

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

07/11/2017

OPDIV:

AHRQ

Name:

AHRQ Data Processing Support System (ADPSS)

PIA Unique Identifier:

P-9924063-864866

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Contractor

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

Describe the purpose of the system.

The ADPSS is a general data processing and analytic support environment located in the Social and Scientific Systems (SSS) Secure Data Center - General Support System (SDC GSS) in Ashburn, Virginia. The system is used to support general analytical/statistical programming activities for the Center for Financing, Access, and Cost Trends (CFACT), the Center for Delivery, Organization, and Markets (CDOM), the Center for Quality Improvement and Patient Safety (CQIIPS), and other Agency for Healthcare Research and Quality (AHRQ) Offices and Centers. Activities include data management, analytic file development and documentation, data analysis and special analytic requests for both internal and external stakeholders, and other technical support. All information stored and processed within the system originates from AHRQ or through AHRQ contractors, Westat and Truven Health Analytics (Truven).

Westat provides the National Health Interview Survey (NHIS) and the Medical Expenditure Panel Survey (MEPS) data and Truven provides the Healthcare Cost and Utilization Project (HCUP) data. Direct AHRQ contractors access the system to perform system development and system maintenance.

Describe the type of information the system will collect, maintain (store), or share.

The systems collect and store MEPS, NHIS, HCUP and the various sources of data that are used to produce the National Healthcare Quality and Disparities Report (NHQDR).

MEPS is a set of large-scale surveys of families and individuals, their medical providers (doctors, hospitals, pharmacies, etc.), and employers across the United States. MEPS data includes specific facts about health services that Americans use, such as how frequently they use them, the cost of these services, and how they are paid for, as well as data on the cost, scope, and breadth of health insurance held by and available to U.S. workers.

The MEPS Household Component collects data from a sample of families and individuals in selected communities across the United States, drawn from a nationally representative subsample of households that participated in the prior year's National Health Interview Survey (NHIS). This type of data includes health insurance offerings information, premiums information, and employee contributions to premiums and other plan details for their establishment as a whole. The NHIS is the principal source of information on the health of the civilian non-institutionalized population of the United States and is one of the major data collection programs of the National Center for Health Statistics (NCHS). The data are also used by the public health research community for epidemiologic and policy analysis of such timely issues as characterizing those with various health problems, determining barriers to accessing and using appropriate health care, and evaluating Federal health programs.

HCUP receives data through voluntary partnerships with state-level Data Organizations. HCUP Partner organizations allow authorized AHRQ staff, their contractors, and guest researchers to utilize hospital administrative billing data for research, tool development, and aggregate statistical reporting. Data received from HCUP Partner organizations contain no direct identifiers such as name, address, phone number, Social Security number, or any type of "key" allowing linkage to medical records. The ADPSS system contains "intramural" HCUP databases which are used by AHRQ staff, their contractors, and guest researchers for activities related to research, public health, and the development of HCUP software tools, products, and reports. Uses of the data also include activities such as producing statistics for other Federal agencies, the development of statistics used on AHRQ's Websites (e.g., HCUPnet), and for AHRQ's Quality Indicator program. Intramural HCUP data are not available to the public.

The NHQDR, mandated by the U.S. Congress, focuses on "national trends in the quality of health care provided to the American people" (42 U.S.C. § 299b-2(b)(2)) and "prevailing disparities in health care delivery as it relates to racial factors and socioeconomic factors in priority populations" (42 U.S.C. § 299a-1(a)(6)). The report tracks more than 250 health care process, outcome, and access measures, covering a wide variety of conditions and settings. Data years vary across measures; most trend analyses include data points from 2000-2002 to 2011-2012. It is important to note that the report provides a snapshot of health care prior to implementation of most of the health insurance expansions included in the Affordable Care Act (ACA) and serves as a baseline to track progress in upcoming years. An exception is rates of uninsurance, which we are able to track through the first half of 2014.

Direct contractors provide their AHRQ email addresses and first and last names, which are then used to provision an account for access to conduct system development and system maintenance tasks.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The system collects and stores data provided by AHRQ and their data collection contractors (Westat and Truven). Each year, Westat fields a new panel of approximately 10,000 households that are invited to participate in a series of 5 interviews over a 2 ½-year period. The design calls for a series of overlapping panels, making it possible each year to combine data from two different panels to create annual estimates for the U.S. civilian population. Respondents report detailed information on health care use and expenditures and a variety of topics related to the use of health care, such as health insurance coverage, employment, income, health conditions, and satisfaction with health care providers. Data collected from household respondents are supplemented with data collected from medical providers and pharmacies.

The ADPSS system contains “intramural” HCUP databases which are used by AHRQ staff, their contractors, and guest researchers for activities related to research, public health, and the development of HCUP software tools, products, and reports. Uses of the data also include activities such as producing statistics for other Federal agencies, the development of statistics used on AHRQ’s Websites (e.g., HCUPnet), and for AHRQ’s Quality Indicator program. Intramural HCUP data are not available to the public. HCUP data in the ADPSS system contain no direct identifiers such as name, address, phone number, Social Security number, or any type of “key” allowing linkage to medical records. AHRQ’s contractors typically receive the data from HCUP Partner organizations, then sends re-formatted data to AHRQ and SSS through Secure File Transfer Protocol (SFTP) for further contract work. SSS uses SAS to provide data analytics support for AHRQ health care research.

The system uses data to perform analysis on the following MEPs topics: Access to Health Care; Medicare/Medicaid/State Children's Health Insurance Program (SCHIP); Men's Health; Children's Insurance Coverage; Mental Health Disability; Minority Health; Elderly Health Care; Obesity; Employment Status; Prescription Drugs; Health Care Disparities; Preventive Care; Health Insurance Coverage; Priority Conditions – Arthritis, Asthma, Cancer, Diabetes, Emphysema and Bronchitis, Heart, High Blood Pressure, High Cholesterol and Strokes; Health Status; Quality of Health Care; Home Health Care; The Uninsured; Injuries; Usual Source of Care; Jobs; Vision Impairment; Medical Conditions; Women's Health.

The ADPSS system contains HCUP intramural databases to support AHRQ in performing research on a broad range of health policy issues, including cost and quality of health services, medical practice patterns, access to health care programs, and outcomes of treatments at the national, State, and local market levels. National (Nationwide) databases are utilized to identify, track, and analyze national trends in health care utilization, access, charges, quality, and outcomes. State-specific databases are utilized to investigate State-specific and multi-State trends in health care utilization, access, charges, quality, and outcomes.

MEPS intramural databases contain PII that includes Name; Mother’s maiden name; Phone number; Date of Birth; Mailing address; Employment status; Geographic information (county information and ZIP code); Fully-specified International Classification of Diseases (ICD) codes; Income/Asset information; Medical provider names; Medical record number; Hospital admission/discharge dates. HCUP intramural databases contain PII that includes county, ZIP codes, hospital admission/discharge dates, and medical provider identification.

Direct contractors provide their AHRQ email addresses and first and last names which are then used to provision an account for access to conduct system development and system maintenance tasks.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Date of Birth

Name

Mother's Maiden Name

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Employment Status

Geographic information

Medical provider names

Income/asset information

Hospital admission/discharge dates

Hospital admission/discharge dates

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees

Public Citizens

Patients

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

PII is collected and used within the MEPS component to support AHRQ's intramural health care research, including performing research on a broad range of health policy issues, including cost and quality of health services, medical practice patterns, access to health care programs, and outcomes of treatments at the national, State, and local market levels. National (Nationwide) databases are utilized to identify, track, and analyze national trends in health care utilization, access, charges, quality, and outcomes. State-specific databases are utilized to investigate State-specific and multi-State trends in health care utilization, access, charges, quality, and outcomes. Direct contractors' AHRQ email addresses and first and last names are used to provision account access to the system for development and maintenance activities.

Describe the secondary uses for which the PII will be used.

None

Identify legal authorities governing information use and disclosure specific to the system and program.

Section 913 and 306 of the Public Health Service (PHS) Act (42 U.S.C. § 299b-2 and 242k(b)). Sections 924(c) and 308(d) of the PHS Act (42 U.S.C. § 299c-3(c) and 242m(d)) provide authority for protecting restrictions on identifiable information about individuals.

Are records on the system retrieved by one or more PII data elements?

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Email

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Other

Identify the OMB information collection approval number and expiration date

OMB clearance has been obtained for information collected thru the application process for "restricted access public release" HCUP databases maintained on another IT system. OMB clearance does not apply to intramural HCUP data in the ADPSS system.

MEPS - OMB CONTROL NUMBER: 0935-0118

EXPIRATION DATE: 12/31/2018

Is the PII shared with other organizations?

No

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

The MEPS database contains personal information and when a household is first contacted, the respondent is given a document called "Important Information About Your Participation in MEPS." This hand-out provides all of the necessary information for providing consent to participate, including a description of the kinds of data that will be collected. It has been approved by the Westat IRB as the tool for obtaining implied consent to participate.

Direct contractors are informed by the system owner that their AHRQ email address and first and last name must be collected to verify employment status and to provision access to the system.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

Participation in any MEPS survey is voluntary and the respondent may withdraw at any time.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

To date, there have been no major changes to the system that would impact the collection or storage of an individual's PII so no process has been developed. The system will notify individuals of any changes to the system that would impact PII to obtain consent to the continued use of PII.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

Individuals that believe their PII was inappropriately obtained, used or disclosed may contact AHRQ at (301) 427-1104 to be routed to the correct system point of contact to address the concern. Any type of inappropriate use or disclosure will be dealt with by the system owner in conjunction with the AHRQ Privacy Office. Individuals who have concerns about the inaccuracy of their PII may contact the system owner or the AHRQ Senior Official for Privacy to directly address their concerns.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

The system operator maintains 1) an information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2) procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls. Reviews of information contained within the system are conducted at least every three (3) years.

Identify who will have access to the PII in the system and the reason why they require access.

Administrators:

The project maintains a role-based security group within Active Directory. Each user must be assigned to the project's security group in order to gain access to the project's resources. Administrators are given access to maintain system operations; however administrators do not use PII during maintenance activities.

Developers:

The project maintains a role-based security group within Active Directory. Each user must be assigned to the project's security group in order to gain access to the project's resources. Developers are given access to develop system operations to improve system functions; however, developers do not use PII during maintenance activities.

Contractors:

Direct AHRQ contractors perform research on the information contained within the system.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

System user access to the data is permitted only through authorization by the AHRQ Project Director after completion of the required data use agreements, security and privacy awareness training, background check, and database-specific security training.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Least privilege concepts are applied to the environment to help ensure that users only have the minimum required access needed to properly perform their job functions. Developer staff have the least privileged account necessary to process data while limiting them in performing other unnecessary tasks such as installing software or modifying system configurations. These concepts follow the tenets outlined by applicable system security plan(s).

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

All employees and contractors must complete the AHRQ Information Security and Privacy Awareness training and acknowledge the AHRQ Rules of Behavior prior to being granted access to the system.

Describe training system users receive (above and beyond general security and privacy awareness training).

SSS's training requirements are documented in standard operating procedure PSOP-AHRQ01-0102.01 Security and Privacy Awareness Training. This training includes basic information assurance and information security topics that supplement AHRQ Information Security and Privacy Awareness training.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

All information stored and processed within the system originates from AHRQ or through AHRQ contractors. Retention and/or destruction of data (including PII) is driven by AHRQ requirements and AHRQ's various data use agreements.

SSS policy in meeting these requirements designates specific project staff with direct responsibility for maintaining, accessing, and securing the data sets, and with adhering to AHRQ retention and destruction schedules. Currently, AHRQ is determining the appropriate records retention schedule for records within this system, and until a schedule is applied, records will be maintained indefinitely.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Administrative: Access to PII is permitted only through authorization by the Project Director, after all required DUAs are signed and confidentiality training performed. SSS manages access to workstations through Microsoft Active Directory (AD) utilizing the “least privilege” concept.

Technical: The data sets are sent to SSS through an encrypted FIPS 140-2 compliant Secure FTP server. Access to the SAS workstations is managed through AD. All employees and contractors must have valid credentials with specific access granted to the SAS workstation. SSS passwords must meet the SSS Password policy and are only valid for three (3) months.

Physical: All PII is securely stored in SSS’s SDC. The facility maintains physical access controls at all entry/exit points equipped with a biometric hand scanner / personalized pin code). In the event the individual is not a current authorized user, a security guard may grant access to the facility where there is a holding room for proper identification and authorization.