

# US Department of Health and Human Services

## Privacy Impact Assessment

**Date Signed:**

01/31/2025

**OPDIV:**

CMS

**Name:**

Performance Metrics Database and Analytics

**PIA Unique Identifier:**

P-9586742-779169

**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.**

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.**

Aside from incremental software to Performance Metrics Database and Analytics (PMDA) and associated software, no changes to the system have been made since the last Privacy Impact Assessment (PIA). The PIA has been updated to only include only Personally Identifiable Information (PII) handled by PMDA as opposed to Identity Management (IDM).

**Describe the purpose of the system.**

The purpose of the Performance Metrics Database and Analytics (PMDA) is to improve states' and Center for Medicaid and Children's Health Insurance Program Services (CMCS) abilities to effectively collect and store performance data, programmatic quality, and other reported information for oversight, monitoring and evaluation of 1115 demonstrations.

The 1115 demonstrations exhibit and evaluates policy approaches such as expanding eligibility to individuals who are not otherwise Medicaid or Children's Health Insurance Program (CHIP) eligible,

providing services not typically covered by Medicaid, using innovative service delivery systems that improve care, increase efficiency, and reduce costs. States who want to request a program under this authority must submit a written application to Centers for Medicare and Medicaid Services (CMS) for approval that details the goals and operational aspects of the program, and those applications are subject to public review and comment.

Programmatic quality for all 1115 demonstrations is that all demonstrations must remain budget neutral and are monitored throughout the lifespan of the demonstration. As a result, the outcome of all demonstrations is categorized as performance data.

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

The system collects financial information regarding performance-based incentive programs from state representatives. The Content Management Application (CMA) within PMDA includes information to include name, email address, phone numbers and user credentials from state users, system administrators, and contractors for identification/authentication and communication purposes.

The types of financial information that are collected are publicly available financials associated with the cost of running a demonstration such as the cost associated with per member, per month.

PMDA user credentials are collected and maintained by the IDM system. IDM is external to PMDA and the PII within IDM is covered by a separate PIA. After initial log into the IDM system, a user inputs a user ID and password to gain access to PMDA. System administrators are granted access to PMDA upon approval of their Enterprise User Administration (EUA) which is a separate system which is covered by its own PIA) user Identification (ID). The EUA user ID is then used to create the CMS Enterprise Portal account to grant access to PMDA.

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

The PMDA system regularly uses PII to retrieve system records including using the email, name, phone number and user credentials to access the PMDA system.

The PMDA was built with the capacity to support the CMCS. The purpose of PMDA is to improve states and CMS' abilities to effectively collect and store performance data, programmatic quality, and other reported information. The system will also validate track performance-based incentives payments and have the capability to provide electronic reports that support CMCS oversight, monitoring, and evaluation of quality and performance metrics and other related incentive payments. PMDA also produces analytic files to support CHIP Services.

State users, which include employees and direct contractors working for the state government, will upload the demonstration documents (required from Section 1115 of the Social Security Act) to share with CMS administrative users to review. There is also a downloading capability that state users may utilize to edit and re-upload documents. These demonstration documents in the system will be maintained in the system permanently.

The CMA within PMDA will include information such as name, email address and phone numbers from state users, system administrators, and contractors for identification/authentication and communication purposes. It also collects financial information, such as publicly available financials associated with the cost of running a demonstration such as the cost associated with per member, per month as provided by state users in the demonstration files.

IDM is used to authenticate users - it collects, stores, and maintains user information such as name, email, phone number, and address.

PMDA user credentials are collected and maintained by the IDM system. IDM is external to PMDA

and the PII within IDM is covered by a separate PIA. After initial logging into the IDM system, a user inputs a user ID and password to gain access to PMDA. System administrators are granted access to PMDA upon approval of their EUA user ID. The EUA user ID is then used to create the IDM Portal account to grant access to PMDA.

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

Yes

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

Name

E-Mail Address

Mailing Address

Phone Numbers

Other: User Credentials

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

Employees

Business Partner/Contacts (Federal/state/local agencies)

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

100-499

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

The PII is used for identification/authentication and communication purposes.

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

Not Applicable.

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

United States Code (U.S.C.) § 7701(c)(1) - Appellate procedures, U.S.C. 552a(b)(1) - Records Maintained on Individuals; 5 U.S.C Section 301, Departmental Regulations

**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.**

09-70-0538, Individuals Authorized Access to CMS Computer Services (IACS)

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

Directly from an individual about whom the information pertains

Online

Government Sources

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

This system is exempt from an OMB information Collection Approval Number.

Non-Governmental Sources

Private Sector

**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.**

Identity Management (IDM), a separate CMS shared system, is used to authenticate PMDA users. IDM independently authenticates users outside of the PMDA application. As part of this IDM authentication, PMDA users access the CMS Enterprise Portal where there is a Privacy Act Statement that users must accept during initial registration and again on a yearly basis. The Privacy Act Statement is included in the Terms and Conditions that the user accepts. Administrator and direct contractor user credentials also utilizes CMS Enterprise Portal. When users request access to PMDA, IDM presents them an acknowledgement screen of the PII maintained in PMDA and the uses of data. Users must consent to receive access.

**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.**

There is no method for users to opt out. The only PII in the system is contact information for system users and State Medicaid Directors (which is also public information). This contact information is needed to contact users about their applications. Users enter this information into the system for this use. Users are state and Federal employees or their representatives and thus have publicly available contact information.

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

IDM collects, stores, and maintain users PII. When users request access to PMDA, IDM presents them an acknowledgement screen of the PII maintained in PMDA and the uses of data. Users must consent to receive access. When there is a major change that occurs to the system, the acknowledgement screen would be updated, and users would then need to accept the terms and conditions before proceeding.

**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.**

IDM collects, stores, and maintains user information such as name, email, phone number, and address. Any concerns of inappropriate gathering or use of an individual's PII should be directed to the IDM Help Desk at 1-855-267-1515 or sent in writing to Medicare following the complaint process outlined in Medicare's Notice of Privacy Practices. A Remedy ticket will be created to record the incident and all relevant information to the incident (i.e., What was disclosed, when, how, by whom). An incident investigation will be initiated, and the results documented in the Remedy ticket and a report provided to the data owner for all involved systems. Appropriate remediation actions will be taken based on the nature of the incident. IDM Help Desk is the primary incident responder since IDM contains the PII source. However, users can contact the PMDA Help Desk at (443) 775-3226 concerning incidents as well. If necessary, the PMDA Help Desk will raise the incident with the IDM Help Desk.

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

PMDA is supported by IDM. IDM is responsible for verifying the accuracy of PII collected on the user's behalf and is subject to and adheres to the security assessment and authorization requirements as outlined in the Risk Management Framework (RMF). The Privacy Impact Analysis document and the System Security Plan are reviewed annually. The annual Risk Assessment is conducted to ensure continued compliance with the CMS Acceptable Risk Standards (ARS).

**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.**

IDM is where the user credentials are processed. IDM roles are defined that govern the access to PII. When users request access to PMDA, they select one of the IDM roles. An administrator approves the user's request.

The IDM roles include, state user, CMS project officer, third party evaluation analyst and Administrator.

**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.**

System administrators are granted access to PII based on the best practice of least privilege in which the appropriate staff is given the lowest level of user rights that they can have and still do their jobs at their highest capacity. As a result, users are granted limited access to PII viewing according to their role assignment through the IDM registration and approval process.

**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 CMS employees and direct contractors are required to take the mandatory annual CMS privacy and security awareness training. An operation manual for PMDA developed by the application administrators is also available. It is accessible to the system owner, managers, operators, and direct contractors.

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

Not Applicable.

**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.**

General Records Schedule (GRS), Records Schedule Items 2, Request for Records Disposition Authority: DAA-0440-2015-0009. Destroy 10 year(s) after cutoff or when no longer needed for agency business occurs, whichever is later.

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

All PII is stored on the encrypted drives. The databases are encrypted at rest and the data is accessed using Federal Information Processing Standards (FIPS) 140-2 requirements. The PII is housed in a cloud environment that is Federal Information Security Management Act (FISMA) compliant and Federal Risk and Authorization Management Program (FedRAMP) approved. The CMS Cloud is responsible for physical and administrative safeguards to include applicable access and audit-based controls.

