

SUPPORTING STATEMENT – PART A
Substance Abuse and Mental Health Services Administration (SAMHSA)
Data Security Requirements for Accessing Confidential Data
OMB Control No. [number]

A. Justification

The Foundations for Evidence-Based Policymaking Act of 2018 (44 U.S.C. 3583) mandates that the Director of the Office of Management and Budget (OMB) establish a standard application process (SAP) for requesting access to certain confidential data assets. While the adoption of the SAP is required for statistical agencies and units designated under the Confidential Information Protection and Statistical Efficiency Act of 2018 (CIPSEA), it is recognized that other agencies and organizational units within the Executive Branch may benefit from the adoption of the SAP to accept applications for access to confidential data assets. The SAP is a standard process through which potential data users may apply to access restricted-use data assets held by the federal statistical agencies that sponsors SAP. With the Interagency Council on Statistical Policy (ICSP) as advisors, the entities upon whom this requirement is levied are working with the SAP Project Management Office (PMO) and with OMB to implement the SAP. The SAP Portal is to be a single web-based common application designed to collect information from individuals requesting access to confidential data assets from federal statistical agencies and units. In late 2022, the National Center for Science and Engineering Statistics (NCSES), in its role as the SAP PMO, published a 60-day Federal Register Notice ([87 FR 53793](#)) and 30-day Federal Register Notice ([87 FR 66754](#)) announcing plans to collect information through the SAP Portal. This collection request was submitted to the Office of Management and Budget as a Common Form in late 2022; the OMB control number for SAP Portal information collection is 3145-0271 and the expiration date is 12/31/2025.

When an application process starts in the SAP Portal, the SAP system will collect information and SAMHSA will review the application to fulfill its data security requirements. This is a required step before providing the individual with access to confidential microdata for the purpose of evidence building. SAMHSA's data security agreements and other paperwork, along with the corresponding security protocols, allow SAMHSA to maintain careful controls on confidentiality and privacy, as required by law. This collection will occur outside of the SAP Portal. On November 22, 2022, SAMHSA published a 60-day Federal Register Notice 87 FR 71346 announcing plans for this collection.

This submission requests approval to collect information from individuals to fulfill SAMHSA data security requirements. This request is from Center for Behavioral Health Statistics and Quality (CBHSQ) within the Substance Abuse and Mental Health Services Administration (SAMHSA).

1. Necessity of the Information Collection

Title III of the Foundations for Evidence-Based Policymaking Act of 2018 (hereafter referred to as the Evidence Act) mandates that OMB establish a Standard Application Process (SAP) for requesting access to certain confidential data assets. Specifically, the Evidence Act requires OMB to establish a common application process through which agencies, the Congressional Budget Office, State, local, and Tribal governments, researchers, and other individuals, as appropriate, may apply for access to confidential data assets collected, accessed, or acquired by a statistical agency or unit. This new process will be implemented while maintaining stringent controls to protect confidentiality and privacy, as required by law.

Data collected, accessed, or acquired by statistical agencies and units is vital for developing evidence on the characteristics and behaviors of the public and on the operations and outcomes of public programs and policies. This evidence can benefit the stakeholders in the programs, the broader public, and policymakers and program managers at the local, State, Tribal, and National levels. The many benefits of access to data for evidence building notwithstanding, SAMHSA is required by law to uphold rigorous controls that allow it to minimize disclosure risk and protect confidentiality. The fulfillment of SAMHSA's data security requirements places a degree of burden on individuals, which is outlined below.

The SAP Portal is a web-based application to allow individuals to request access to confidential data assets from federal statistical agencies and units. The objective of the SAP Portal is to broaden access to confidential data for the purposes of evidence building and reduce the burden of applying for confidential data. Once an individual's application in the SAP Portal has received a positive determination, SAMHSA will begin the process of collecting information to fulfill its data security requirements.

This Paperwork Reduction Act (PRA) supporting statement outlines the SAP Policy, the steps to complete an application through the SAP Portal, and the process SAMHSA uses to collect information to fulfill its data security requirements.

The SAP Policy

At the recommendation of the ICSP, the SAP Policy establishes the SAP to be implemented by statistical agencies and units and incorporates directives from the Evidence Act. The policy is intended to provide guidance as to the application and review processes using the SAP Portal, setting forth clear standards that enable statistical agencies and units to implement a common application form and a uniform review process. The SAP Policy may be found in OMB [Memorandum 23-04](#).

Method of Collection

The SAP Portal

The SAP Portal is an application interface connecting applicants seeking data with a catalog of metadata for data assets owned by the federal statistical agencies and units. The SAP Portal is not a new data repository or warehouse; confidential data assets will continue to be stored in secure data access facilities owned and hosted by the federal statistical agencies and units. The Portal will provide a streamlined application process across agencies, reducing redundancies in

the application process. This single SAP Portal will improve the process for applicants, tracking and communicating the application process throughout its lifecycle. This reduces redundancies and burden on applicants who request access to data from multiple agencies. The SAP Portal will automate key tasks to save resources and time and will bring agencies into compliance with the Evidence Act statutory requirements.

Data Discovery

Individuals begin the process of accessing restricted use data by discovering confidential data assets through the SAP metadata catalog maintained by federal statistical agencies at www.researchdatagov.org. Potential applicants can search by agency, topic, or keyword to identify data of interest or relevance. Once they have identified data of interest, applicants can view metadata outlining the title, description or abstract, scope and coverage, and detailed methodology related to a specific data asset to determine its relevance to their research.

While statistical agencies and units shall endeavor to include information in the SAP metadata catalog on all confidential data assets for which they accept applications, it may not be feasible to include metadata for some data assets (e.g., potential special tabulations of administrative data). A statistical agency or unit may still accept an application through the SAP Portal even if the requested data asset or special tabulation is not listed in the SAP metadata catalog.

SAP Application – Researcher Information

Individuals who have identified and wish to access confidential data assets can apply for access through the SAP Portal at www.researchdatagov.org. Applicants must create an account and follow all steps to complete the application. Applicants begin by entering their personal, contact, and institutional information, as well as the personal contact, and institutional information of all individuals on their research team.

SAP Application – Research Description

Applicants provide summary information about their proposed project to include project title, duration, funding, and timeline. Other details provided by applicants include the data asset(s) they are requesting and any proposed linkages to data not listed in the SAP metadata catalog, including non-federal data sources. Applicants then enter detailed information regarding their proposed project, including a project abstract, research question(s), list of references, research methodology, project products, and requested output. Within the application, applicants must demonstrate a need for confidential data, outlining why their research question cannot be answered using publicly available information.

Submission for Review

Upon submission of their application, applicants will receive a notification that their application has been received and is under review by the data-owning agency or agencies (in the event where data assets are requested from multiple agencies). During the application process, applicants are informed that application approval alone does not grant access to confidential data, and that, if approved, applicants must comply with the data-owning agency's security requirements outside of the SAP Portal, which may include a background check.

Data discovery, the SAP application process, and the submission for review take place within the web-based SAP Portal.

Access to Confidential Data

In the event of a positive determination, the applicant will be notified that their proposal has been accepted. The positive or final adverse determination concludes the SAP Portal process. In the instance of a positive determination, the data-owning agency (or agencies) will contact the applicant to provide instructions on the agency's security requirements that must be completed by the applicant to gain access to the confidential data. The completion and submission of the agency's security requirements will take place outside of the SAP Portal.

Collection of Information for Data Security Requirements

In the instance of a positive determination for an application requesting access to a SAMHSA - owned confidential data asset, SAMHSA will contact the applicant(s) to initiate the process of collecting information to fulfill its data security requirements. This process allows SAMHSA to place the applicant(s) in a trusted access category and includes the collection of the following information from applicant(s):

- Designated Agent Form: This form allows the applicant to be designated CIPSEA agents to access the confidential data files.
- Data Use Agreement Form: This form is an agreement between the applicant and SAMHSA that the applicant agrees to only conduct analyses related to the research question for which they have received approval and follow all disclosure risk procedures.
- SAMHSA RDC Student Data User Acknowledgment Form: This form is intended for university students and their advisors. Students are non-contractually related to the university and therefore must have a contractually bounded individual (i.e., their advisor) sign this agreement with them.

Authorization

This collection is authorized by Confidential Information Protection and Statistical Efficiency Act (CIPSEA) of 2002 (P.L. 107-347, title V, 44 U.S.C. 3501 note).

2. Needs and Uses

The Paperwork Reduction Act (PRA) seeks to maximize the usefulness of information created, collected, maintained, used, shared, and disseminated by or for the federal government while also ensuring the greatest possible public benefit from such information. The PRA moreover mandates that the disposition of information by or for the federal government is consistent with laws related to privacy and confidentiality. SAMHSA's data security agreements ensure that SAMHSA is compliant with PRA requirements.

Data collected, accessed, or acquired by statistical agencies and units is vital for developing evidence on conditions, characteristics, and behaviors of the public and on the operations and outcomes of public programs and policies. Access to confidential data on businesses, households, and individuals from federal statistical agencies and units enables agencies, the

Congressional Budget Office, State, local, and Tribal governments, researchers, and other individuals to contribute evidence-based information to research and policy questions on economic, social, and environmental issues of national, regional, and local importance. This evidence can benefit the stakeholders in the programs, the broader public, as well as policymakers and program managers at the local, State, Tribal, and National levels.

Many applicants will be academic research faculty or students at U.S. universities or other types of research institutions. Other applicants are likely to include analysts at nonprofit organizations and research groups in U.S. Government organizations (Federal, State, local, and Tribal). Scientific research typically results in papers presented at scientific conferences and published in peer-reviewed academic journals, working paper series, monographs, and technical reports. The scientific community at large benefits from the additions to knowledge resulting from research with statistical agencies and units' data. Results inform both scientific theory and public policy and can assist agencies in carrying out their missions.

Approved applicants using confidential data can provide insights on how statistical agencies and units may improve the quality of the data collected or acquired; identify shortcomings of current data collection programs and data processing methods; document new data needs; and develop methods to address survey nonresponse or improve statistical weights.

3. Use of Information Technology

SAMHSA will contact individuals whose approved applications requesting access to SAMHSA's confidential data via email. Applicants complete SAMHSA's required forms and resubmit by email.

4. Efforts to Identify Duplication

SAMHSA is required by law to maintain careful controls on confidentiality and limit disclosure risk. Its security forms are required for each approved research project to ensure minimal disclosure risk of SAMHSA's confidential data. SAMHSA has reviewed its security requirements to eliminate duplication.

5. Impact on Small Entities

Small businesses or their representatives may choose to participate in this voluntary collection of information. The burden of this collection does not represent a significant barrier to participation from small businesses and is not large enough to pose significant costs to respondents, including small businesses.

6. Consequences of Less Frequent Collection

SAMHSA requires and collects information for its security forms for all individuals who will access data and output that has not been cleared for disclosure review. Less frequent collection would compromise SAMHSA's ability to secure its confidential data.

7. Special Circumstances

There are no special circumstances.

8. Consultations Outside the Agency

On November 22, 2022, SAMHSA published a notice in the Federal Register (87 FR71346) inviting the public and other federal agencies to comment on plans to submit this request. SAMHSA did not receive any comment(s).

9. Paying Respondents

No payments or gifts are given to holders of user accounts in the system.

10. Assurance of Confidentiality

All personal identifiers are protected under the Privacy Act of 1974 and SAMHSA confidentiality privacy and practices.

11. Justification for Sensitive Questions

NSDUH collects data that includes sensitive information (for example, sex assigned at birth, sexual identity, race/ethnicity, income, education, and/or drug use or mental health problems). Questions of this nature require some sensitivity in how they are worded and approached. In face-to-face data collection, every attempt was made to ensure the interview was conducted in as private a setting as possible. The data that the applicant is requesting will not be retained once the data have been analyzed, nor will the information become part of the applicant's output that can be used for retrieval.

12. Estimate of Hour Burden

The amount of time to complete the agreements and other paperwork that comprise SAMHSA security requirements will vary based on the confidential data assets requested. To obtain access to SAMHSA confidential data assets, it is estimated that the average time to complete and submit SAMHSA's data security agreements and other paperwork is 40 minutes. This estimate does not include the time needed to complete and submit an application within the SAP Portal. All efforts related to SAP Portal applications occur prior to and separate from SAMHSA's effort to collect information related to data security requirements.

The expected number of applications in the SAP Portal that receive a positive determination from SAMHSA in a given year may vary. Overall, per year, SAMHSA estimates it will collect data security information for 15 application submissions that received a positive determination within the SAP Portal. SAMHSA estimates that the total burden for the collection of information for data security requirements over the course of the three-year OMB clearance will be about 30 hours and, as a result, an average annual burden of 10 hours.

- Type of submission: Security documents and paperwork
- Average submission time: 40 minutes
- Annual number of security form submissions: 15 submissions
- Total burden hours over the three-year OMB clearance: 3 years x [time to complete security forms] x [number of approved applications] = 30 hours
- Annual burden hours over the three-year OMB clearance: 30 hours/3 years = 10 hours

The total cost to applications requesting access to SAMHSA data for the 30 total burden hours is estimated to be \$1,053.

This estimate is based on an estimated median annual salary of \$73,000 per applicant.¹ Assuming a 40-hour workweek and a 52-week salary, this annual salary translates to an hourly salary of \$35.10. Over the three-year OMB clearance period, the average annual cost to the public for SAMHSA’s security forms is estimated to be \$351.

Category of Respondents	Number of Respondents	Number of Responses	Total Responses	Hours per Response	Total Hours
Data Requesters	15	3	45	0.67	30
Total			45		30

13. Estimate of Cost Burden

Not applicable. SAMHSA does not impose any fees, charges, or costs to individuals submitting SAMHSA’s security forms.

14. Cost to Federal Government

We estimate the average annual cost to the Federal Government for the collection and review of SAMHSA security documents to be approximately \$150,000 per year for Fiscal Years 2023, 2024, and 2025. These figures are based on required contractual and staff resources necessary to collect and review documents given the expected annual number of submitted applications.

15. Reason for Change in Burden

Not applicable.

¹Applicant salary estimates were based on annual median salary estimates for employed college graduates using data from the 2019 National Survey of College Graduates.

16. Project Schedule

The information provided by applicants to SAMHSA is received on an ongoing basis and is not subject to any schedule. Users provide information voluntarily and at their discretion.

17. Request to Not Display Expiration Date

The expiration date of OMB approval will be displayed on SAMHSA's security forms.

18. Exceptions to the Certification

There are no exceptions.

B. Collections of Information Employing Statistical Methods

Not applicable. Because applications requesting access to SAMHSA data are voluntary, this information collection will not employ statistical methods.