US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/26/2016

OPDIV:

CMS

Name:

Payment Reconciliation System

PIA Unique Identifier:

P-8139487-826878

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.

Payment Reconciliation System (PRS) has not undergone any changes within the last 12 months.

Describe the purpose of the system.

Payment Reconciliation System (PRS) aggregates payment data from Medicare Advantage and Prescription Drug (MARx) system, prescription drug event (PDE) data from the Drug Data Processing System (DDPS), and bid/direct and indirect remuneration data from the Health Plan Management System (HPMS) in order to perform the calculations for the Part D payment reconciliation.

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

PRS aggregates data from other CMS systems, MARx, PDE data from DDPS, and bid/direct and indirect remuneration data from HPMS for purposes of calculating Part D final payment.
The data includes name, date of birth (DOB), mailing address, phone numbers, Health Insurance

Claim Number (HICN), and plan member ID. System users access PRS using password and user ID.

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

Payment Reconciliation System (PRS) aggregates data related to Part D contracts and plans from HPMS, beneficiary enrollment and prospective payment information from MARx, actual drug utilization costs from Drug Data Processing System (DDPS), annual budget neutrality amounts, risk sharing rates, threshold percentages, and plan level adjustment amounts from CMS Department of Payment Reconciliation (DPR). Once the results of the reconciliations are accepted, PRS creates a payment file to send to the Automated Plan Payment System (APPS). In order to access PRS, system users such as CMS employees and CMS contractor support, enter their user ID and password.

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

Mailing Address

Phone Numbers

Other - Medicare beneficiary identifiers: plan member ID and HICN; system user credentials: user ID

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

Employees

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

Vendor/Suppliers/Contractors

Patients

Medicare beneficiaries and other complainants.

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

System shares PII with Part D plans in which individuals are enrolled for purposes of explaining costs and payments used in calculating the reconciliation. In order to access PRS, system users such as CMS employees and CMS contractor support, enter their user ID and password.

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

There is no secondary use for which PII is used.

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

The Privacy Act permits the disclosure of information without an individual's consent if the information is to be used for a purpose that is compatible with the purpose for which the information was collected. Any such disclosure of data is known as a "routine use."

This system contains Protected Health Information as defined by HHS regulation "Standards for Privacy of Individually Identifiable Health Information" (45 CFR Parts 160 and 164, 65 FR 82462 (Dec. 28, 00), as amended by 66 FR12434 (Feb. 26, 01)). Disclosures of Protected Health Information authorized by these routine uses may only be made if, and as, permitted or required by the "Standards for Privacy of Individually Identifiable Health Information."

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.

09-70-0553, "Medicare Drug Data Processing System (DDPS)"

SORN is In Progress

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Other HHS OpDiv

Identify the OMB information collection approval number and expiration date

Data used in the Payment Reconciliation System (PRS) has already been collected from another CMS system; therefore, no OMB information collection approval number is required. The information collected in person is system user credentials.

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.

Data used in the Payment Reconciliation System (PRS) has already been collected from other CMS systems. As the PRS receives information from other systems, rather than directly from individuals, it is the responsibility of the systems collecting the information directly from individuals to provide prior notice. Upon enrollment in Part D plans, beneficiaries are provided with the Privacy Act and notified that they must provide data in order to enroll in a Medicare Part D plan.

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.

Individuals cannot opt out of the collection of their information because data used in the Payment Reconciliation System (PRS) has already been collected from other CMS systems. This data does not involve direct collection or sharing of PII with anyone other than the plan in which the individual enrolled and to whom the individual granted permission to use this information.

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

Data used in the Payment Reconciliation System (PRS) has already been collected from other CMS systems. Because PRS only receives data collected by a different system, there is no process in place for notifying individuals or obtaining their consent. Upon enrollment in Part D plans, participants are given the choice and choice is offered and also informed that the data is necessary in order to enroll in a Medicare Part D plan.

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.

Data used in the Payment Reconciliation System (PRS) has already been collected from other CMS systems. Individual are notified annually in the Medicare & You handbook of their right to complain about any alleged violation of their privacy rights. Participants in the Part D Drug program may complain to their Plan sponsors to whom they provided their information.

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

There is no direct data collection of Personally Identifiable Information within the PRS application; therefore, a review of the data integrity is not performed at the application level, rather it relies on other CMS systems for data verification processes to ensure PII is timely, accurate and relevant. However, file integrity is performed each time PRS receives flat files for reconciliation. File integrity checks ensure the data integrity performed at the Plan Sponsor (at which time the patient data is collected) remains accurate. PRS system developers and contractors ensure the availability of PRS and the PII contained within the system. PRS undergoes rigorous security audits on an annual basis to ensure required administrative and technical safeguards are in place to protect the confidentially, integrity and availability of data.

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

Users:

Internal CMS systems are considered ‘users’ and they require access to information about beneficiary enrollments and payment calculations.

Administrators:

For system administration

Developers:

The staff necessary to develop, test, validate, and support the developed system.

Contractors:

The staff necessary to develop, test, validate, and support the developed system.

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

CMS system administrators grant access to authorized and approved users by assigning job codes restricted to least privilege and need to know basis. User access is recertified yearly in line with CMS security policy requirements.

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.

Mainframe access enforcement developed, documented, and implemented on the system. Access is always based on least privilege, explicitly denied unless otherwise granted.

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.

Security Awareness and Privacy training is provided to personnel on an annual basis and acknowledge successful training after passing a test at the end of training and the system verifies completion. Included in the training is education about how to properly handle sensitive data. A separate training module for Records Management is also completed.

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

There are no users of the PRS system in the traditional sense of the term. PRS is a batch file system operating on the CMS Mainframe. Therefore, there is no PRS specific user training that is above and beyond the general CMS Security and Privacy Awareness training.

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.

Records are maintained with identifiers for all reconciliations for an indefinite period currently, due to appeal and reopening
requirements. Thereby the records disposition is permanent and to be cut off annually. Pre-accession files to the National Archives are 5 years after cutoff. PRS will legally transfer individual files in acceptable format (following current CFR guidelines) to the National Archives annually, 20 years after cutoff. Include an electronic copy of the system documentation (i.e., codebooks, record layout, user guides and any other technical specifications) with the transfer. (Disposition Authority: N1-440-09-04). PRS records such as ad hoc reports (includes but not limited to: MCO-level payment amount, beneficiary complaints, prescription drug events, Medicare Advantage, Prescription Drug Costs, premium and payment reports, withheld drug premiums are held temporarily. They are to be destroyed when no longer needed for administrative, legal, audit or other operational purposes, provided the printouts do not contain substantive information, such as substantive annotations, that is not included in the electronic records (Disposition Authority: NARA's GRS 20, item 16).

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

Payment Reconciliation System (PRS) beneficiary level data resides on the CMS mainframe which is housed in the Baltimore data center behind locked doors and is only accessible by approved personnel. All policies relating to information security are addressed in the CMS organizational security and privacy policy and procedures, including the CMS policy for Information Security Program and CMS Acceptable Risk Safeguards (ARS). Records are housed in both active and archival files in an encrypted format to protect data confidentiality and integrity. Technical controls include access controls which are established to limit operations and maintenance user access to the data based on role based design and assigned on a need to know basis. Data is protected by the mainframe security configuration and Resource Access Control Facility (RACF) controls.