US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/20/2025

OPDIV:

CMS

Name:

Payment Recovery Information System (PRIS) Plan Portal

PIA Unique Identifier:

P-8728155-795925

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?

Yes

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.

There have been no changes to the system.

Describe the purpose of the system.

The Business Purpose of the Payment Recovery Information System (PRIS) Plan Portal application is to serve as a portal for Centers for Medicare & Medicaid Services (CMS)/Center for Program Integrity (CPI)/Division of Prescription Drug Audits (DPDA), Plan Program Integrity (PPI) Medicare Drug Integrity Contractor (MEDIC), and the Medicare Advantage (MA/Part C) and Prescription Drug (Part D) Plans organizations to collaborate on the data and documents related to the Medicare Part C and Part D audit findings, Program Integrity (PI) findings, and communicating to Plan Sponsors for Education and Outreach related to the subject audit.

The three primary end user groups who interact with the system are:

PPI MEDIC Data User.

CMS/CPI/DPDA Data User.

Plan User.

The PRIS Plan Portal application helps to manage and safeguard the documents and data related to the audit, record decisions, and automate workflow based on the governing business process to reach business outcome.

The CMS function that will be benefited by this application is the CMS/CPI/DPDA business division.

The first release of the application will be the implementation of the Self-Audit business workflow.

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

Following are the data elements stored in the system:

Subject of the Audit (Medicare Audit Type, Parent Organization, Plan Contract Numbers, Audit Year).

Project Title/Description of the Audit in question (Self-Audit).

Prescription Drug Event (PDE) record count - Original and Final value.

Inappropriate PDE counts - Original, Adjusted, and Final values.

Inappropriate Payment Amount (Return on Investment) - Estimated and Final values.

Document Request List (DRL) items submitted by CMS.

Information about Person: Name, Email Address, and Physical Address.

The following are the documents uploaded to PRIS Plan Portal to support the analysis of the audit and its findings: Project Proposal, Project Timeline, PDE Records File, Engagement Letter, Closeout Letter, Deletion Check Report document/file, Self-Audit Attestation Workbook, Meeting Agenda, Meeting Minutes, Kick-off call Presentation, and Plan Sponsor Supporting Documents. Following are some of the key data elements contained in one or more of these documents: Phone number, Medical Notes, Medical Records Number, Date of birth, Sex, National Provider Identifier (NPI), and Drug Generic Name/Identifier.

The data from the documents are not extracted by or used in any other way by the system.

All this information is stored within PRIS for the length of time appropriate to satisfy the CMS Records Management requirements. The management and maintenance of the user information to create user accounts for the PRIS Plan Portal User Interface (UI) is handled within CMSs Identity Management (IDM) system. Usernames and passwords are collected by CMS IDM system separate from PRIS and is covered by its own Privacy Impact Assessment (PIA).

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

The CMS/CPI/DPDA, with the help of the PPI MEDIC identifies and justifies scenarios where improper payments are likely to have been made in Medicare Part C and Part D programs. This is initiated by evidence found in a partial sampling of existing PDEs records and targeted industry research performed by the PPI MEDIC and includes clear criteria for identifying these situations

within an audit framework. If the scenario is approved for auditing by CMS, transactions matching the criteria are audited using the Supporting Documentation and PDE records to verify their validity in the specific context. Additionally, CMS/CPI/DPDA works with PPI MEDIC to oversee the integrity of these audit programs for its effectiveness to comply with CMS requirements, identifying program vulnerabilities, and ensuring Plan Sponsor's adherence to regulatory requirements. The PRIS Plan Portal application will be the system for CMS/CPI/DPDA to achieve this business mission.

The three primary end user groups who interact with the system are:

PPI MEDIC Data User.

CMS/CPI/DPDA Data User.

Plan User.

The PRIS Plan Portal system collects and maintains (stores) the information to increase transparency related to the Medicare Advantage and Prescription Drug Plan programs plan audits and other various types of audits to help drive the industry towards improvements in the delivery of health care services in the Medicare Advantage and Prescription Drug programs. The following are the documents uploaded to PRIS Plan Portal to support the analysis of the audit and its findings: Project Proposal, Project Timeline, PDE Records File, Engagement Letter, Closeout Letter, Deletion Check Report document/file, Self-Audit Attestation Workbook, Meeting Agenda, Meeting Minutes, Kick-off call Presentation, and Plan Sponsor Supporting Documentation.

The information collected in the system is not shared with any third-party vendor, or outside system other than the individual/organization who is the subject of the audit and/or who have a need-to-know of the audit results and findings. All this information is stored within the PRIS Plan Portal for the length of time appropriate to satisfy the CMS Records Management requirements.

The first release of the application will be the implementation of:

Self-Audit business workflow.

System/Email Notifications.

Reports.

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 Records Number
Medical Notes
Financial Accounts Info
Sex, Medical Notes, Pharmacy/Prescriber National Provider Identifier (NPI), Drug Generic Name/Identifier, etc.

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

Employees
Vendor/Suppliers/Contractors
Patients

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

To monitor and address Medicare Part C and Part D Program Integrity and Vulnerability.

Ensure compliance with regulatory requirements.

Most of the Personal Identifiable Information (PII)/Protected health information (PHI) information is contained within the PDE Records file, Supporting Documentation and Deletion Check Report. This data is not extracted by or used in any other way by the system.

The PDE records are used to justify the existence, volume, and validity of a particular audit issue that is the subject of the audit. This will be a smaller random sub-set of the total PDE records available within a given time frame. The PDE Records are uploaded by the PPI MEDIC as part of the audit workflow process based on the criteria and volume required by the associated approved project proposal. These details help CMS and PPI MEDIC determine whether the payment was properly done, or improper, as the name suggests.

Supporting Documentation is provided by the Plan Sponsors through the UI and is used as reference to make a final decision on the audit that is the subject of investigation.

Deletion Check Report is used to monitor the status of the Plan Sponsors compliance to audit results and findings.

The information collected in the system is not shared with any third-party vendor, or outside system other than the individual/organization who is the subject of the audit and/or who have a need-to-know of the audit results and findings.

The usernames and passwords are handled through the login procedure of CMSs IDM system prior to PRIS Plan Portal, and do not get recorded by the PRIS Plan Portal system.

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.

Under §§ 1874(a) and 1875 of the Social Security Act (the Act) and Title 42 United States Code (U. S.C.) section 1395kk(a) and 1395ll 5 U.S.C. 552a

Are records on the system retrieved by one or more PII data elements?

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Other

Government Sources

Within the OPDIV

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

Not Applicable.

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.

Prior notice is given to the individuals at the time of accessing the PRIS Plan Portal (PMPP) application. This information is provided as approved business use from the original collection source under CMSs use as part of PDEs and Plan Sponsor's submissions.

Before users are allowed to logon to PMPP application, they are required to select "Agree to our Terms & Conditions".

This "Agree to our Terms & Conditions" button notifies the user of the following:

OMB No.0938-1236 | Paperwork Reduction Act Updated Departmental Standard Warning Banner for HHS Information Systems, Memo dated July 14, 2016 This warning banner provides privacy and security notices consistent with applicable federal laws, directives, and other federal guidance for accessing this Government system, which includes (1) this computer network, (2) all computers connected to this network, and (3) all devices and storage media attached to this network or to a computer on this network. This information system is provided for Government-authorized use only. Unauthorized or improper use of this system is prohibited and may result in disciplinary action and/or civil and criminal penalties. Personal use of social media and networking sites on this system is limited as to not interfere with official work duties and is subject to monitoring. By using this system, you understand and consent to the following: The Government may monitor, record, and audit your usage, including usage of personal devices and email systems for official duties or to conduct HHS business. Therefore, you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this system. At any time, and for any lawful Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this system. Any communication or data transiting or stored on this system may be disclosed or used for any lawful Government purpose.

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 option to opt-out of the collection or use of PII within PRIS Plan Portal because the data used in PRIS Plan Portal application has already been collected from other CMS systems. This data does not involve direct collection or sharing of PII with anyone other than those involved in auditing these payments as part of the original agreement to participate in the Medicare Part C and Part D audit programs.

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

The PII/PHI within the PRIS Plan Portal is provided by CMS and PPI MEDIC on behalf of those the PII relates to. Participants are given the choice and informed that the data is necessary and may be later used when being audited in this way to enroll in a Medicare Part C and Part D plan. Prior notice is given to the individuals at the time of accessing the PMPP application. This information is provided as approved business use from the original collection source under CMSs use as part of PDEs and Plan Sponsor's submissions.

If a major change occurs, it would be the responsibility of the Plan Sponsor to provide written communication/agreement that data is required to be reported to CMS when requested for various legal matters. This would include audits.

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.

Any individual who has concerns should contact CMS through the Office for Civil Rights (OCR), which can be done by visiting https://www.hhs.gov/hipaa/filing-a-complaint/. Information about the ability to file a complaint is available at this same address.

If the Internet is not accessible, and you have questions about this topic, CMS can be reached by phone at 1-800-MEDICARE (1-800-633-4227). When calling, ask to speak to a customer support rep about Medicare’s Privacy Notice. TTY users may call 1-800-486-2048.

Individuals who wish to file a complaint directly without access to the Internet may directly call OCR at 1-800-368-1019. TTY users may call 1-800-537-7697 to file their complaints.

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

CMS has a National Institute of Standards and Technology (NIST)-compliant continuous monitoring program to ensure system integrity and availability for all data submitted to PRIS Plan Portal application. Yearly testing of the system is required to review and update this process for disaster recovery purposes. Back-ups are in place to ensure information is readily available, even if one or more servers should fail. All files uploaded are virus scanned and secured to ensure that changes or unauthorized disclosures are prevented.

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 to the PMPP is granted through IDM authentication. Users are required to go through the registration and Remote Identity Proofing (RIDP) process in IDM for an IDM identification (ID) and should request the appropriate user role for the PMPP application. Contingent upon the user's role being approved by CMS, the user can logon to the application.

CMS/CPI/DPDA Business Owner is approved by IDM Tier 2 Helpdesk role. This is based on the workflow model set up in IDM system for application integrated with IDM system.

PPI MEDIC Users, CMS/CPI/DPDA Audits Users, External Points of Contact (EPOC) Users, and Administrator Users are approved by the CMS/CPI/DPDA Business Owner through the appropriate procedures within IDM system. Each user is provided the specific security IDM job role that is appropriate for their needed business role.

Administrators are also authorized by the CMS/CPI/DPDA Business Owner. Their access is limited to support functions in support of the helpdesk process.

Plan Users are approved by EPOC users specific to contracts that the users represent and have access to within the IDM system.

Those in the developer role are not provided direct access to any production data that may contain PII.

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 the PMPP is granted through IDM authentication. Users are required to go through the registration and RIDP process in IDM for an IDM ID and should request the appropriate user role for the PMPP application. Contingent upon the user's role being approved by CMS, the user can logon to the application.

Access to PRIS Plan Portal is granted if the user's job role is approved in IDM by the CMS/CPI/DPDA Business Owner. Users' system access is limited to the functions and information which is essential to their job functions based on their role.

Further, access privileges dictated by CMS within the user interface will restrict users to access and view only the minimum information needed to perform their job function.

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 employees and contractors are required to take the annual CMS role-based privacy and security awareness training. Internal and external security and privacy staff attend the CMS quarterly security awareness training and meetings throughout the year to keep abreast of relevant and timely security issues. Additionally, all the users are required to complete annual recertification of their user roles to continue to have access to the PMPP application.

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

Administrators and Developers receive role-specific yearly training for role-based security.

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 has employed a records retention schedule referred to as a "Bucket Approach," or otherwise known as flexible scheduling. More about this approach, what it means, and how it is applied at Federal Agencies can be found on the National Archive's (NARA) website at: https://www.archives.gov/records-mgmt/faqs/flexible-scheduling.html

Since the PDE records and Supporting Documentation in packages that are used for reviewing the compliance and ensuring the integrity of Medicare programs, they are considered part of Retention Schedule Bucket 9: Compliance and Integrity within the records schedule number for CMS (DAA-0440-2015-0012) with the following authorities: Performance Measurement Reports (DAA-0440-

2013-0010, Item 0001) and Overpayment Reports (NC1-440-79-01, Item, II/18 (39) and III/R). All files within this grouping are considered Temporary; they do not have to be transferred for Permanent storage at NARA once the amount of time they must be retained is complete. All files within this category must be destroyed after ten (10) years old or when no longer needed for agency business, whichever is later.

Every January, relevant files for the previous calendar year are reviewed for deletion based on the date of their creation. For example, in January of 2018, all the packages created from January to December of 2010 will be reviewed. Packages that are currently part of a legal discovery or otherwise related to active agency business as determined by the system owners/COs will be removed from consideration and kept. All exceptions will be included in the following year's review. The rest of these packages are then deleted and removed by the system administrators.

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

The PRIS Plan Portal data resides in the AWS Cloud Data Center which is housed in the AWS US East Data Zone and is only accessible by approved personnel. The physical security of the data center is outside the scope of the PRIS Plan Portal Application Development Organization (ADO).

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).

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.

The application is regularly assessed using the CMS security policies and controls that include administrative, technical, and physical controls. All controls are tested within a 3-year period as part of annual FISMA evaluations.

Identify the publicly-available URL:

https://pmpp.cms.gov/

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

No

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null