US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/11/2022

OPDIV:

AHRQ

Name:

Medical Expenditure Panel Survey - Medical Provider Component

PIA Unique Identifier:

P-1316957-706022

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

Indicate the following reason(s) for updating this PIA.

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

none

Describe the purpose of the system.

The Medical Expenditure Panel Survey Medical Provider Component (MEPS-MPC) is a major application that collects data about medical costs from medical providers. Data collected in the MEPS-MPC are used to impute estimates of medical expenditures not captured in the MEPS-HC (Medical Expenditure Panel Survey-Household Component). Data from the MPC are used in tandem with data from the HC and are critical to developing expenditure estimates that can withstand intense public scrutiny. The MPC also provides information about physician charges associated with hospital care but not billed by hospitals, and is a primary source of expenditure information for Medicaid recipients.

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

The MEPS MPC collects data from all hospitals, emergency rooms, home health care agencies, outpatient departments, long term health care facilities and pharmacies reported by MEPS HC respondents as well as all physicians who provide services for patients in hospitals but bill separately from the hospital. The MPC collects data on dates of visits/services, use of medical care services, charges and sources of payments and amounts, and diagnoses and procedure codes for medical visits/encounters. Data requested in the MPC includes several record systems (medical records, billing, laboratory, etc.). The objective of the MPC is to compare provider data with household data collected in the HC and then AHRQ employees and direct contractors compare and normalize the data for reporting. Data may be collected via telephone, web, or hardcopy form.

Concerning the data elements: date of birth, name, email address, mailing address, phone numbers, medical records number, medical notes and employment status, only employment status is released to the public (once all identifiers have been removed), direct contractor usernames and passwords for system access. The remaining data items are used for data collection and processing purposes only and are not released to the public.

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

The MEPS Medical Provider Component (MPC) collects data from a sample of providers (physicians, hospitals, home health agencies, and pharmacies) who provided medical care to MEPS Household Component respondents. The MPC collects data on dates of visits/services, use of medical care services, charges and sources of payments and amounts, and diagnoses and procedure codes for medical visits/encounters. The MPC survey requests medical treatment information from medical care providers medical records, billing records, laboratory records, and information about physician charges associated with hospital care but not billed by hospitals. The information is compared and used to generate statistical data that is used to spot trends in health care spending.

Concerning the data elements: date of birth, name, email address, mailing address, phone numbers, medical records number, medical notes and employment status, only employment status is released to the public (once all identifiers have been removed), direct contractor usernames and passwords for system access. The remaining data items are used for data collection and processing purposes only and are not released to the public.

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

Yes

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

laboratory records

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

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

System users

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The PII of survey respondents is used to correlate and combine data received from the Household Component (HC) and the Medical Provider Component (MPC) to generate statistical data that is used to spot trends in health care spending. The PII of MPC 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 HC 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 use 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.

Identify the OMB information collection approval number and expiration date

OMB 0935-0118, Exp. 11/30/21

Is the PII shared with other organizations?

Yes

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

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

MEPS-MPC has an interconnection agreement with Social and Scientific Systems (SSS) to allow access to the MEPS-MPC data.

Describe the procedures for accounting for disclosures.

Data that includes PII is collected and maintained by AHRQ employees and direct contractors who administer the MPC and HC surveys and compare the data to provide the analysis. These processes are documented within the MEPS-MPC System Security Plan (SSP).

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, MPC and HC interviewees who are survey participants 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.

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 the survey 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.

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

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. A major change to the system will change the MEPS processes and would require a new type of collection, of which participants would be notified prior to new process for collection.

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.

All survey participants 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 noted in this PIA to resolve a concern with the submission of PII.

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, "Risk Management Framework for Information Systems and Organization: A System Life Cycle Approach for Security and Privacy" and the controls required by NIST SP 800-53 Rev 5, "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.

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-MPC 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, and will be kept indefinitely until a records retention schedule is established for the data within the system.

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.

Note: web address is a hyperlink.