Billing Code: 4120-03

Department of Health and Human Services

Office of the Secretary

Privacy Act of 1974; System of Records Notice

AGENCY: Department of Health and Human Services (HHS), Office of the Secretary (OS)

ACTION: Notice to establish a new system of records and delete an existing system of records.

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, as amended (5 USC 552a), HHS is establishing a new department-wide system of records, "Records about Restricted Dataset Requesters," System Number 09-90-1401, to cover 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. The System of Records Notice (SORN) previously published at 78 FR 32654 for "Online Application Ordering for Products from the Healthcare Cost and Utilization Project (HCUP)," System Number 09-35-0003, is being deleted and replaced by this new department-wide SORN.

DATES: Effective Dates: The department-wide SORN proposed in this Notice is effective

upon publication, with the exception of the routine uses. The routine uses will be effective 30 days after publication of this Notice, unless comments are received that warrant revisions to this Notice. Written comments on the routine uses should be submitted within 30 days. The deletion of System Number 09-35-0003 will be effective 30 days after publication of this Notice.

ADDRESSES: The public should address written comments to: Beth Kramer, HHS Privacy Act Officer, Mary E. Switzer Building – Room 2210, 330 C Street, S.W., Washington, DC 20201, beth.kramer@hhs.gov. Comments will be available for public viewing at the same location. To review comments in person, please contact Beth Kramer at beth.kramer@hhs.gov or (202) 690-6941.

FOR FURTHER INFORMATION CONTACT: Beth Kramer, HHS Privacy Act Officer, Mary E. Switzer Building – Room 2210, 330 C Street, S.W., Washington, DC 20201, beth.kramer@hhs.gov.

SUPPLEMENTARY INFORMATION:

The new system of records will cover records about individuals within and outside HHS who request restricted datasets and software products from HHS, 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. "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. 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. 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; 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 USC 3501 at note). To impose and enforce the restrictions, it is necessary to collect information about the data requesters.

Currently, this system of records covers data requester records in ordering and delivery systems administered by three HHS Operating Divisions, but only to the extent that the records pertain to requesters seeking *restricted* datasets. These ordering and delivery systems retrieve requester records directly by personal identifier:

- 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 Agreement & Data Shipping Tracking System (DADSS)." DADSS was established in 2004 to track authorization, payment status, shipping status, and ownership of restricted and unrestricted data extracts between CMS, its contractors, and other authorized entities. DADSS is slated to be replaced in 2015 with an electronic information system designed to provide a traceable record of CMS' data disclosures.
- Substance Abuse and Mental Health Services Administration (SAMHSA) "Online Application for the Data Portal (SAMHDA)." This online data portal was established in 2013 to more efficiently make restricted datasets from SAMHSA 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 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 that 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 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, "Correspondence Tracking Management System (CTMS)" SORN #09-70-3005; "Consumer Mailing List" SORN #09-90-0041; and "Unified Financial Management System (UFMS)" SORN #09-90-0024 if a fee is involved), 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 current DADSS system and its successor, which 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 name and/or a requesting entity's name, and then by an individual researcher's or record custodian's name.

The Privacy Act (5 USC 552a) governs the means by which the U.S. Government collects, maintains, and uses information about individuals in a system of records. A "system of records" is a group of any records under the control of a federal agency from which information about an individual is retrieved by the individual's name or other personal identifier. The Privacy Act requires each agency to publish in the *Federal Register* a system of records notice (SORN) identifying and describing each system of records the agency maintains, including the purposes for which the agency uses information about individuals in the system, the routine uses for which the agency discloses such information outside the agency, and how individual record subjects can exercise their rights under the Privacy Act.

A report on the proposed new system of records has been sent to OMB and Congress in accordance with 5 USC 552a(r).

SYSTEM NUMBER:

09-90-1401

SYSTEM NAME:

Records About Restricted Dataset Requesters

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATIONS:

Electronic files are maintained at the following server locations:

- AHRQ: Social & Scientific Systems Data Center, Ashburn, Virginia
- CMS: CMS Data Center, Baltimore, Maryland
- SAMHSA: Substance Abuse and Mental Health Data Archive, Rockville, Maryland

Hard-copy files are maintained at the System Manager locations; see "System Manager(s)" section below.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

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:

Categories of records include:

1. 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.
2. 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).
3. 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., Affidavit of Nondisclosure; Declaration of Nondisclosure; Confidential Data Use and Nondisclosure Agreement (CDUNA); Individual Designations of Agent; DUA number and expiration date), tracking information, and any on-site inspection information.
4. 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.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

AHRQ: 42 USC 299-299a; 42 USC 299c-2

CMS: 5 USC 552a(e)(10); 45 CFR 164.514(e); 44 USC 3544; 42 USC 1306

SAMHDA: 42 USC 290aa(d)(1); 44 USC 3501(8)

See also: CIPSEA, codified at 44 USC 3501 note.

PURPOSE(S) OF THE SYSTEM:

The purposes of this system of records is 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., United Financial Management System, SORN #09-90-0024; and Debt Management and Collection System, SORN #09-40-0012).

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

Information about an individual data requester may be disclosed to parties outside HHS without the individual's prior, written consent pursuant to the following 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 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 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.

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, 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 litigation or has an interest in such litigation and, by careful review, HHS determines that the records are both relevant and necessary to the litigation and that, therefore, the use of such records by the DOJ, court or other tribunal is deemed by HHS to be compatible with the purpose for which the agency collected the records.
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 federal agencies and Department contractors that have a need to know the information for the purpose of assisting the Department's efforts to respond to a suspected or confirmed breach of the security or confidentiality of information maintained in this system of records, when the information disclosed is relevant and necessary to that assistance.

Information about an individual data 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 USC 552a(b)(2) and (b)(4)-(11).

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM—

STORAGE:

Records are stored in electronic databases and hard-copy files. DADSS, and its successors', records may also be stored on portable media.

RETRIEVABILITY:

Records are retrieved by the data requester's name, registrant/user name, User ID number, or data use agreement (DUA) number.

SAFEGUARDS: Records are safeguarded in accordance with applicable laws, rules and policies, including the HHS Information Technology Security Program Handbook, all pertinent National Institutes of Standards and Technology (NIST) publications, and OMB Circular A-130, Management of Federal Resources. Records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. Safeguards conform to the HHS Information Security and Privacy Program, http://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, requiring encryption for records stored on removable media, and training personnel in Privacy Act and information security requirements.

RETENTION AND DISPOSAL: Records needed to enforce data use restrictions are retained for 20 years by AHRQ (see DAA-0510-2013-0003-0001) and 5 years by CMS

(see N1-440-10-04) after the agreement is closed, and may be kept longer if necessary for enforcement, audit, legal, or other purposes. The equivalent SAMHSA records will be retained indefinitely until a disposition schedule is approved by the National Archives and Records Administration (NARA). SAMHSA anticipates proposing a 5 year retention period to 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.

SYSTEM MANAGER(S) AND ADDRESS(ES):

- AHRQ: HCUP Project Officer, Center for Delivery, Organization, and Markets, 540 Gaither Road, Rockville, MD 20850; Telephone: 301-427-1410; HCUP@AHRQ.GOV.
- CMS: DADSS and its successor, Division of Data and Information Dissemination, Data Development and Services Group, Office of Enterprise Data and Analytics, Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Mailstop: B2-29-04, Office Location: B2-03-37, Baltimore, MD 21244-1870.
- SAMHSA: SAMHDA Project Officer, CBHSQ, 1 Choke Cherry Road, Rockville, MD 20857.

NOTIFICATION PROCEDURE:

An individual who wishes to know if this system of records contains records about him or her

should submit a written request to the relevant System Manager at the address indicated above. 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 five thousand dollar fine.

RECORD ACCESS PROCEDURE:

Same as notification procedure.

CONTESTING RECORD PROCEDURES:

An individual seeking to amend the content of information about him or her in this system should contact the relevant System Manager and reasonably identify the record, specify the information contested, state the corrective action sought, and provide the reasons for the amendment, with supporting justification.

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.

EXEMPTIONS CLAIMED FOR THIS SYSTEM:

None.

Celeste Dade-Vinson
Health Insurance Specialist
Centers for Medicare & Medicaid Services

[FR Doc. 2015-07444 Filed: 3/31/2015 08:45 am; Publication Date: 4/1/2015]