US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/22/2016

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.

HPMS began collecting personally identifiable information on Medicare providers that are participating in a Medicare Shared Savings Accountable Care Organization (ACO) as well as personally identifiable information on Medicare beneficiaries in our Audit module.

Describe the purpose of the system.

HPMS supports the plan enrollment and compliance business operations of the Medicare Advantage (MA) and Part D programs (PDP). These operations include, but are not limited to, applications, formularies, bids, marketing, audits, plan reporting and assessment, complaint tracking, and financial reporting.

Core Functions Include:

HPMS collects MA, Part D, Special Needs Plan (SNP), and employer group waiver applications from

both new organizations and existing organizations intending to expand their contract service area

HPMS enumerates all MA, PDP, cost, Program for All Inclusive Care of the Elderly (PACE), and demonstration contracts

HPMS performs automated reviews of MA, Part D, SNP, and employer group waiver applications, including pharmacy network and health services delivery (HSD) adequacy.

HPMS collects plan formulary submissions from all contracts offering Part D. HPMS collects plan bids and benefit packages from MA, PDP, cost, PACE, and demonstration plans.

HPMS collects Direct and Indirect Remuneration (DIR) data from all contracts offering Part D for payment reconciliation.

HPMS collects Medication Therapy Management (MTM) programs from all contracts offering Part D.

HPMS collects beneficiary complaints on MA and Part D plans and provides a casework resolution function for CMS, plan, Medicare Drug Integrity Contractor (MEDIC), and State Health Insurance Assistance Program (SHIP) staff.

HPMS collects the audit results for routine, focused, ad-hoc, plan bid, cost report, and financial audits of MA, PDP, cost, PACE, and demonstration plans.

HPMS collects marketing material submissions from MA, PDP, cost, PACE, and demonstration contracts.

HPMS collects fiscal solvency data from MA, PDP, cost, PACE, and demonstration contracts.

HPMS collects Part C and D plan reporting data and presents performance metric results for plan view.

HPMS enumerates Shared Savings Accountable Care Organization (ACO) program agreements.

HPMS performs automated reviews of ACO applications and participant lists.

HPMS collects marketing material submissions from ACOs.

HPMS provides monthly operational data feeds to the MA/Part D systems and the Social Security Administration (SSA) to support enrollment, payment, and premium withhold activities.

HPMS calculates the benchmarks and Part D plan premiums.

HPMS provides monthly operational data feeds to www.medicare.gov to support Medicare Options Compare (MOC) and Medicare Prescription Drug Plan Finder (MPDPF).

HPMS provides an interactive dashboard to assess plan and program performance.

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.

User Account Information: Every HPMS user must have a CMS account and be pre-approved for HPMS before being assigned access to the HPMS application. HPMS contains personally identifiable information in the User Account Maintenance modules for every user granted access to the application. In addition to the User ID, HPMS contains the first name, middle initial (optional), last name, e-mail address, organization name, address, city, state, zip code, phone number, and fax number (optional) for each registered user of the system. CMS uses these personally identifiable data to communicate with the registered users of HPMS for the following purposes: contacting individual users for help desk services, broadcasting announcements about system maintenance activities, creating audit records of activity within the application, and disseminating CMS policy and operational guidance. There are approximately 26 different user roles defined within the HPMS application ranging from internal CMS staff, state agency personnel, Office of the Inspector General, Health Plan staff, a variety of external contractor staff (contractors hired by various groups to assist with analyzing and processing HPMS data), and direct contractor/administrator staff hired to help maintain the HPMS application.

HPMS also collects certain personally identifiable information on Medicare beneficiaries and complainants in our Complaints Tracking Module (CTM). Specifically, HPMS collects the first name, last name, organization name, address, city, state, zip code, phone number, e-mail address, Health Insurance Clain Number (HICN), and plan member ID. Only the first and last names are required for complainants. None of these fields are required for Medicare beneficiaries. CMS uses these personally identifiable data to investigate Medicare Advantage (MA) and Part D complaints and perform casework activities.

HPMS displays personally identifiable information on Medicare beneficiaries enrolled in Medication Therapy Management Programs (MTMP). Specifically, HPMS displays the first name, last name, HIC number, and date of birth. Plan reporting data validation contractors use these data to validate plan data submissions. These data are required for MTMP submissions.

HPMS collects personally identifiable information on Medicare providers that are participating in a Medicare Shared Savings Accountable Care Organization (ACO). Specifically, HPMS collects the Taxpayer Identification Number (TIN) for participating providers. These data are used to uniquely identify and validate Medicare providers.

Lastly, HPMS collects personally identifiable information on Medicare beneficiaries in our Audit module including beneficiary name and HICN. These data are included in sample records provided by the MA or Part D organization undergoing the routine audit. CMS uses these data to run analyses to determine whether the organization is meeting program requirements.

This is the entirety of PII collected in the HPMS application.

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 of the data collected in the HPMS application is used to manage the following MA and Part D plan enrollment and compliance processes: application submission, formulary submission, bid and benefit package submissions, marketing material reviews, plan monitoring and oversight, complaints tracking, plan connectivity,

financial reporting, financial and plan bid audits, plan surveys, operational data feeds for enrollment, payment, and premium withhold, and data support for the Medicare & You handbook and the www.medicare.gov website. HPMS also supports the Shared Savings ACO program by managing the application submission, participant list submission, and marketing submission business processes.

HPMS User Access data is collected and maintained in order to grant appropriate access within the applications and to maintain an audit trail of user activity within the application.

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

Medicare beneficiary identifiers: HICN and plan member ID,

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

Public Citizens: includes only Medicare beneficiaries and other complainants - not the general public.

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The majority of PII collected in HPMS is used to support Medicare Advantage (MA) and Part D complaints and perform casework activities. These data are also shared with other federal agencies (e.g., Office of the Inspector General (OIG)) for research purposes.

HPMS collects personally identifiable information on Medicare beneficiaries enrolled in Medication Therapy Management Programs (MTMP) offered by Part D plans. These data are 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 providers that are participating in a Medicare Shared Savings Accountable Care Organization (ACO). These data are used to uniquely identify and validate Medicare providers.

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

meeting program requirements.

HPMS maintains information on the all the HPMS users, both internal and external as described in question 12, in order 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.

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

There are no secondary uses for the PII collected and stored within HPMS.

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

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) – 2/28/2018
0938-0944 (BPT) – 4/30/2017
0938-0469 (Fiscal Soundness) - 6/30/16
0938-0935 (MA application) - 1/31/2019
0938-0936 (Part D application) - 11/30/2017
0938-0992 (Part D reporting requirements) - 9/30/2016

0938-1054 (Part C reporting requirements) - 4/30/2017

0938-1000 (Audit) - 12/31/2016

Is the PII shared with other organizations?

Yes

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

Within HHS

HPMS data is used across HHS/CMS for the purposes of sharing communication; casework; program evaluation; research; and plan assessment information across the organization.

Other Federal Agencies

HPMS provides monthly data feeds to SSA to support enrollment, payment, and premium withholding activities. Additionally, other agencies may receive extracts of HPMS data to perform research.

State or Local Agencies

State/local agencies may access HPMS in order to support the resolution of complaints/casework; perform research; and/or obtain information on plan assessments.

Private Sector

External entities, such as Health Plans, access HPMS to support complaint/casework resolution and other activities involved in establishing and reporting on MA, MA-PD PD and ACO plans.

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

CMS has MOUs in place with States to support information sharing on complaint data.

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 ID request form. Moreover, due to the sensitive nature of the complaint, audit, ACO, 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 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.

In regard to the MTMP, CTM, Audit, and ACO 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. In regard to MTMP, audit, and ACO, these are records obtained through routine program administration activities in support of the Medicare Parts C and D and Medicare Shared Savings programs.

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. 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. ACO data is audited and validated by designated participant list reviewers as part of the ACO participant list submission and change request processes. HPMS users can access and update their account information at any time. HPMS collects only relevant PII necessary to implement application functionality. Information is removed from the application per the 10 year retention period defined in the HPMS SORN.

The job codes assigned via EUA to the user's credentials are periodically reviewed to ensure the user has the HPMS-Production job code. User 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.

Users:

Users require access to HPMS to perform casework activities on Medicare beneficiary complaints; to monitor plan performance; and, to perform research and analysis

Administrators:

HPMS system administrators have back end access to the HPMS architecture and it's data to ensure the stable system operations.

Developers:

Developers may have access to PII as part of their contracted task to make programming changes to HPMS, perform ad-hoc reporting, optimize performance and perform overall maintenance of the site.

Contractors:

Direct contractors may access the system to submit/review PII per their defined contracts. For example, audit data may be reviewed by CMS direct contractor staff.

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

Access to complaint, audit, ACO, and beneficiary-level MTMP data is 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.

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 to complaint, audit, ACO, and beneficiary-level MTMP data is 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 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 and ACO 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 conducted 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.

To ensure the security of the complaint information, AspEncrypt is used to encrypt and decrypt the HICN and Plan Member ID data as it is loaded to and read by the web server. AspEncrypt encrypts and decrypts the HICN and Plan Member ID using a 128-byte RC2 cipher. The HICN and Plan Member ID data remain encrypted while at rest in the database. This same approach is used to protect the MTMP data.

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

All traffic is encrypted using SSL;

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.