**Billing Code:** 4184-29-P

**DEPARTMENT OF HEALTH AND HUMAN SERVICES**

**Administration for Children and Families**

**Privacy Act of 1974; System of Records**

**AGENCY:** Administration for Children and Families, Department of Health and Human Services.

**ACTION:** Notice of a modified system of records.

**SUMMARY:** In accordance with the requirements of the Privacy Act of 1974, as amended, the Department of Health and Human Services (HHS) is altering an existing department wide system of records, "Records About Restricted Dataset Requesters," System Number 09-90-1401, to add records maintained by HHS' Administration for Children and Families (ACF) and to make other changes, including changing the system of records name to "Records About Requesters of Restricted Datasets." This system of records covers records about individuals within and outside HHS who request restricted datasets and software products from HHS (e.g., for health-related scientific research and study purposes), when HHS maintains the requester records in a system from which they are retrieved directly by an individual requester's name or other personal identifier.

**DATES:** In accordance with 5 U.S.C. 552a(e)(4) and (11), this modified system of records is effective [INSERT DATE OF PUBLICATION IN THE *FEDERAL REGISTER*], subject to a 30-day comment period on the revised routine use described below. Please submit any comments by [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

**ADDRESSES:** The public should submit written comments, by mail or email, to Anita Alford, Senior Official for Privacy, Administration for Children and Families, 330 C Street SW, Washington DC 20201, or anita.alford@hhs.gov.

**FOR FURTHER INFORMATION CONTACT:** General questions about the system of records should be submitted by mail or email to Beth Kramer, HHS Privacy Act Officer, at 200 Independence Ave. SW - Suite 729H, Washington, DC 20201, or beth.kramer@hhs.gov, or (202) 690-6941.

**SUPPLEMENTARY INFORMATION:** This departmentwide system of records covers records about individuals within and outside HHS who request restricted datasets and software products from HHS, when HHS maintains the requester records in a record system they are retrieved directly by an individual requester's name or other personal identifier. It currently includes records maintained by four HHS Operating Divisions. It is being revised to add records maintained by a fifth Operating Division, the Administration for Children and Families (ACF), and to make other changes, as explained below:

- The system of records name has been changed to "Records About Requesters of Restricted Datasets."
- The alterations made to add ACF's records affect the System Location, System Manager(s), Authorities, Categories of Records, and Retention sections of the System of Records Notice (SORN).
- Centers for Medicare and Medicaid Services (CMS) and Substance Abuse and Mental Health Services Administration (SAMHSA) System Manager information has been updated.
- In the Categories of Records section, additional examples of records (license application, data protection plan, and Institutional Review Board (IRB) approval records) have been added.
- Routine use 6, authorizes disclosures to the U.S. Department of Justice (DOJ) or a court in litigation, has been revised to change "litigation" to "litigation or other proceedings" and to remove wording that required the disclosures to be compatible with the purpose the original disclosed information was collected, which is redundant because it repeats

part of the definition of a routine use.

- The sections specifying procedures for making access, amendment, and notification requests have been revised to reference HHS' Privacy Act regulations in 45 CFR; to state that the requests must contain the requester's full name, address, date of birth, and signature; and to require identity verification in the Contesting Records Procedures section and state that the right to contest records is limited to information that is factually inaccurate, incomplete, irrelevant, or untimely (obsolete).

"Restricted" datasets and software products are those that HHS makes affirmatively available to qualified members of the public but provides subject to restrictions, because they contain identifiable data and/or anonymized data that has the potential, when combined with other data, to identify the particular individuals, such as patients or providers, whose information is represented in the data; or because they contain other types of data that require confidentiality protection (for example, proprietary business data submitted to HHS with restrictions imposed by the submitting entity). The datasets and products are made available through an on-line or paper-based ordering and delivery system that provides them to qualified requesters electronically or by mail.

The restrictions are necessary to protect the privacy of individuals whose information is represented in the datasets or software products, or to protect proprietary business interests or other interests needing confidentiality protection. The restrictions typically limit the data requester to using the data for research, analysis, study, and aggregate statistical reporting; prohibit any attempt to identify any individual or establishment represented in the data or to reveal proprietary data or other protected data; and require specific security measures to safeguard the data from unauthorized access. HHS is required by law to impose, monitor, and enforce the restrictions (see, for example, provisions in the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA), 44 U.S.C. 3501 at note). To

impose and enforce the restrictions, it is necessary to collect information about the data requesters.

The modified system of records will cover records in the following five information technology (IT) systems, or any successor IT systems, about requesters of restricted datasets:

- *Administration for Children & Families, Children's Bureau (ACF/CB) "National Data Archive on Child Abuse and Neglect (NDACAN)."* NDACAN is a data repository maintained by a contractor funded by ACF's Children's Bureau, containing deidentified child abuse and neglect data from national surveys, large-scale longitudinal surveys, state administrative data, and data collected by individual investigators. NDACAN delivers distributable datasets to researchers who apply for and receive a license. No distributable datasets contain information that is directly identifying; however, some are restricted because they have the potential to identify particular individuals if combined with other data, and thus require researchers to not only obtain a license but also submit a data protection plan and obtain Institutional Review Board (IRB) approval to receive the dataset. Records about researcher-applicants who seek restricted datasets (including the license application, data protection plan, and IRB approval records) are retrieved by the researcher-applicant's name or other personal identifier, so are Privacy Act records. (NDACAN also collects identifiable customer information about researchers who seek unrestricted datasets, in order to deliver its products and services to them; however, because minimal information is collected about them, it would be covered by system of records 09-90-1901 if it is retrieved by personal identifier; see the below "Note.")
- *Agency for Healthcare Research and Quality (AHRQ) "Online Application Ordering for Products from the Healthcare Cost and Utilization Project (HCUP)."* HCUP is an online system established in 2013; it makes restricted databases and software available for qualified applicants to purchase for scientific research and public health use. Applicants may be researchers, patients, consumers, practitioners, providers, policy

makers, or educators. The HCUP databases are annual files containing anonymous information from hospital discharge records for inpatient care and certain components of outpatient care. The HCUP software tools enhance the use of the data. The online system supports AHRQ's mission of promoting improvements in health care quality.

- *Centers for Medicare & Medicaid Services (CMS) Data Use Agreement (DUA) tracking system*. This system tracks disclosures of data containing Protected Health Information (PHI) or Personally Identifiable Information (PII), including authorization, payment status, and shipping status of data extracts, between CMS, its contractors, and other authorized entities.
- *National Institutes of Health (NIH) "Controlled Data Access Systems."* NIH supports "NIH-designated data repositories" that archive and distribute controlled-access, de-identified human data and results from scientific studies under the NIH Genomic Data Sharing Policy. Controlled-access data in NIH-designated data repositories are made available for secondary research only after investigators have obtained approval from NIH to use the requested data for a particular project. The National Center for Biotechnology Information database of Genotypes and Phenotypes (dbGaP) serves as a central portal to submit, locate, and request access to controlled-access, human genomic (e.g., GWAS, sequencing, expression, epigenomic) data. The dbGaP's capacity and functionality are extended by repositories managed by public or private organizations through structured partnerships ("trusted partnerships") established by NIH through a contract mechanism. Information about investigators, Institutional Signing Officials, and other users of NIH-designated controlled access repositories may be located and viewed by approved staff using the dbGaP or trusted partner-managed systems. Sharing research data supports the mission of the NIH and is essential to facilitate the translation of research results into knowledge, products, and procedures that improve human health.
- *Substance Abuse and Mental Health Services Administration (SAMHSA) "Online Application for the Data Portal (SAMHDA)."* This online data portal was established

in 2013 to make restricted datasets from SAMHSA more efficiently available to designated, approved researchers. The Data Portal and all applications are maintained through the Substance Abuse and Mental Health Data Archive (SAMHDA). Currently, data from the Drug Abuse Warning Network (DAWN), DAWN Medical Examiner/Coroner component, National Survey on Drug Use and Health (NSDUH), and NSDUH Adult Clinical Interview data are available through the portal. Data recipients must complete a web-based application process and receive project approval from SAMHSA's Center for Behavioral Health and Statistics and Quality (CBHSQ), and they can use the datasets for statistical purposes only. No fees are charged for the datasets. The online portal supports SAMHSA's mission to make substance use and mental disorder information and research more accessible.

Note: This system of records does not include:

- *Records about requesters who seek unrestricted datasets, publications, or other information products from an HHS on-line or paper-based ordering and delivery system*. Unrestricted materials are also proactively made available to the public by HHS, but they are released without restrictions (though some may be subject to terms or conditions of use and require registration for an account and payment of a fee). Because the requests or order forms collect minimal information about the requester (i.e., the requester's name, mailing address or email address, telephone number, or other contact or delivery information, and payment information if a fee is imposed), they would be adequately covered by other SORNs (for example, 09-90-1901, HHS Correspondence, Comment, Customer Service, and Contact List Records and 09-90-0024 HHS Financial Management System Records), if a SORN is required (i.e., if the records are retrieved directly by an individual requester's name or other personal identifier). Examples include records about requesters who order materials online from AHRQ's Publications Online Store & Clearinghouse or by mail from AHRQ's Publications

Clearinghouse, which provide only unrestricted publications and other information products; and records about requesters ordering unrestricted datasets from CMS's DUA tracking system processes orders for both restricted and unrestricted datasets.

- *Records about data requesters that are not retrieved directly by an individual requester's name or other personal identifier.* These records are not subject to the Privacy Act and are not required to be covered in a SORN, even when they are associated with a restricted dataset and include additional information about the requester (such as, the requester's intended research purpose, qualifications, signed Data Use Agreement, and confidentiality training certificate). An example would be requester records that are retrieved first by a dataset identifier and/or a requesting entity's name, and then by an individual researcher's or record custodian's name.

A report on the modified system of records has been sent to OMB and Congress in accordance with 5 U.S.C. 552a(r).

**Rebecca Jones Gaston,**

*Commissioner,*

*Administration on Children, Youth and Families.*

**SYSTEM NAME AND NUMBER:**

Records About Requesters of Restricted Datasets, 09-90-1401.

**SECURITY CLASSIFICATION:**

Unclassified.

**SYSTEM LOCATION:**

The address of each agency component responsible for the system of records is:

- *ACF*: Child Welfare Program Specialist, Children's Bureau, Administration for Children and Families, 330 C Street SW, Washington, DC 20201.
- *AHRQ*: HCUP Project Officer, Center for Delivery, Organization, and Markets, 540 Gaither Road, Rockville, MD 20850.

- *CMS*: DUA tracking system, Division of Data and Information Dissemination, Data Development and Services Group, Office of Enterprise Data and Analytics, Centers for Medicare & Medicaid Services, 7500 Security Blvd., Mailstop: B2-29-04, Office Location: B2-03-37, Baltimore, MD 21244-1870.
- *NIH*: Office of the Director, Office of Science Policy, Division of Scientific Data Sharing Policy, 6705 Rockledge Drive - Suite 750, Bethesda, MD 20817.
- *SAMHSA*: SAMHDA Project Officer, CBHSQ, 5600 Fishers Lane, Rockville, MD 20857.

**SYSTEM MANAGER(S):**

- *ACF*: Child Welfare Program Specialist, Children's Bureau, Administration for Children and Families, 330 C Street SW, Washington, DC 20201; Email: cara.kelly@acf.hhs.gov, or 202-205-8636.
- *AHRQ*: HCUP Project Officer, Center for Delivery, Organization, and Markets, 540 Gaither Road, Rockville, MD 20850; Telephone: 301-427-1410; HCUP@AHRQ.GOV.
- *CMS*: DUA tracking system, Office of Enterprise Data and Analytics, Data & Information Dissemination Group, Centers for Medicare & Medicaid Services, 7500 Security Blvd., Mailstop: B2-29-04, Office Location: B2-03-37, Baltimore, MD 21244-1870; datauseagreement@cms.hhs.gov.
- *NIH*: Office of the Director, Office of Science Policy, Division of Scientific Data Sharing Policy, 6705 Rockledge Drive - Suite 750, Bethesda, MD 20817.
- *SAMHSA*: SAMHDA Project Officer, CBHSQ, 5600 Fishers Lane, Rockville, MD 20857; 877-726-4727. ("SAMHDA" refers to Substance Abuse and Mental Health Data Archive.)

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

The following legal authorities authorize the collection and maintenance of these records:

- *ACF*: 42 U.S.C. 5101 et seq.; 45 CFR 1355.40 and 1356.80 through 1356.86.

- *AHRQ*: 42 U.S.C. 299 through 299a and 299c-2.
- *CMS*: 5 U.S.C 552a(e)(10); 45 CFR 164.514(e); 44 U.S.C. 3544; 42 U.S.C. 1306.
- *NIH*: 42 U.S.C. 217a, 241, 281, 282, and 284; 48 CFR subpt. 15.3; E.O. 13478.
- *SAMHDA*: 42 U.S.C. 290aa(d)(l); 44 U.S.C. 3501(8).

*See also*: CIPSEA, codified at 44 U.S.C. 3501 note.

**PURPOSE(S) OF THE SYSTEM:**

The purposes of this system of records are to provide restricted datasets and software products to qualified data requesters in a timely and efficient manner and consistent with applicable laws, and to enable HHS to enforce data requesters' compliance with use and security restrictions that apply to the data. Relevant HHS personnel use the records on a need-to-know basis for those purposes; specifically:

- *Contact and user registration information* is used to communicate with the requester, enable the requester to access requested data electronically (for example, the requester's email address would be used to register the requester to use a public access web portal or link, and to notify the requester when data has been delivered electronically to his registered account), locate the requester (e.g., for on-site inspections or to otherwise check compliance with the data use agreement), and deliver and track data provided by mail (e.g., to document receipt for enforcement purposes and report lost shipments to security personnel).
- *Qualifications, planned use of the data, confidentiality training information, signed data use agreement, data receipt information, on-site inspection information, and information about data breaches or contract violations* is used to grant the request (consistent with data use restrictions) or deny the request, bind the requester to the applicable data use restrictions and other security requirements, conduct on-site inspections or otherwise check the requester's compliance with the data use agreement, enforce the agreement if breached, and share information about data breaches and

contract violations with other HHS components administering restricted dataset requests involving the same requesters.

- *Payment information* is used to collect any applicable fee. Any payment information shared with HHS accounting and debt collection systems is also covered under the accounting and debt collection systems' SORNs and is subject to the routine uses published in those SORNs (see, e.g., HHS Financial Management System Records, SORN #09-90-0024; and Debt Management and Collection System, SORN #09-40-0012).
- *Any of the above records* could be used to evaluate accomplishment of HHS functions related to the purposes of this system of records and to evaluate performance of contractors utilized by HHS to accomplish those functions.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

The records are about individuals within and outside HHS who request restricted datasets and software products that HHS makes proactively available to qualified members of the public, usually for health-related scientific research and study purposes. Examples include individual researchers and records custodians, project officers, or other representatives of entities such as universities, government agencies, and research organizations.

**CATEGORIES OF RECORDS IN THE SYSTEM:**

The categories of records include:

- *Request records*, containing the requester's name and contact information (telephone number, mailing address, email address), affiliated entity (e.g., if making the request as a records custodian or other employee), and a description of the dataset requested.
- *Order fulfillment records*, containing user registration information such as email address and IP address (if the requester is provided access to the dataset electronically through a public access web portal or link) or mailing information (if the dataset is mailed to the requester on a disk or other media), and tracking information (providing

proof of delivery).

- *Data use restriction records*, containing the requester's identification, contact, and affiliated entity information, qualifications, intended use of the data (e.g., study name, contract number), confidentiality training documentation (e.g., a coded number indicating the individual completed required confidentiality training), signed and notarized data use agreement documents (e.g., license application; affidavit of nondisclosure; declaration of nondisclosure; confidential data use and nondisclosure agreement (CDUNA); data protection plan; individual designations of agent; DUA number and expiration date; Institutional Review Board (IRB) approval records), tracking information, and any on-site inspection information.
- *Payment records (if a fee is charged)*, consisting of the requester's credit card account name, number, and billing address, or bank routing number and checking account name, address, and number.

**RECORD SOURCE CATEGORIES:**

Information in this system of records is obtained directly from the individual data requester to whom it applies or is derived from information supplied by the individual or provided by HHS officials.

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:**

Information about an individual dataset requester may be disclosed to parties outside HHS, without that individual's consent, as provided in these routine uses:

1. Disclosures may be made to federal agencies and department contractors that have been engaged by HHS to assist in accomplishment of an HHS function relating to the purposes of this system of records (including ancillary functions, such as compiling reports and evaluating program effectiveness and contractor performance) and that have a need to have access to the records in order to assist HHS in performing the activity.

Any contractor will be required to comply with the requirements of the Privacy Act.

2. Records may be disclosed to student volunteers, individuals working under a personal services contract, and other individuals performing functions (including ancillary functions) relating to the purposes of this system of records for the department but technically not having the status of agency employees if they need access to the records in order to perform their assigned agency functions. For example, disclosure may be made to qualified experts not within the definition of HHS employees as prescribed in HHS regulations, for opinions as a part of the controlled data access process.
3. CMS records may be disclosed to a CMS contractor (including but not limited to Medicare Administrative Contractors, fiscal intermediaries, and carriers) that assists in the administration of a CMS-administered health benefits program, or to a grantee of a CMS-administered grant program, when disclosure is deemed reasonably necessary by CMS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud, waste, or abuse in such program.
4. Records may be disclosed to another federal agency or an instrumentality of any governmental jurisdiction within or under the control of the United States (including any state or local governmental agency) that administers federally funded programs, or that has the authority to investigate, potential fraud, waste or abuse in federally funded programs, when disclosure is deemed reasonably necessary by HHS to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy or otherwise combat fraud, waste or abuse in such programs.
5. When a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate public authority,

whether federal, foreign, state, local, tribal, or otherwise, responsible for enforcing, investigating or prosecuting the violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to the enforcement, regulatory, investigative, or prosecutorial responsibility of the receiving entity.

6. Information may be disclosed to the U.S. Department of Justice (DOJ) or to a court or other tribunal, in litigation or other proceedings, when:
   a. the agency or any component thereof, or
   b. any employee of the agency in his or her official capacity, or
   c. any employee of the agency in his or her individual capacity where DOJ has agreed to represent the employee, or
   d. the United States Government

   is a party to the proceedings or has an interest in the proceedings and, by careful review, HHS determines that the records are both relevant and necessary to the proceedings.
7. Records may be disclosed to a federal, foreign, state, local, tribal, or other public authority of the fact that this system of records contains information relevant to the hiring or retention of an employee, the retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for further information if it so chooses. HHS will not make an initial disclosure unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to another federal agency for criminal, civil, administrative, personnel, or regulatory action.
8. Information may be disclosed to a Member of Congress or Congressional staff member in response to a written inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained. The Congressional office does

not have any greater authority to obtain records than the individual would have if requesting the records directly.

9. Records may be disclosed to the U.S. Department of Homeland Security (DHS) if captured in an intrusion detection system used by HHS and DHS pursuant to a DHS cybersecurity program that monitors Internet traffic to and from federal government computer networks to prevent a variety of types of cybersecurity incidents.
10. Disclosures may be made to appropriate agencies, entities, and persons when (1) HHS suspects or has confirmed that there has been a breach of the system of records; (2) HHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, HHS (including its information systems, programs, and operations), the federal government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with HHS efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
11. Disclosure may be made to another federal agency or federal entity, when HHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the federal government, or national security, resulting from a suspected or confirmed breach.
12. Disclosure of past performance information pertaining to contractors engaged by HHS to assist in accomplishment of an HHS function relating to the purposes of this system of records may be made to a federal agency upon request and may include information about dataset requesters.
13. NIH dataset requester records may be included in records disclosed to governmental or authorized non-governmental entities with a signed data access agreement for system data

that includes records about individuals requesting and receiving restricted datasets, to use in compiling reports (such as, on the composition of biomedical and/or research workforce; authors of publications attributable to federally funded research; information made available through third-party systems as permitted by applicants or awardees for agency grants or contracts; or grant payment information reported to federal databases).

14. When records about a requester of an NIH restricted dataset are related to an award or application for award under an NIH award program, the dataset requester records may be disclosed to the award applicant, principal investigator(s), institutional officials, trainees or others named in the application, or institutional service providers for purposes of application preparation, review, or award management, and to the public consistent with reporting and transparency standards and to the extent disclosure to the public would not cause an unwarranted invasion of personal privacy.
15. HHS may disclose records from this system of records to the National Archives and Records Administration (NARA), General Services Administration (GSA), or other relevant federal agencies in connection with records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

Information about a dataset requester may also be disclosed from this system of records to parties outside HHS without the individual's consent for any of the uses authorized directly in the Privacy Act at 5 U.S.C. 552a(b)(2) and (b)(4) through (11).

**POLICIES AND PRACTICES FOR STORAGE OF RECORDS:**

Records are stored in electronic databases and hard-copy files. CMS' DUA tracking system records may also be stored on portable media.

**POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:**

Records are retrieved by the data requester's name, registrant/user name, User ID Number, email address, or DUA number.

**POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:**

Records needed to enforce data use restrictions are retained for 20 years by AHRQ (see DAA-0510-2013-0003-0001), 5 years by CMS (see Nl-440-10-04), and 3 years by NIH (see DAA-0443-2013-0004-0004) after the agreement is closed, and may be kept longer if necessary for enforcement, audit, legal, or other purposes. The equivalent ACF and SAMHSA records will be retained indefinitely until a disposition schedule is approved by the National Archives and Records Administration (NARA). Records of payments made electronically are transmitted securely to a Payment Card Industry-compliant payment gateway for processing and are not stored. Records of payments made by check, purchase order, or wire transfer are disposed of once the funds have been received. Records are disposed of using destruction methods prescribed by NIST SP 800-88.

**ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:**

Records are safeguarded in accordance with applicable laws, rules, and policies, including HHS policies, pertinent National Institutes of Standards and Technology (NIST) publications, and OMB Circular A-130, Managing Information as a Strategic Resource. Records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. Safeguards conform to the HHS Information Security and Privacy Program, https://www.hhs.gov/ocio/securityprivacy/.

The safeguards include protecting the facilities where records are stored or accessed with security guards, badges and cameras; securing hard-copy records in locked file cabinets, file rooms or offices during off-duty hours; limiting access to electronic databases to authorized users based on roles and the principle of least privilege, and two-factor authentication (user ID and password); using a secured operating system protected by encryption, firewalls, and intrusion detection systems; using an SSL connection for secure encrypted transmissions, and requiring encryption for records stored on removable media; and training personnel in Privacy Act and information security requirements.

**RECORD ACCESS PROCEDURES:**

An individual who wishes to access records about him or her in this system of records must submit a written access request to the relevant System Manager at the address indicated in the "System Manager(s)" section above, in accordance with the Department's Privacy Act implementation regulations in 45 CFR. The request must contain the requester's full name, address, date of birth, and signature. The individual must verify his or her identity by providing either a notarized request or a written certification that the requester is who he or she claims to be and understands that the knowing and willful request for acquisition of a record pertaining to an individual under false pretenses is a criminal offense under the Privacy Act, subject to a fine of up to $5,000.

**CONTESTING RECORD PROCEDURES:**

An individual seeking to correct a record about him or her in this system of records must submit a written correction request to the relevant System Manager at the address indicated in the "System Manager(s)" section above, in accordance with the Department's Privacy Act implementation regulations in 45 CFR. The request must contain the requester's full name, address, date of birth, and signature, reasonably identify the record, specify the information contested, and state the corrective action sought and the reasons for the correction. The request should include any supporting documentation. The individual must verify his or her identity in the same manner required for an access request. The right to contest records is limited to information that is factually inaccurate, incomplete, irrelevant, or untimely (obsolete).

**NOTIFICATION PROCEDURES:**

An individual who wishes to know if this system of records contains a record about him or her must submit a written notification request to the relevant System Manager at the address indicated in the "System Manager(s)" section above, in accordance with the Department's Privacy Act implementation regulations in 45 CFR. The request must contain the requester's full name, address, date of birth, and signature. The individual must verify his or her identity in the same manner required for an access request.

**EXEMPTIONS PROMULGATED FOR THE SYSTEM:**

None.

**HISTORY:**

83 FR 11213 (Mar. 14, 2018).

[FR Doc.
2023-23147
Filed:
10/19/2023
8:45 am;
Publication
Date:
10/20/2023]