DEPAR

Substance Abuse and Mental Health Services Administration

Proposed Information Collection Activity; Data Security Requirements for Accessing Confidential Data

AGENCY: Substance Abuse and Mental Health Services Administration; Center for Behavioral Health Statistics and Quality; Department of Health and Human Services.

ACTION: Submission for OMB review; comment request.

SUMMARY: Substance Abuse and Mental Health Services Administration (SAMHSA) within the Department of Health and Human Services has submitted the following information collection requirement to OMB for review and clearance under the Paperwork Reduction Act of 1995. This is the second notice for public comment; the first was published in the Federal Register on November 22, 2022 and no comments were received. SAMHSA is forwarding the proposed Data Security Requirements for Accessing Confidential Data information collection to the Office of Management and Budget (OMB) for clearance simultaneously with the publication of this second notice. The full submission may be found at: http://www.reginfo.gov/public/do/PRAMain.

DATES: Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to www.reginfo.gov/public/do/PRAMain . Find this particular information collection by selecting "Currently under 30-day Review - Open for Public Comments" or by using the search function.

FOR FURTHER INFORMATION CONTACT: Carlos Graham, SAMHSA Reports Clearance Officer, 5600 Fishers Lane, Room 15E57-A, Rockville, Maryland 20857, ***OR*** e-mail a copy to **Carlos.Graham@samhsa.hhs.gov**.

SUPPLEMENTARY INFORMATION: SAMHSA may not conduct or sponsor a collection of information unless the collection of information displays a currently valid OMB control number and the agency informs potential persons who are to respond to the collection of information that

such persons are not required to respond to the collection of information unless it displays a currently valid OMB control number.

Comments: Comments regarding (a) whether the collection of information is necessary for the proper performance of the functions of [agency], including whether the information will have practical utility; (b) the accuracy of [agency's] estimate of the burden of the proposed collection of information; (c) ways to enhance the quality, use, and clarity of the information to be collected, including through the use of automated collection techniques or other forms of information technology; (d) ways to minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated or other forms of information technology should be addressed to the points of contact in the FOR FURTHER INFORMATION CONTACT section.

Title of collection: Data Security Requirements for Accessing Confidential Data

OMB Control Number: 3145-0271

Summary of Collection: Title III of the Foundations for Evidence-Based Policymaking Act of 2018 (44 U.S.C. 3583; hereafter referred to as the Evidence Act) mandates that 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 to be a process through which agencies, the Congressional Budget Office, State, local, and Tribal governments, researchers, and other individuals, as appropriate, may apply to access confidential data assets held by a federal statistical agency or unit for the purposes of developing evidence. 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. When an application for confidential data is approved through the SAP Portal, SAMHSA will collect information to fulfill its data security requirements. This is a required step before providing the individual with access to restricted use 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. SAMHSA's collection of data security information will occur outside of the SAP Portal.

The following bullets outline the major components and processes in and around the SAP Portal, leading up to SAMHSA's collection of security requirements.

- *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 SAP Policy may be found in OMB Memorandum 23-04.
- *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 provides a streamlined application process across agencies, reducing redundancies in the application process.
- *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.

- *SAP Portal Application Process*: Individuals who have identified and wish to access confidential data assets apply through the SAP Portal. Applicants must create an account and follow all steps to complete the application. Applicants enter personal, contact, and institutional information for the research team and provide summary information about their proposed project.
- *Submission for Review*: Agencies approve or reject an application within a prompt timeframe. Agencies may also request applicants to revise and resubmit their application.
- *Access to Confidential Data*: Approved applicants are notified through the SAP Portal that their proposal has been accepted. This concludes the SAP Portal process. Agencies will contact approved applicants to initiate completion of their security documents. 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 an 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.

Estimate of Burden: The amount of time to complete the agreements and other paperwork that comprise SAMHSA's 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.

Comments: As required by 5 CFR 1320.8(d), comments on the information collection activities as part of this study were solicited through the publication of a 60-Day Notice in the Federal Register at [insert FR citation]. SAMHSA received [number] comments, to which we here respond.

Updates: This section is needed if there have been any major changes since the first FRN was published, for example, if estimates of burden (in terms of hours or respondents), scope, sampling, etc. were changed. Outline what the initial FRN specified, the new information, and the reason(s) why it changed.

Carlos Graham,

Reports Clearance Officer.

[FR Doc. 2023-17176 Filed: 8/9/2023 8:45 am; Publication Date: 8/10/2023]