US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/17/2022

OPDIV:

AHRQ

Name:

AHRQ Management Cloud

PIA Unique Identifier:

P-8268693-209551

The subject of this PIA is which of the following?

General Support System (GSS)

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.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

No

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

PIA Validation

Describe the purpose of the system.

The AHRQ Management Cloud was developed to host multiple systems management tools providing authentication back end, anti-virus applications, and vulnerability/compliance scanning tools into one infrastructure. AHRQ Management Cloud is established as a General Shared Service (GSS) to provide shared resources to the projects that reside within the environment, as well as provide those resources to external, cloud-based business partners.

Additionally, the AHRQ Management Cloud will host data provided through the Medical Expenditure Panel Survey (MEPS) SecureLAN transfer. Each individual MEPS component involved in the SecureLAN transfer (both the Medical Provider Component and the Household Component) have their own approved PIAs that specifically address the risks and mitigation practices involved in the collection, use, and dissemination of the MEPS data sets.

MEPS SecureLAN - The purpose of Medical Expenditure Panel Survey Secure LAN (MEPS) information system, along with the Medical Expenditures Panel Survey Enclave (MEPS-ENCL) 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 Secure LAN Information System supports research into the data collected in the Household Component and the Medical Provider Component as explained below, and provides workstations for de-identified data set generation, viewing and manipulation.

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 AHRQ Cloud Management system serves to collect for analysis data on the applications, tools, and systems it hosts to monitor compliance, vulnerabilities, patch data, and functionality.

User level data (and potential PII) associated with the system would be the username and password required by AHRQ employees and contractors to obtain a user account on the AHRQ management cloud.

MEPS SecureLAN - 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. MEPS collects PII that includes first and last name, email address, medical notes and medical record provider, mailing address, employment status, date of birth, username and password for system access, and medical information including specific health conditions, current health status, visits to health care providers, medications, employment, and health insurance. This data is collected under the "Household Component" of the survey and participation is completely voluntary.

The MEPS Medical Provider Component (MPC) collects data from all hospitals, emergency rooms, home health care agencies, outpatient departments, long term health care facilities and pharmacies reported by MEPS Household Component (HC) respondents as well as all physicians who provide services for patients in hospitals but bill separately from the hospital. We collect and store provider name, provider address, provider phone number and one or more contact names and phone numbers.

Data provided by MEPS establishes a foundation for estimating the impact of changes in sources of payment and insurance coverage on different economic groups or special populations of interest, such as poor, elderly, uninsured, or racial minorities. MEPS is co-sponsored by the AHRQ and the National Center for Health Statistics (NCHS), but NCHS does not provide any PII to AHRQ.

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

Usernames of application level users (AHRQ employees and contractors) will be collected and maintained by the system. System administrators will have access to the list of system users in order to manage the system and the accounts on it. However, usernames of system users are not system specific, they are simply the username associated with an individual's employee/contractor Personal Identity Verification (PIV) account within the Health and Human Services (HHS) environment.

Account usernames and passwords are stored in the system.

MEPS SecureLAN - The MEPS Secure LAN Information System which is owned and operated directly by AHRQ, aggregates data received from both the MEPS Household Component (in the MEPS Enclave Information System operated by a 3rd party contractor which has its own PIA), and the MEPS Medical Provider Component or MPC (in the MEPS MPC Information System which is also operated by a 3rd party contractor, and also has its own PIA). MEPS collects PII that includes first and last name, email address, medical notes and medical record provider, mailing address, employment status, username and password for system access, and medical information including specific health conditions, current health status, visits to health care providers, medications, employment, and health insurance. This data is collected to provide research statistics for each of the households, families, and person-level files, providing specific health services data that Americans use, how frequently they use them, the cost of these services, and how services are paid for, as well as data on the cost, scope, and breadth of health insurance held by the households, families.

The information collected in the Household Component (HC) 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.

The MPC survey requests medical treatment information from medical care providers.

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.

Health insurance

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

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

Usernames and Passwords are used by system users to create and maintain an account on the AHRQ Management Cloud for access to the tools and applications therein. Administrators have access to usernames in order to manage accounts on the system.

MEPS SecureLAN - 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. Privacy Act of 1974; E-Government Act of 2002; OMB M-03-22, OMB 07-16, OMB M-10-23.

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 & NMES 2

Identify the sources of PII in the system.

Identify the OMB information collection approval number and expiration date

N/A

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.

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.

Creation of an account (and accompanying username and password) is entirely voluntary and users may choose not to create an account or to delete their account at any time.

MEPS SecureLAN - The information is gathered through an interview process with the selected participants and is provided on a 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.

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.

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.

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

There are no anticipated major changes for the use of username and password data in the information system, so there is no process to obtain consent for this. However, if the system develops additional capabilities that involves PII for additional navigation of the system, or additional features that require user accounts to be upgraded, system administrators will notify users of the change to the way PII will be used, and during notification users will be able to delete their accounts or access the changes to the use of PII within the system.

MEPS SecureLAN - 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.

Users (AHRQ employees and contractors) who have concerns that their information has been inappropriately used can contact the system administrators via phone or email to either disable/delete the user account, or work with administrators to change passwords.

MEPS SecureLAN - 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.

User information is not used for any other purpose, and there are no evaluations or determinations made about an individual based upon the PII. As a result, there is no periodic review of PII contained within the system. Should users need to change information about their account, users can contact the system administrators to request this change.

MEPS SecureLAN -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.

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

Only system administrators will have access to user account usernames in order to manage the

accounts within the system. The system owner is responsible for approving account creation requests and notifies system administrators to create accounts.

MEPS SecureLAN - 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.

The system owner limits all system administrator account creation and monitors the number of users who have access to the system, and to PII, at all times as part of the system owner role. The System Owner's approval for all new privileged account is based on the access needed for a user to perform his/her duties and is contingent upon that user's favorable adjudication of AHRQ security/background investigations.

MEPS SecureLAN - 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.

System personnel take the HHS security awareness training and Rules of Behavior training on an annual basis, in addition to role based security training provided by AHRQ.

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

MEPS SecureLAN - 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.

NARA General Records Schedule 3.2: Information Systems Security Records (DAA-GRS-2013-0006-0003)

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

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.

Administrative Controls include: procedural safeguards: Users must comply with terms of use on reinforce the confidentiality protection requirements, and the confidentiality policy is reviewed and signed on an annual basis, security training and ongoing awareness programs, such as posters and newsletters,

Access controls, including termination procedures to ensure only authorized personnel have access to facilities and systems, commensurate with their job duties, review of system activity logs to monitor for issues, Risk Management plans to include Risk assessments, Security Plans, Continuity of Operations/Disaster Recovery plans, background and reference checks are performed on all

IFMC personnel.

Technical controls: Access is role-based and includes controls for the flow and protection of information to limit access on a need-to-know basis. Only administrators that require access to user account information granted access. Additional controls include: Authorized users using user passwords and a hard token-One Time Password Device for access to the secured areas of the website, separation of duties, filters and parameters are set up in accordance with an approved configuration to enforce the security policy, data back up on a daily and weekly basis, with the weekly tapes going off-site for storage, destruction of electronic information, as appropriate, via sanitization of the systems holding the information, audit of events initiated by each individual user, i. e., entry of UserID and password, program initiation, file creation, file deletion, file open, file close, and other user related actions, audit trails identify the individual user initiating the event, date, and time the event occurred, success, or failure of each event, and location where the event was initiated.

Physical Controls: Physical controls include but are not limited to: building access cards and ID badges are required in the main facility and only authorized personnel have access to the locked data center where the hardware used to process this system data is located, security guards are present during working hours and off-hour visits are made by security personnel, CCTV is used for monitoring of the facility, back up media is stored offsite in a secure, climate controlled storage facility, visitor process includes signing in and out, visitor badges and escorting of all visitors, uninterruptible Power System (UPS) with a diesel generator back up to ensure ongoing system operation and an orderly shutdown when necessary, power to the data center is separated from the power to the rest of the facility and additional HVAC with humidity controls is in place, Locked shred bins are utilized for document and media destruction and certificates of destruction are received from the bonded destruction company upon completion.