

# US Department of Health and Human Services

## Privacy Impact Assessment

**Date Signed:**

06/01/2016

**OPDIV:**

CMS

**Name:**

Automated Plan Payment System

**PIA Unique Identifier:**

P-9220941-496715

**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.**

No major changes have occurred in the system since the last review.

**Describe the purpose of the system.**

Automated Plan Payment System (APPS) computes interim and monthly payments to the plans that provide medical services and prescription drugs to Medicare beneficiaries. APPS tracks and collects User Fees, Coverage Gap Discount invoices and demonstration quality withhold payments. APPS processes files for the annual Part D Reconciliations and re-openings. Monthly/interim payment files are created for the Healthcare Integrated General Ledger Accounting System (HIGLAS) so that plans can be paid. APPS also creates payment reports for the plans.

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

APPS collects and stores banking information (Bank name/address, Employer identification number, account number) from plans, Part C/D payment data summarized at the contract level from the

Medicare Advantage and Prescription Drug system (MARx) and plan type, contract number and payment status from the Health Plan Management System (HPMS). This data is used to produce the monthly payment file for HIGLAS to send to Treasury.

APPS users must log into APPs through Access Manager with a user ID and password. Access Manager maintains the CMS user email address, name and phone numbers.

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

The APPS application provides the Centers for Medicare & Medicaid Services (CMS) with a mechanism for consolidating capitated payments from the Medicare Advantage Prescription Drug (MARx) system and ensuring that the Managed Care organizations (MCO) are paid every month. The application stores input data from several systems and provides interfaces through which CMS personnel review, update and refine the final payments due to the MCOs.

APPS stores payment information at the plan level (not at the beneficiary level) to process monthly plan payments and to create plan reports and the file to HIGLAS. There is no beneficiary PII collected, stored or processed by APPS.

APPS collects/stores the following information:

APPS receives its financial data from MARx on a monthly basis. The MARx system sends one file of all of the prospective payments due to the plans and another file containing all of the retroactive adjustments that took place during the payment period. Periodically the Payment Reconciliation System (PRS) supplies Part D drug payment data at the contract level to APPS that adjusts previous Part D payments already made to the MCOs.

The HPMS data are comprised of information about the MCO. It contains both current and historical data including, among other things, the payment status, plan name, plan type and other pertinent information about the MCO. These are critical for the monthly payment processing of APPS.

APPS users (about 35 internal users) are exclusively CMS personnel located at CMS headquarters. All access to the application is behind the firewall and through access manager. No user has the capability to access the application from the Internet, however, a user ID and password are collected in order to gain system access.

The data is stored permanently in the APPS databases and is shared with plans via monthly payment reports and with HIGLAS via the monthly payment file. The only purpose for this data is to compute accurate payments for active plans.

**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

Phone Numbers

Financial Accounts Info

Other - E-mail/Phone numbers are CMS not personal; CMS User ID and Password; Bank

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

Employees

Yes - MEDICARE ADVANTAGE, COST-BASED, DEMONSTRATION, PACE AND PRESCRIPTION DRUG PLANS

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

<100

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

To allow user access to the application and account maintenance. The user role assigned with the user ID defines the data that can be accessed.

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

There are no secondary uses.

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

42 Code of Federal Regulations 423.401(Medicare Prescription Drug Improvement and Modernization Act); 5 U.S.C 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.**

09-70-4001, Medicare Advantage Prescription Drug System

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

Online

**Government Sources**

Within OpDiv

**Non-Governmental Sources**

Other

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

N/A - the only PII is the information needed to allow authorized users to access the application.

**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.**

Before users are allowed to logon to APPS, they are prompted to select either "I accept" or "Decline" the terms and conditions for access to the application. The "I Accept" button notifies the user that their PII (CMS user ID/password, work email and work telephone number) is being collected and used.

**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.**

If users need to access APPS, there is no "opt- out" method. The users agree to the use of their information by selecting the "I Accept" button prior to each time that they log on. If they select "Decline", they cannot log on to APPS

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

It is highly unlikely that the use of the user access information would change. It is only used during the login process. If this usage changed, the process would be to notify the users via their CMS e-mail addresses. Follow ups using the CMS phone numbers would occur if needed.

**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.**

Since user credentials are collected in the Enterprise User Administration (EUA) system before being stored in APPS the EUA team would be responsible for breach reporting and resolution. The process is for the information system security officer (ISSO) of APPS to report the incident to EUA and they would direct the remedial action.

User information is obtained from EUA (ID/Password) and the CMS Outlook (email and phone number), so there is almost no chance of error. If an error is discovered, it is reported to the APPS ISSO for correction in the application.

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

In order to maintain the integrity, availability, accuracy, and relevancy of the PII stored within the database, the System Administrator, semi- annually, performs a crosswalk between the EUA listing of individuals with the user job code and APPS' listing of active users. Any anomalies (i.e. name change, or mismatch) is addressed and resolved by contacting the user, and modifying their user data, or by removing their access to APPS, if no longer required under their current job description.

Under this process, outdated, unnecessary, irrelevant, and inaccurate PII is identified and deleted from APPS. The PII is available as needed, and is sufficient (minimum required) for the purposes needed. The PII fields are locked and cannot be changed; The process to ensure that individuals who provide or modify PII cannot repudiate that action is done within the source (EUA) system. The process to ensure PII is available when needed is by having nightly updates run between the EUA systems and APPS; the process to ensure that PII is sufficiently accurate for the purposes needed is ensured when the nightly updates are sync. Users, can at any time, request that their PII (access) be deleted, by contacting their CMS

Access Administrator (CAA), who in turn, would take the corresponding action via EUA.

**Identify who will have access to the PII in the system and the reason why they require access.**

**Administrators:**

The APPS Application administrators are assigned the responsibility for adding, updating, and/or deleting user accounts.

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

In the APPs, the only PII is user access information. APPS uses role-based access and separation of duties policies to assign roles. Based on this, the only application role assigned to maintain user access records is the application administrator; of which there are 2. No other application roles can view/update user credential information.

**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.**

There are about 35 CMS users of APPS but the function to view and update user access information is limited to 2 individuals. No other application roles can access this PII data. Three quarters of the users can only request plan payment reports. The other quarter have various update capabilities depending on their job duties and assigned roles. These activities do not involve PII.

**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.**

CMS provides security awareness and privacy training that all CMS users are required to complete at least annually. The application administrators who are the only individuals/roles that allow access to the PII are information system security officers (ISSOs) who are required to attend additional role-based access training classes throughout the year.

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

The APPS application administrators attend role-based, privacy, security safeguards and other related training offered periodically during the year by the security office and office of technology solutions.

**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.**

If an APPS user needs to be removed; the APPS job codes are deleted from their user profile in EUA. When this occurs, an e-mail is created. The application administrators inactivate the User's PII (CMS user's ID, name, work email address and work telephone number) in APPS. This information is retained as inactive indefinitely by the application. Auditors request this information at the annual security controls assessment and the chief financial officer (CFO) audit. This information is only retained for the purpose of an application audit trail and is destroyed when no longer needed or when business ceases per 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.**

Physical controls such as the security of the physical plant, which include such items as providing long term power supply, emergency lighting, and fire protection are under the purview of the Baltimore Data Center staff. This includes physical access; which no APPS user has.

Technical controls are in place such as the Data Center manages remote access, equipment ordering/testing, and has responsibility for the EUA system (management of user accounts), which defines the privileges for each user of the information system(s); Information Security and Privacy Group coordinates compliance with security controls and the artifacts that document compliance by each application; and General Support System manages, among others, telecommunications, remote access, and transmission confidentiality. As the physical and technological aspects

Administrative control: APPS enforces role based security; users can only access data allowed for their role. All application roles are reviewed monthly by an ISSO for appropriate access. Access, or a change in Roles, can occur based on these reviews.