US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/23/2017

OPDIV:

AHRQ

Name:

Medical Expenditure Panel Survey Enclave

PIA Unique Identifier:

P-9514857-091972

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 purpose of Medical Expenditures Panel Survey Enclave (MEPS-ENCL) information system, along with the Medical Expenditure Panel Survey Secure LAN (MEPS) Information System and the Medical Expenditures Panel Survey Medical Provider Component (MEPS-MPC) is to support the Medical Expenditures Panel Survey program as a whole. Specifically the MEPS Enclave Information System supports the Household Component of the survey which is further described below.

Each separate information system plays a vital role to the purpose of the MEPS program to continually provide researchers, policymakers, health care administrators, businesses, and others with timely, comprehensive information about health care use and costs in the United States.

In particular, MEPS data helps individuals understand how the dramatic growth of managed care, changes in private health insurance, and other dynamics of today's market-driven health care delivery system have affected, and are likely to affect, the kinds, amounts, and costs of health care that Americans use. MEPS data is also used in policy-related and behavioral research, predominantly on the determinants of health care use, spending, and insurance coverage in order to project who benefits from, and who bears the cost of, changes to existing health policy and the creation of new policies.

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

The MEPS program is used to provide national data on health care expenses of the civilian population living in the United States. Specifically, MEPS captures detailed statistics on the type of medical services used, how frequently they are used, the cost of those services, and how they are paid for, as well as health conditions and health insurance availability and coverage. Moreover, MEPS is the only national survey that links data on health services spending and health insurance to demographic, employment, economic, health status, and other characteristics of survey respondents. Medical Provider Data is also gathered, and Interviewer Data is provided with each survey as well. This data is collected under the "Household Component" of the survey and participation is completely voluntary.

The MEPS Enclave Information System supports the Household Component of the survey only.

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

The MEPS Enclave Information System which is operated by a third party contractor on behalf of AHRQ, is used to support the collection of data in the Household Component of the Survey. The MEPS Secure LAN (MEPS) information system and the MEPS Medical Provider Component (MEPS-MPC) information system both have their own separate PIA.

The information collected in the Household Component is: the age, race, and sex of each family member; Health conditions; Current Health Status; Visits to health care providers (doctors, dentists, hospitals, etc.); Charges and Payments for Health Care; Medications; Employment; Health Insurance. The information is used to generate statistical data that is used to spot trends in health care spending.

The HC survey questions specifically request information on medical care providers, including: provider name, provider address, provider phone number and one or more contact names and phone numbers.

Information about the individual conducting the interview for each survey in the Household Component is also collected (questions request PII pertaining to Navigators/interviewers such as name and contact information).

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

E-Mail Address

Mailing Address

Phone Numbers

Medical Records Number

Medical Notes

Employment Status

Age, Race, Gender

Charges/Payments for Health Care

Usernames for System Access

Medical Information including: Specific Health Conditions, Current Health Status, Visits to health care providers, medications, employment, and health insurance.
Usernames for System Access

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

Employees

Public Citizens

Patients

System Users

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

See the answers to Q11-13 for PII usage information. The agency does not share the PII. Only non-PII information is shared. The PII of survey respondents is used to correlate and combine data received from the Household Component and the Medical Provider Component to generate statistical data that is used to spot trends in health care spending. The PII of Medical Care Providers is used to contact them to request supplemental data to that received in the survey for the Household Component. Interviewer PII is only used to initially track submission of Household Component surveys.

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

n/a

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?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or identify if a SORN is being developed.

09–35–0002 MEPS & Nat'l Med Expend. Surv. 2

09-35-0002 MEPS & NMES 2

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Non-Governmental Sources

Public

Private Sector

Other

Identify the OMB information collection approval number and expiration date

OMB 0935-0118, Exp. 12/31/18; OMB 0935-0110, Exp. 11/30/2018.

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Within HHS

Agency for Healthcare Research and Quality - Designated Agents for the purpose of sampling, event matching and data quality monitoring.

Private Sector

A 3rd party contractor to AHRQ initially collects PII as it conducts the survey for the Household Component. Limited data is then transmitted to another contractor which performs the data collection under the Medical Provider Component (MPC).

Describe any agreements in place that authorizes the information sharing or disclosure.

N/A

Describe the procedures for accounting for disclosures.

The information systems supporting MEPS all have strong Incident Response procedures consistent with Federal Law under the Federal Information Security Management Act (FISMA) as required under NIST SP800-53 Rev 4. Disclosure of PII follows HHS and AHRQ Incident Response Plans, and is tracked and coordinated with HHS Computer Security Incident Response Center (CSIRC). Specific procedures include notification to individuals whose PII has been compromised and access to credit monitoring where appropriate.

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

Prior to the interview process, the interviewees are given an option to decline participation. Participation is voluntary, and participants are informed that their PII is collected by the interviewer, and by their own review of the interview questions. Also see response to Q27.

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.

The information is gathered through an interview process with the selected participants and is provided on an voluntary basis. Prior to the interview process, it is explained to the participants what data is being collected, why, and how the data is shared and protected. Interviewees are given the option to decline answering questions. No data containing PII is shared.

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

The AHRQ Incident Response plan includes the specific process followed to notify individuals whose PII is in the system in the event of a disclosure. There is no process to obtain consent for major changes to the system such as data use, as no major changes are anticipated after initial consent is provided.

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.

The individuals are advised to and have the ability to contact AHRQ and the Center for Financing, Access and Cost Trends (CFACT) Project Director via mail, email, or telephone with the POC listed here in field 6 and that individual's direct contact info.

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

At every stage of the project, the MEPS management team provides guidelines and required field procedures for preventing exposure of confidential information and for the reporting of lost or stolen project items that contain respondent information. Each year, all field staff are required to read and sign the AHRQ Affidavit for Contractors. Field staff are required to adhere to confidentiality procedures and are also required each year to review the procedures related to protecting PII that appears on all hard-copy case materials as well as in the laptop computer used for conducting interviews. The document they sign defines PII, lists hard-copy project materials that include PII, and explains the protocol for reporting loss or theft.

On the project, we attempt to minimize the number of documents on which PII appears, but some documents with identifying information are essential to the operation of the study. Because these materials contain PII, they must be protected from disclosure to anyone who is not part of the project team. Laptops used by interviewers to complete MEPS interviews with household members represent another potential source of PII, although all MEPS laptops have full-disk encryption using software that is FIPS 140-2 compliant. This encryption software protects the laptop and stored data from access by unauthorized users.

AHRQ strictly adheres to the standards set forth by the Federal Information Security Management Act (FISMA) and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" and the controls required by NIST SP 800-53 Rev 4, "Security and Privacy Controls for Federal Information Systems and Organizations" to protect the Confidentiality, Integrity and Availability of the information system and all the data (including PII) that it contains.

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

Users:

Statistical Analysis

Administrators:

Statistical Analysis

Developers:

Developers of the MEPS instrument and data delivery software

Contractors:

Statistical Analysis

Others:

Statistical Analysis

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

Business and functional requirements dictate who may access PII, and access is provided on a "least privilege" basis such that only AHRQ employees and contractors that need access to PII receive it.

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.

Permissions are limited through the use of system roles that were identified during the requirements gathering phase of the project. The system roles only allow access to a minimum amount of information necessary for system administrators to adequately perform their job.

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.

HHS Annual Information Systems Security Awareness Training and Privacy Awareness Training training is used.

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

Individuals with significant security responsibilities such as Information System Owners, Information Security and Privacy Staff, System Administrators, and Executives take Role Based Training from HHS.

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.

The National Archives and Records Administration (NARA) Retention Schedules for MEPS Enclave data are being determined. PII will be protected by AHRQ and its contractors based on the security control requirements listed in NIST SP800-53 Rev 4.

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

The PII is secured on a protected network that only accessible from specific terminals. This network has no access to the Internet or any other network. For Continuity of Operations Plan (COOP) purposes the data is mirrored to an off-site host and is only accessible via VPN or at recovery facility. Administrative, technical, and physical security controls required for the system are defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 4, "Security and Privacy Controls for Federal Information Systems and Organizations." These controls strengthen the information systems and the environment in which it operates, and are reviewed on an annual basis. For physical security, server hardware is locked in cabinets, in a locked data center with FIPS 140-2 compliant encryption protecting the PII data.