entity could be identified or the data furnished by or related to any particular responding entity could be identified.

I do solemnly swear (or affirm) that I will observe and follow all of the requirements listed above as attested to by my signature below.

Signature _____ Date _____

Subscribed and sworn (or affirmed) before me this _____ day of _____, 20__

at_____ (city), _____ (state). Witness by my hand and official Seal.

_____ [SEAL]
(Notary Public Signature)

My commission expires_____ .

Note: The penalty for unlawful disclosure of Confidential Data under this affidavit is a fine of not more than $250,000, or imprisonment for not more than five years, or both (see P.L. 107-347, Title V, Section 513). The word "swear" may be stricken when a person elects to affirm the affidavit rather than swear to it.

Substance Abuse and Mental Health Services Administration (SAMHSA)
Center for Behavioral Health Statistics and Quality (CBHSQ)

Appendix D: Confidential Data Use and Nondisclosure Agreement

Designation of Agent and Declaration of Nondisclosure for Employees of the Federal Government

I, _____ (print name), declare under penalty of perjury under the laws of the United States of America that the following is true and correct.

I agree that:

A. I have read and will follow the requirements stated in the SAMHSA/CBHSQ Confidential Data Use and Nondisclosure Agreement and the Confidential Data Procedures Manual for the SAMHSA/CBHSQ Data Portal.

B. I have completed the required SAMHSA/CBHSQ confidentiality training that covered applicable federal laws (including CIPSEA, the Public Health Service Act, and the Privacy Act), security requirements, and disclosure review of researcher results within the last year and understand these requirements and penalties associated with unauthorized disclosures of Confidential Data.

C. I will only use the Confidential Data obtained under the Confidential Data Use and Nondisclosure Agreement for statistical purposes as defined by the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA).

D. I will not share, release, disclose or redistribute any Confidential Data. I understand that I am subject to the penalties of federal law for unauthorized disclosures of any Confidential Data.

E. I will not make any disclosures or publication of the data where a responding entity could be identified or the data furnished by or related to any particular responding entity could be identified.

_____ _____
(Signature) Date

This declaration is authorized under 28 U.S.C. 1746 as a substitute for an Affidavit of Nondisclosure as otherwise required under the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA) for access to Confidential Data by agents of the Center for Behavioral Health Statistics and Quality (CBHSQ). Persons who provide this Declaration are subject to penalties of unlawful disclosure of a fine of not more than $250,000, or imprisonment for not more than five years, or both (see P.L. 107-347, Title V, Section 513).

Appendix 3

Application Requirements

The Application for Access to Confidential Data ("Application") requires a thorough description of your planned research project. As you fill out your Application for Access to Confidential Data in the Data Portal, please keep in mind the requirements that are listed below. All of these requirements must be met for an Application to be approved. If all the requirements cannot be met, access to the Data Portal cannot be provided.

Please take into account these requirements in the early stages of planning your research project. This will give you sufficient time to address the requirements in your project development or determine that the project will not be feasible at your organization or location.

For more information, refer to this *Manual* or to the section of the Confidential Data Use and Nondisclosure Agreement (CDUNA) as referenced (given in parentheses).

Call for Applications
An Application for Access will only be considered if it is submitted to SAMHDA as a paper copy with the original-signature page by the deadline of a Call for Applications. A copy of the application as a Word document should also be emailed to SAMHDA at dataportal@ icpsr.umich.edu.

Organizations
- CBHSQ provides Confidential Data only to qualified organizations in the 50 United States and District of Colombia. (CDUNA III)
- The Receiving Organization must be an institution of higher education, a research organization, or a government agency. (CDUNA III)
- Individual researchers must apply through a recognized organization (e.g., a government agency, university, or research institution).
- No Application will be approved for a Receiving Organization that is operating within a private residence.

Project Team
- The Principal Project Officer (PPO) must be directly employed by the Receiving Organization (i.e., the PPO cannot be a visiting faculty member, temporary employee, contractor or outside consultant); for institutions of higher education, the PPO must have an advanced degree (e.g., Ph.D., J.D., M.D. or Ed. D). (CDUNA II)
- Research Staff must be directly employed by or students currently enrolled at the Receiving Organization. (CDUNA II.N)
- There can be no more than 10 researchers on a project, including all Receiving Organizations involved in the project. (CDUNA IV.O).

Multiple Receiving Organizations

- Separate Applications for Access are required from each Receiving Organization involved in a project. These Applications for Access must reference each organization and the research project description must cover all the Receiving Organizations.
- Requests for dataset(s) must encompass the research across all organizations involved in the project.
- Prior to submitting the Application for Access, the PPO must obtain IRB approval (if required) from each Receiving Organization that requires it.

Software

- The software provided for use within the Data Portal includes SAS 9.2 which includes the Education Analytical Suite; SAS Enterprise Miner Client, SAS/GIS, and SAS/SPECTRAVIEW; SPSS 19 with add-ons for (a) Regression Models and (b) Advanced Models; Stata/SE 11; SUDAAN 10.0.1 (SAS-callable library); StatTransfer 9, R 2.11.1, and Microsoft Office 2010 (Access, Excel, InfoPath, OneNote, PowerPoint, Publisher, and Word).
- If you need other software, contact SAMHDA (dataportal@icpsr.umich.edu) to check if the additional software can be provided and, if so, include this information in your Application.

Computers

- Only desktop computers can be used to access the Data Portal.
- Only Windows computers can be used to access the Data Portal. Mac computers could not be used at this time.

Security Requirements

- VMware Client software must be installed on the desktop computers in Secure Project Office(s) for connection to the Data Portal. (The software can be downloaded from the University of Michigan ITS website.) Please confirm with your IT group that installing VMware will be allowed by your organization.
- The Secure Project Office(s) is the only place from which the Data Portal may be accessed. Make sure your organization has such space available. (Manual Section 3, CDUNA IV.c)
- Applicants must confirm that their computers and Secure Project Offices meet the physical security requirements for computer set-up and locations as required in the Application and Agreement. (Appendix 2, CDUNA Appendix B)
- All researchers must follow all security requirements covered in this *Manual* and the Confidential Data Use and Nondisclosure Agreement. (CDUNA Appendix B)