# US Department of Health and Human Services

## Privacy Impact Assessment

### Date Signed:

11/05/2024

### 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)?**

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.**

When the AMC PIA was first created, the PIA was filled out with the intention that the system would not collect PII/PHI. However, upon further investigation, the system does store, manage, and processes PII/PHI. There was never any PII in the system that was being collected, processed, or managed, so therefore we wanted to update the PIA to reflect that the application does store PII/PHI.

**Describe the purpose of the system.**

The AHRQ Management Cloud (AMC) was developed to host multiple systems security management tools providing an authentication back end, centralized patch management, and vulnerability/compliance scanning tools into one infrastructure. The AHRQ Management Cloud (AMC) 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. The GSS provides a standard operating system configuration for AHRQ to utilize. There are two major variations that are provided; Microsoft Windows 2016 and CentOS Linux

7. All deployed Operating Systems (OS) are configured in accordance with the Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGS). Any deviations from the standard DISA STIG is documented with a justification. The GSS also provides a secure environment and Information Assurance (IA) tools.

The AMC is implemented using four accounts within Amazon Web Services (AWS). The primary management account hosts security management applications and an end-user computing environment supporting the Medical Expenditure Panel Survey in separate Virtual Private Clouds (VPCs). These VPCs are interconnected through another account, the Transit network, using a combination of AWS Transit Gateway (TGW) and a pair of fault-tolerant Palo Alto Firewalls. The Transit account also provides for simplified, yet secure, interconnections with external business partner environments as referenced in Section 11, System Interconnections. A third account acts as an offsite backup storage location. While the backups stored are for the AHRQ Business Operations and Program Support System (BOPSS) and Medical Expenditure Panel Survey (MEPS) systems, this environment is managed as part of the AMC, hence its inclusion in the system boundary. A fourth account, currently not utilized, is intended for use as a centralized logging destination for all AMC environments.

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

The AMC provides systems management and Continuous Diagnostics and Mitigation (CDM) capabilities to existing and future AHRQ information systems. Additionally, it provides network security services, including traffic inspection, routing, and secure private application access (VPN) to itself and external business partner environments.

The information security architecture of the AMC was conceived as a private enclave within the Cloud to provide security monitoring of external business partner systems as well as provide self-monitoring capabilities.

The AMC serves to collect for analysis data on the applications, tools, and systems it hosts to monitor compliance, vulnerabilities, patch data, and functionality.

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

The AMC serves to collect for analysis data on the applications, tools, and systems it hosts to monitor compliance, vulnerabilities, patch data, and functionality.

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

Yes

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

Medical Notes
Age range (5 year increments), Sex, Gender, Ethnicity, Race, Primary language, education level, residence zip code
Self-reported health status
Visits to Health Care Providers (doctors, other clinicians, clinics)
Health insurance type

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

Patients

**How many individuals' PII is in the system?**

50,000-99,999

**For what primary purpose is the PII used?**

The PII is part of data being collected to evaluate the AHRQ Long COVID Care Network's performance on reach, structure and process, and impact measures. All PII will be aggregated for analysis across 12 grantees and multiple clinics and will be used to conduct subgroup analyses (e. g., to examine initiative reach across age groups, race/ethnicity groups, education level, rural/urban residence, etc). The findings will be summarized in an evaluation report. Individual patient-, clinic-, or grantee-level data will not be reported publicly; they will only be examined for data quality checks. Only aggregate data across initiative grantees will be publicly reported.

**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?**

No

09-35-0002 MEPS & NMES 2

**Identify the sources of PII in the system.**

Non-Governmental Sources

Private Sector

**Identify the OMB information collection approval number and expiration date**

N/A

**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.**

N/A - we are not collecting personal information, we are receiving it.

**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.**

Grantee organizations submitting data have the option to opt-out and provide aggregate data at the clinic or grantee level.

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

N/A - we are not collecting personal information, we are receiving it.

**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.**

N/A - we are not collecting personal information, we are receiving it.

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

Upon receipt, the Contractor will review the data for quality control and resolve any inaccuracies, gaps, and discrepancies with grantees.

**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.**

Both administrators and contractor personnel who are system users will have access to PII.

**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.**

Only the minimum amount of PII necessary for the evaluation is being received and all PII are required to conduct the evaluation. System users will have access to all PII received.

**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 (https://securityawareness.usalearning.gov/piiv2/content/index.html), in addition to role based security training provided by AHRQ.

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

The contractor, 2M, conducts internal training throughout the year in settings like staff meetings that reinforce key messages from their employee handbook that employees attest to when they join 2M:

Employees agree to 2M’s security procedures, which include the following:
Never share confidential data, including personally identifiable information (PII), with another employee unless the employee has been authorized by the data custodian (typically the head of the department that collects and maintains the data).
Never store confidential data, including PII, on portable storage devices such as portable hard drives, USB flash drives, CDs, DVDs, mobile phones, and personal digital assistants.
Never store confidential data, including PII, on a laptop unless there is a legitimate business purpose and the data is encrypted on the laptop.
Avoid sending confidential data and never send PII in an email message. Password protect or encrypt email attachments that contain confidential or sensitive data.
Always adhere to 2M password protocols of the 2M networking environment to maintain a secure information technology environment.

Personnel who work in 2M's primary data collection/survey research center complete additional trainings related to HIPAA as well as data privacy/security on the Mineral platform. These topics include:
IT Security for End Users; IT Security Fundamentals
Cybersecurity – Browser Safety
Cybersecurity – Practical Steps to Avoid Risk
Cybersecurity Awareness for Employees: Security Awareness Essentials

**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.**

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.