US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

07/23/2025

OPDIV:

CMS

Name:

Health Plan Management System

PIA Unique Identifier:

P-9317971-241429

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.

June 2023 - Drug Price Negotiation: HPMS collects the email address and name of participants submitting data for the voluntary Drug Price Negotiation survey. The email address is used to limit the number of survey submissions to one per email. It is not used in the data analysis.

December 2021: HPMS displays personally identifiable information for Medicare beneficiaries and providers in the FWA Reporting module. Specifically, HPMS collects the beneficiary's name, MBI, phone number, address, and email address as well as the provider's NPI, tax ID, and medical license number. Centers for Medicare & Medicaid Services (CMS) uses this data to investigate suspected FWA activity in the Medicare Advantage (MA) and Prescription Drug programs.

Describe the purpose of the system.

The Health Plan Management System (HPMS) is an internet accessible web application that serves as the primary plan-based information system supporting the Medicare Advantage (MA) and

Prescription Drug Plan (PDP) programs. HPMS is defined as a major application and is maintained for Centers for Medicare & Medicaid Services (CMS) by three contractor groups: Softrams, CGI Federal, and the Office of Information Technology (OIT) Cloud Navigator. HPMS is comprised of two web sites; the primary HPMS data collection/display site and a dashboard site that provides management level summation of the data contained with HPMS.

HPMS is a day-to-day operational system that addresses the input, data processing, and output needs of CMS users and external user communities. HPMS provides CMS with the means to collect, manage, and disseminate critical MA and PDP data. The primary data sources for benefits, co-payment, and beneficiary education information are the:

Plan Benefit Package (PBP);
Summary of Benefits (SB) sentences;
Bid Pricing Tool (BPT).

Other key data sources include:

Contract and service area data;
Formulary Data;
Marketing Data;
MA and PDP complaint data;
MA county demographics data; and
Financial Data.

These source data provide the basic information upon which most of the HPMS modules act and operate. HPMS also provides data extracts for a variety of CMS and other Federal government systems.

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

HPMS is a day-to-day operational system that addresses the input, data processing, and output needs of the CMS and external user communities. HPMS provides CMS with the means to collect, manage, and disseminate critical MA and PDP data. The primary data sources for benefits, co-payment, and beneficiary education information are the: Plan Benefit Package (PBP); Summary of Benefits (SB) sentences; and, Bid Pricing Tool (BPT).

Other key data sources include: Contract and service area data; Formulary Data; Marketing Data; MA and PDP complaint data; MA county demographics data; and, Financial Data.

Additionally, HPMS collects data that may contain Personal Identifiable Information (PII) and/or Protected health information (PHI) for:

User Account Maintenance - for system operations
Part C Improper Payment Measure - for audit activities
Part D Improper Payment Measure - for audit activities
Medication Therapy Management Program (MTMP) - evaluate MTMP activities
Performance Metrics Module - MTMP data
Audit Module - for audit activities
Fraud, Waste and Abuse Tracking Module - investigate Medicare Advantage (MA) and Prescription Drug (PD) Plan activities
Compliance Activity Module - plan oversight activities
Online Enrollment Center - support beneficiary plan enrollment
Fraud, Waste, and Abuse Reporting module - report on MA/PD activities
Drug Price Negotiation

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

HPMS is a web-enabled information system that supports the ongoing business operations of the Medicare Advantage (MA) and Prescription Drug (Part D) programs. All the data collected in the HPMS application is used to manage the MA and Part D programs.

User Account Maintenance: HPMS collects the first name, middle initial (optional), last name, e-mail address, organization name, address, city, state, zip code, phone number, and fax number (optional) from each registered user of the system. CMS uses this data to communicate with the users.

HPMS collects personally identifiable information on Medicare beneficiaries in the:

Part C Improper Payment Measure module: HPMS collects the beneficiary's first name, last name, Medicare Beneficiary Identifier (MBI), date of birth, and medical record information. CMS uses this data to estimate the error rate for Part C payment.

Medication Therapy Management Program (MTMP): HPMS collects the beneficiary's first name, last name, MBI, and date of birth. CMS uses this data to evaluate and monitor MTMPs administered by Part D organizations.

Performance Metrics Module: HPMS displays the beneficiary-level MTMP data submitted by Part D plans via CMS EFT, as described above, in the MTMP Gentran Submissions section of the Performance Metrics module.

Audit Module: HPMS collects universe files in the Audit module, which may contain beneficiary-level data. These data are used by CMS to administer program audits.

Part D Improper Payment Measure Module: HPMS collects the beneficiary's first name, last name, MBI, and prescription drug information. CMS uses this data to estimate the error rate for Part D payment.

Fraud, Waste and Abuse Tracking Module (FWA): HPMS displays the provider's National Provider Identifier (NPI) number, first name, last name, practice address, city, state, zip code, tax ID, and medical license number. CMS uses this data to investigate suspected FWA activity in the Medicare Advantage (MA) and Prescription Drug programs.

Compliance Activity Module (CAM): HPMS collects information from plans in response to CMS inquiries related to compliance review activities. These submissions may contain beneficiary-level data. CMS uses this data to perform oversight activities.

Online Enrollment Center (OEC): HPMS allows designated plan users to download OEC enrollment requests, including, but not limited to, the beneficiary's first and last name, birth date, address, phone number, email address, MBI, Medicare Part A and B statuses, and primary care physician. MA and Part D organizations use these data to process beneficiary requests to enroll in the selected plan.

Drug Price Negotiation - HPMS collects email address, name and organization from voluntary survey participants. The survey is used to collect information from the public about the drugs selected for the new Part D drug price negotiation program. We collect email to limit the number of survey submissions to one per email.

Fraud, Waste, and Abuse Reporting - HPMS collects the beneficiary's name, MBI, phone number, address, email address and medical record information as well as the provider's NPI, tax ID, and medical license number. CMS uses this data to investigate suspected FWA activity in the Medicare Advantage (MA) and Prescription Drug programs.

HPMS also contains the Health Insurance Claim Number (HICN) in legacy data in these modules: complaint tracking module (CTM), Part C IPM, Part D IPM, MTMP and OEC.

The MBI may be used to access records - via a search capability - in the CTM module.

HPMS data is stored permanently or for a minimum of ten years as required by the HPMS SORN.

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 Notes
Beneficiary identifier HICN/MBI), plan member ID, User ID, organization name, sex, taxpayer ID, provider NPI, fax number, medical record, and medical license.

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

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

Most Personal Identifiable Information (PII) collected in HPMS is used to support Medicare Advantage (MA) and Part D complaints and perform casework activities.

HPMS collects personally identifiable information on Medicare beneficiaries enrolled in Medication Therapy Management Programs (MTMP) offered by Part D plans. This data is submitted to HPMS via CMS' Electronic File Transfer (EFT) system, and the resulting data is shared with Part D plans and other approved users via the MTMP Gentran Submissions Module in HPMS. These data are collected under the Part D Reporting Requirements Paperwork Reduction Act (PRA) for program evaluation.

HPMS collects personally identifiable information on Medicare beneficiaries in our Audit module. This data is included in sample records provided by the MA or Part D organization undergoing the routine audit. CMS uses this data to run analyses to determine whether the organization is meeting program requirements.

HPMS collects personally identifiable information on Medicare beneficiaries in our Risk Adjustment

Validation module including beneficiary name, beneficiary Date of Birth (DOB), beneficiary identifier and beneficiary medical records. The data is used to calculate the national payment error rate.

HPMS collects personally identifiable information on Medicare beneficiaries in our Prescription Drug Event Validation module including beneficiary name, beneficiary identifier and prescription drug records. The data is used to calculate the part D payment error rate.

HPMS displays personally identifiable information for Medicare providers in the FWA Tracking module. Specifically, HPMS displays the provider's NPI number, first name, last name, practice address, city, state, and zip code, tax ID, and medical license number. CMS uses this data to investigate suspected FWA activity in the Medicare Advantage (MA) and Prescription Drug programs.

HPMS collects the email address and name of participants submitting data for the voluntary Drug Price Negotiation survey. The email address is used to limit the number of survey submissions to one per email. It is not used in the data analysis.

HPMS displays personally identifiable information for Medicare beneficiaries and providers in the FWA Reporting module. Specifically, HPMS collects the beneficiary's name, MBI, phone number, address, and email address as well as the provider's NPI, tax ID, and medical license number. CMS uses this data to investigate suspected FWA activity in the Medicare Advantage (MA) and Prescription Drug programs.

HPMS maintains information on all HPMS users, both internal and external, to provide the appropriate access for every user within the application. The password is NOT stored in the HPMS application. The CMS Enterprise User Administration (EUA) application is the system of record for issuing, maintaining and authenticating the user credentials. (EUA is covered under a separate PIA for CMS)

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

This data is also shared with other federal agencies (e.g., Office of the Inspector General (OIG) for research purposes).

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

Authority for maintenance of the system is given under section 1875 of the Social Security Act (the Act) (42 U.S.C. 1395ll), entitled Studies and Recommendations; section 1121 of the Act (42 U.S.C. 1121), entitled Uniform Reporting System for Health Services Facilities and Organizations; and § 1876 of the Act (42 U.S.C. 1395mm), entitled Payments to Health Maintenance Organizations and Competitive Medical Plans. Authority for maintenance and dissemination of Health Plan information is also given under the Balanced Budget Act of 1997 (Pub. L. 105–33).

42 CFR 422.503

42 CFR 422.504

42 CFR 423.504

42 CFR 423.505

42 CFR 423.153

42 CFR 425.118

42 CFR 425.204

The Improper Payments Elimination and Recovery Act of 2012; Public Law 112-248 and 42 CFR § 422.310

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.

09-70-0500 - Health Plan Management System

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Email

Online

Government Sources

Within OpDiv

State/Local/Tribal

Other Federal Entities

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

0938-0763 (PBP/Formulary/MTMP) – 3/31/2026

0938-0944 (BPT) – 7/31/2024

0938-0469 (Initial Soundness) - 8/31/2025

0938-0935 (MA Application) - 1/31/2024

0938-0936 (Part D application) - 7/31/2024

0938-0992 (Part D reporting requirements) - 1/31/2025

0938-1054 (Part C reporting requirements) - 10/31/2024

0938-1000 (Audit) - 5/31/2024

0938-1327 (PACE Audit) - 11/30/2025

OMB 0938-1449 (Drug Price Negotiation) - 8/31/2024

OMB 0938-1262 (Fraud, Waste, and Abuse Reporting)

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.

The Complaint Tracking Module business owner has a Memorandums of Understanding (MOU) in place with States (SHIPs) to support information sharing on complaint data.

HPMS has a Data Use Agreements (DUA) agreement for each HPMS Development Contractor.

Describe the procedures for accounting for disclosures.

HPMS is a web-based application and all access to HPMS data is obtained via the user interface. HPMS does not mail/distribute information outside of CMS by any other means. All HPMS users must request access to the system using the standard CMS user identification

(ID) request form. Moreover, due to the sensitive nature of the complaint, audit, performance metrics, and beneficiary-level MTMP data, each user must separately request access to those functions in the system. End user utilization is tracked in the system and samples are reviewed quarterly.

Additionally, there are Data Use Agreements in place with our development contractors which track what data is being disclosed, with whom, when and for what purpose.

HPMS contains PII policy information in the Website Policy section of the application - accessible to all users.

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

HPMS provides its users with a privacy policy page that explains how we will use their account information.

Regarding the MTMP, CTM, National RADV, Prescription Drug Event Validation, CAM, OEC, Performance Metrics and Audit modules these are records obtained through routine program administration activities in support of the Medicare Parts C and D and Medicare Shared Savings programs. Beneficiaries are asked to provide their PII information as part of the complaint submission process controlled by 1-800-Medicare.

EUA is the system of record for issuing the CMS User ID. HPMS is a consumer of that information.

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 formal 'opt out' policy. Submission of a complaint is a voluntary action on the part of an individual as is requesting access to HPMS.

The user's credentials are issued via the EUA system and not under the purview of HPMS.

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

All major system changes concerning PII are published for comment in the Federal Register as part of a modification of the HPMS System of Record (SOR).

The user's credentials are issued via the EUA system and not under the purview of HPMS.

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.

Medicare beneficiaries would need to report these concerns to 1-800-Medicare.

HPMS users would report any PII concerns to the HPMS Help Desk. The individual should be able to identify the information/record in question and identify the desired remediation action.

The user's credentials are issued via the EUA system and not under the purview of HPMS.

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

HPMS maintains data integrity by designing the application per Federal security standards and by ensuring adherence to those standards via an annual independent security audit. All PII is encrypted at rest in the database or on the file servers, e.g. pdf uploads. Application data is backed up per approved agency schedules to guarantee recoverability in the event of a data loss/corruption. Application availability is maintained via a combination of built in redundancies, for example, server

clustering and disaster recovery site, and relies on approved agency web hosting contractor sites/staff. PII data is reviewed for accuracy via a variety of module specific activities including Complaint records are reviewed and analyzed individually by trained caseworkers as part of the complaint casework and resolution process. MTMP records are audited by trained plan data validation review consultants as part of the plan reporting business process. Audit submissions are reviewed by designated audit staff as part of the routine audit business process. HPMS users can access and update their account information at any time. HPMS collects only relevant PII necessary to implement application functionality.

The job codes assigned via EUA to the user's credentials are periodically reviewed to ensure the user has the HPMS-Production job code. Users are required to accept the HPMS Rules of Behavior annually to maintain their access and must recertify their user credentials per EUA controls.

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.

Access for the modules that contain PHI/PII are classified using sensitive access types in HPMS. Designated CMS user access administrators only grant access to those developers and contractors whose work requires such data. System and database administrators are restricted to the encrypted data only. Uploaded files that contain PHI/PII are encrypted at rest and can only be viewed via the website.

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.

Access for the modules that contain PHI/PII are classified using sensitive access types in HPMS. Additionally, restrictions are in place so that a given user, e.g. a plan, can only see records/data applicable to their beneficiaries in the CTM module.

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.

We have defined security roles as well as a security awareness training plan, as mandated by Federal Information Security Management Act (FISMA). Additionally, all HPMS users are required to recertify their access annually and take a computer-based security course. Users annually review and accept the HPMS rules of behavior, which outline a user's responsibilities for accessing PII including adherence to the Privacy Act of 1974.

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

End users working with HPMS complaint data must attend routine caseworker trainings and meetings as well as abide by standard operating procedures. Plan data validation reviewers must also take required training prior to accessing HPMS and the related plan reporting data. Audit reviewers are provided training and must adhere to standard operating procedures.

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.

CMS will retain HPMS data for a minimum of 10 years.

The following disposition schedules apply:

Medicare Advantage Data: Disposition Authority - N1-440-09-4, Item1a (Medicare Advantage – Temporary. Cutoff annually. Delete/destroy 10 years after cutoff)

Part D/Formulary Data: Disposition Authority - N1-440-09-4, Item 1b (Prescription Drug Records – Temporary. Cutoff annually. Delete/destroy 10 years after cutoff.)

The destruction of PII will conduct in accordance with all CMS policies in place at the time of the data removal.

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

The system encrypts all PII/PHI at rest in the database or on the file server, e.g. PDF upload using Advanced Encryption Standard (AES) encryption (symmetric encryption - one single key for both encrypting/decrypting files on the server.)

Other methods for securing these data include, but are not limited to:

All traffic is encrypted using Transport Layer Security (TLS);

Users must obtain CMS user IDs and passwords and are granted access to only those HPMS modules and contract numbers required by their job functions;

Contractor staff undergo background investigations and security checks;

Contractor staff undergo security awareness training; and

Use of a multi-zone security architecture, operating system integrity and hardening, monitoring and maintenance of all hardware components, administration of firewalls, host and network-based intrusion detection services. Additionally, HPMS is hosted at a CMS approved data center that adheres to all CMS required physical security controls, using security guards and locked cages. The web hosting contractor is required to undergo an annual independent security audit to ensure adherence to those controls.