**Data Portal Confidentiality Procedures Manual**

**[[1]](#footnote-1)**

# August 2017

## 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)

**5600 Fishers Lane Rockville, MD 20857**

**Table of Contents**

1. [INTRODUCTION. 2](#_TOC_250030)
2. [LEGAL BACKGROUND 3](#_TOC_250029)
3. [THE APPLICATION PROCESS 5](#_TOC_250028)

[OVERVIEW 5](#_TOC_250027)

[STEPS IN THE APPLICATION PROCESS 6](#_TOC_250026)

[RECEIVING ORGANIZATIONS 10](#_TOC_250025)

[MULTIPLE RESEARCH PROJECT TOPICS 12](#_TOC_250024)

1. [SECURITY 13](#_TOC_250023)

[OVERVIEW 13](#_TOC_250022)

[DATA AND SOFTWARE IN THE SECURE DATA PORTAL 13](#_TOC_250021)

[SECURITY REQUIREMENTS 14](#_TOC_250020)

1. [DISCLOSURE REVIEW PROCESS: SAFEGUARDING CONFIDENTIALITY 18](#_TOC_250019)

[OVERVIEW 18](#_TOC_250018)

[DISCLOSURE 18](#_TOC_250017)

1. [SITE INSPECTION. 21](#_TOC_250016)

[VIOLATIONS 21](#_TOC_250015)

1. [MODIFICATIONS TO THE APPLICATION 23](#_TOC_250014)

[MODIFICATIONS AT ONE RECEIVING ORGANIZATION 23](#_TOC_250013)

[MODIFICATIONS FOR OVERALL PROJECT 23](#_TOC_250012)

1. [CLOSING OUT A PROJECT 25](#_TOC_250011)

[PROJECT ARCHIVE 25](#_TOC_250010)

[CONFIDENTIALITY 25](#_TOC_250009)

[PUBLICATIONS 25](#_TOC_250008)

1. [RESPONSIBILITIES 26](#_TOC_250007)

[PRIMARY CONTACT RESPONSIBILITIES (IN ADDITION TO BEING A PPO) 26](#_TOC_250006)

[PPO RESPONSIBILITIES (IN ADDITION TO BEING TEAM MEMBER) 26](#_TOC_250005)

[PROJECT TEAM MEMBER RESPONSIBILITIES 26](#_TOC_250004)

[CBHSQ RESPONSIBILITIES 27](#_TOC_250003)

[SAMHDA RESPONSIBILITIES 27](#_TOC_250002)

[GLOSSARY. 27](#_TOC_250001)

[APPENDICES 31](#_TOC_250000)

# 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 laws and regulations and security requirements governing the use of these data. It describes how applicants and users can obtain the Data Portal Application and Users Guides. It does not replace the provisions of the actual Confidential Data Use and Nondisclosure Agreement (i.e., data use agreement).

# Legal Background

CBHSQ data are collected pursuant to SAMHSA’s authority under Section 5051 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) Act2, 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 20024 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](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=browse_usc&amp;docid=Cite%3A%2B42USC290aa-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](http://frwebgate3.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=54521924645%2B13%2B0%2B0&amp;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 19745 and the Federal Information Security Management Act of 20026.

**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.

# 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, prior to starting your application, please review the *Data Portal Application Instructional Manual* and the *Data Portal Users Manual,* as well as the *Confidential Data Use and Nondisclosure Agreement*. These documents are available at the SAMHDA website at <https://www.datafiles.samhsa.gov/>. 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 difficulty with **passwords** or other Data Portal **access issues**, please contact the RTI ITS Help Desk at 919-541-6600. For other technical questions, please contact SAMHDA Help using the SAMHDA website at <https://www.datafiles.samhsa.gov/info/samhda-technical-assistance-form-nid3423>, or call 888.741.7242 (please leave a message if you are calling outside normal business hours, 8 a.m. to 5 p.m. Eastern Time). At the bottom-left of the website screen, you may also click [Report Problem with SAMHDA site](https://www.datafiles.samhsa.gov/info/samhda-technical-assistance-form-nid3423) to report technical issues

###### 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 and 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 at https://www.datafiles.samhsa.gov.

**STEP 1 - SUBMIT APPLICATION FOR ACCESS**

The Data Portal application process is covered in detail in the *Data Portal Application Instructional Manual.* Please refer to the latest version of this Manual to be sure to have the most current information.

Once submitted applications are approved by CBHSQ, applicants have six (6) months to complete the required confidentiality training and to submit the required forms. Applications will be terminated for any applicant who fails to meet these requirements within six (6) months of application approval. Applicants with terminated applications will need to reapply for Data Portal access during a future call for applications

**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 purpose7 for which the data were collected, and
* 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.

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.sam](http://www.samhsa.gov/data/DAWN.aspx))h[sa.gov/data/DAWN.aspx)](http://www.samhsa.gov/data/DAWN.aspx)) and NSDUH (<http://www.samhsa.gov/data/NSDUH.aspx)>resources.

* *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**

Once submitted applications are approved by CBHSQ, applicants have six (6) months to complete the required confidentiality training and to submit the required forms. Applications will be terminated for any applicant who fails to meet these requirements within six (6) months of application approval. Applicants with terminated applications will need to reapply for Data Portal access during a future call for applications.

1. **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*.
2. 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.

1. 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).**
2. 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 and the *Data Portal User Guide* 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.

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.

# 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.

The technical requirements and processes for complying with the Data Portal security requirements are covered in the *Data Portal Users Manual.* Please refer to the latest version of this Manual to be sure to have the most current information.

# Disclosure Review Process: Safeguarding Confidentiality

### Overview

Analysis results must go through the disclosure review process at SAMHDA 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 notifies SAMHSA using the SAMHDA TA Form:

[https://www.datafiles.samhsa.gov/info/samhda-technical-assistance-form-nid3423](https://www.datafiles.samhsa.gov/info/samhda-technical-assistance-form-nid3423 ) 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.

# 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.

# 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.

# 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 notifies Data Portal staff via the SAMHDA TA Form:

<https://www.datafiles.samhsa.gov/info/samhda-technical-assistance-form-nid3423> 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 using the SAMHDA TA Form at

<https://www.datafiles.samhsa.gov/info/samhda-technical-assistance-form-nid3423>

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 using the SAMHDA TA form:

https://www.datafiles.samhsa.gov/info/samhda-technical-assistance-form-nid3423

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.

# 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 SAMHDA at

[https://www.datafiles.samhsa.gov/info/samhda-technical-assistance-form-nid3423]( https://www.datafiles.samhsa.gov/info/samhda-technical-assistance-form-nid3423) 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.
* At the end of the project, the Primary Contact prepares the archive folder and notifies [SAMHDA](mailto:dataportal@icpsr.umich.edu) that the archive folder is ready.

### 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.

### 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.](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 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.

*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 RTI International 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.

1. [↑](#footnote-ref-1)