Federal Government 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)–(11).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are stored in electronic databases and hard-copy files. CMS's 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 data use agreement (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 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.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL 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, 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, *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.

RECORD ACCESS PROCEDURES:

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.

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.

NOTIFICATION PROCEDURES:

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.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

80 FR 17447 (April 1, 2015).

[FR Doc. 2018–05176 Filed 3–13–18; 8:45 am]

BILLING CODE 4140–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Privacy Act of 1974; System of Records Notice

AGENCY: Health Resources and Services Administration (HRSA), Department of Health and Human Services (HHS).

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the Privacy Act, HHS is establishing a new system of records to be maintained by HRSA System No. 09–15–0092 ''HRSA Trainee Information Portal (TRIP).'' The new system of records will cover data about health professionals/trainees receiving health care training supported by Bureau of Health Workforce (BHW) Federal awards (including, grants, cooperative agreements, contracts, scholarships and loans) (collectively referred to as awards), which BHW will use in evaluating the success of its programs. The new system of records is explained in the ''Supplementary Information'' section of this notice and fully described in the System of Records Notice (SORN) published in this notice.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this notice is effective upon publication, subject to a 30-day period in which to comment on the routine uses, described below. Please submit any comments by April 13, 2018.

ADDRESSES: The public should address written comments on the new system of records to Director, National Center for Health Workforce Analysis (NCHWA), BHW, HRSA, 5600 Fishers Lane, Rockville, Maryland 20857.

FOR FURTHER INFORMATION CONTACT: General questions about the system of records may be submitted to Director, National Center for Health Workforce Analysis (NCHWA), BHW, HRSA, 5600 Fishers Lane, Rockville, Maryland 20857.

SUPPLEMENTARY INFORMATION: Pursuant to the Government Performance and Results Act (GPRA) of 1993 and the GPRA Modernization Act of 2010, BHW requires all recipients of Health Professions awards to report annual performance data to BHW to enable BHW to determine the success of its programs. The performance data must include information about health

professionals who directly or indirectly benefit from a BHW award.

Currently, HRSA awardees submit performance data into the Electronic Handbooks (EHBs), an enterprise grants management system at HRSA. To reduce the reporting burden on awardees, BHW is developing a data collection portal that will allow awardees to collect individual-level trainee data (consisting of the trainee's name, training program, demographic information, aspects of their training, and employment information upon completion of training) directly from trainees via online surveys. For awardees that decide to communicate with trainees for this data collection, trainee email addresses may also be included. The survey responses will be collected, monitored, and managed in the portal, and awardees will be able to transmit and submit the data electronically into EHBs. Awardees will be able to send reminders or notifications to the trainees for initial surveys or any follow-up reminders. Awardees will also have the ability to directly upload bulk individual-level data rather than key in every required data field.

Data elements collected in the portal about individual trainees will be the same as those already being collected in the EHBs; only the source and retrieval method are changing. Enabling awardees to collect individual level trainee data directly from trainees may result in more accurate annual reports to BHW. Retrieving information about individual trainees directly by trainee name or other personal identifier will improve BHW's ability to follow the trainees even after the completion of their training to find out if they are employed in health care and/or work in underserved areas, as required to evaluate the effectiveness and success of BHW health professions programs.

SYSTEM NAME AND NUMBER:

HRSA Trainee Data Collection Portal System, 09–15–0092.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

The address of the agency component responsible for the system of records is National Center for Health Workforce Analysis (NCHWA), BHW, HRSA, 5600 Fishers Lane, Rockville, Maryland 20857.

SYSTEM MANAGER(S):

Director, National Center for Health Workforce Analysis (NCHWA), BHW, HRSA, 5600 Fishers Lane, Rockville, Maryland 20857.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Section 761 of the Public Health Service Act (42 U.S.C. 294n), Health Professions Workforce Information and Analysis; Section 792 of the Public Health Service Act (42 U.S.C. 295k), Health Professions Data.

PURPOSE(S) OF THE SYSTEM:

The purpose of this system of records is to provide the agency with training data about individual health professionals benefitted by health care training funded by BHW programs, so that BHW can follow the trainees even after the completion of their training to find out if they are employed in health care and/or work in underserved areas, in order to evaluate the effectiveness and success of BHW health professions programs.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The records pertain to health care professionals who are reported by awardees as benefitting from health care training supported by BHW awards.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system will collect and store demographic, training and general employment related information about the trainees at awardee and other funding recipient locations supported by BHW awards. Records about a particular trainee will be grouped by program and will contain data elements such as those listed below:

Name; email address; HRSA unique ID; health professions training program; length of training program; National Provider Identifier (NPI) number (where applicable); enrollment status; sex; age; race; ethnicity; rural residential background status; disadvantaged background status; veteran status; BHW award received; academic years receiving BHW awards; % Full-Time Equivalent (FTE) paid; primary discipline; whether the individual received training in a primary care setting, medically underserved community, or rural area; number of hours of training received in a primary care setting, medically underserved community, or rural area; graduation/completion status; program attrition status; employment data city, state, and ZIP code; type of employment, training/employment status 1-year after graduation; employment status.

RECORD SOURCE CATEGORIES:

The sources of the trainee data reported to BHW will be Health Professions awardees and their trainees. Sources of the data BHW subsequently obtains to determine if trainees are employed in health care and/or work in underserved areas will include the trainees and their employers. NPI Number will be obtained from records maintained by HHS' Centers for Medicare & Medicaid Services.

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

Information about an individual trainee may be disclosed from this system of records to parties outside the agency without the individual's prior, written consent pursuant to these routine uses:

1. Any trainee data that a BHW awardee reports for its awards will be disclosed to that awardee organization, to use for its own award administrative purposes.

2. Records may be disclosed to agency contractors who have been engaged by the agency to assist in accomplishment of an HHS function relating to the purposes of this system of records and who need to have access to the records in order to assist HHS. Any contractor will be required to comply with the requirements of the Privacy Act.

3. 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.

4. Records may be disclosed 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's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

5. Records may be disclosed 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.

6. 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.

The disclosures authorized by publication of the above routine uses pursuant to 5 U.S.C. 552a(b)(3) are in addition to other disclosures authorized directly in the Privacy Act at 5 U.S.C. 552a(b)(4)–(11).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

The agency will maintain the records on database servers with disk storage and backup tapes.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

The agency will retrieve records about an individual trainee by the trainee's name or other personal identifier, such as unique ID or email address.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

BHW is developing a record retention policy and disposition schedule for Training Information Portal (TRIP) records. Until a disposition schedule has been approved by the National Archives and Records Administration (NARA), the records will be retained indefinitely.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Authorized users include awardees and internal users such as government and contractor personnel who will provide support. Other than awardees, users are required to obtain favorable adjudication for a Level 5 Position of Public Trust. Government and contractor personnel who support the system must attend security training, sign a Non-Disclosure Agreement, and sign the Rules of Behavior, which is renewed annually. Users are given role-based access to the system on a limited need-to-know basis. All physical and logical access to the system is removed upon termination of employment. The system leverages the current HRSA EHBs process for authentication and authorization of all external awardee users.

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, 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, *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. Records that are eligible for destruction will be disposed of using secure destruction methods prescribed by NIST SP 800–88.

RECORD ACCESS PROCEDURES:

An individual seeking access to records about himself or herself in this system of records must submit a written request to the System Manager (see above ''System Manager'' section). An access request must contain the name and address of the requester, email address or other identifying information, and his/her signature. To verify the requester's identity, the signature must be notarized or the request must include the requester's written certification that he/she is the person he/she claims to be and that he/she understands that the knowing and willful request for or acquisition of records pertaining to an individual under false pretenses is a criminal offense subject to a $5,000 fine. Requesters may also ask for an accounting of disclosures that have been made of their records, if any.

CONTESTING RECORD PROCEDURES:

An individual seeking to amend a record about him or her in this system of records must submit a written request to the System Manager (see above ''System Manager'' section). An amendment request must include verification of the requester's identity in the same manner required for an access request, and must reasonably identify the record and specify the information being contested, the corrective action sought, and the reasons for requesting the correction, along with supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant.

NOTIFICATION PROCEDURES:

An individual who wishes to know if this system of records contains records about himself or herself must submit a written request to the System Manager (see above ''System Manager'' section) and verify his or her identity in the same manner required for an access request.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

Dated: March 8, 2018.

George Sigounas,

Administrator.

[FR Doc. 2018–05062 Filed 3–13–18; 8:45 am]

BILLING CODE 4160–15–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

Submission for OMB Review; 30-Day Comment Request; Generic Clearance for the Collection of Qualitative Feedback on Agency Service Delivery (NIH)

AGENCY: National Institutes of Health, HHS.

ACTION: Notice.

SUMMARY: In compliance with the Paperwork Reduction Act of 1995, the National Institutes of Health (NIH) has submitted to the Office of Management and Budget (OMB) a request for review and approval of the information collection listed below.

DATES: Comments regarding this information collection are best assured of having their full effect if received within 30-days of the date of this publication.