US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/06/2024

OPDIV:

CMS

Name:

Retiree Drug Subsidy System

PIA Unique Identifier:

P-2107900-997591

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.

None

Describe the purpose of the system.

The purpose of the system is that it serves as a payment system for Plan Sponsors participating in the Retiree Drug Subsidy (RDS).

The Core Functions of RDS are that it Enrolls Organizations (Plan Sponsors) into the Retiree Drug Subsidy (RDS); Verifies the Plan Sponsor's covered retirees are Medicare/Part D eligible; and calculates and generates payments to the authorized Plan Sponsors. Plan Sponsors also have the ability to appeal and dispute RDS decision.

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

The system collects demographic and financial information (Account and Routing numbers) on the Plan Sponsors (End User) and Demographic Data on Medicare Eligible persons (Plan Sponsors' retirees) enrolled in RDS (Medicare Part D) Plans as well as users of the system.

Beneficiary data about the Plan Sponsors' retirees is needed to confirm eligibility as a "qualified covered retiree" for purpose of payment. A qualified covered retiree is eligible for, but not enrolled in a Part D Plan.
Beneficiary data includes Social Security Number (SSN) and work demographic information (Workplace and Title), CMS Health Insurance Claim Number (HICN) and benefit paid information/Benefit Option Identifier of the retirees.

User (Plan Sponsor) Data, or Personally Identifiable Information (PII) pertaining to Authorized Representatives, Account Managers, Designees, and Actuaries is used to validate an individual against United States (US) Office of Inspector General (OIG) and US Government Accountability Office (GAO) for registration of user credentials. This includes Name, Address, Social Security Number (SSN), Plan Sponsor Address, Email Address, Date of Birth, Photo ID, Driver License Number, Employer Identification Number, Organization Name, Employer Banking information, security questions, Employer Website, Phone and extension, and Fax Numbers to verify and assure the users' identity.

Users (Plan Sponsors) gain access through self -registration on the RDS Public Website (PWS). The RDS System collects End User PII user credentials, user ID password, and Google Authenticator Key during registration to verify and assure the identity of the End User process.

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

The RDS system is designed to facilitate the distribution of a subsidy to various retirement programs (state, local, union, etc.) that provide their members a drug prescription benefit. This is intended to ensure that such programs simply do not fold their drug benefits and push their users onto Medicare Part-D, which would add enormous expense to the program. RDS collects the Social Security Number (SSN) and work demographic information of the end user (Plan Sponsor) (to verify their employment/disbarment status) as well as CMS Health Insurance Claim Number (HICN) and benefit paid information/Benefit Option Identifier to calculate the subsidy that will be issued. This data is stored in an Oracle database component of the system permanently due to the legal requirements of the program. RDS retrieves demographics and entitlement records about beneficiary using key (MBI/HCIN/SSN) from CMS BIC (Beneficiary In Cloud) interface on a daily basis through batch cycles. End user (Plan Sponsors) data (Name, Address, Telephone Number, Email Address, Date of Birth, Photo IDs, Driver License Number, SSN, Workplace, title, Employer Banking information, Security Question/Answers, Employer Website) is shared with the LexisNexis Group, to verify a system end user is associated with the company requesting the subsidy. User Credentials, which are created by the users themselves, are also collected and stored.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Social Security Number
Date of Birth
Name
Photographic Identifiers
Driver's License Number
Mother's Maiden Name
E-Mail Address

Mailing Address
Phone Numbers
Medical Records Number
Financial Accounts Info
Military Status
Taxpayer ID
Other: Date of Death, Health Insurance Claim Number (HICN); Medicare Beneficiary Identifier (MBI); Plan Sponsor identification number, Benefit Option Identifier; Workplace, title, Employer Banking information, Employer Website; benefit paid information/Benefit Option Identifier of the retirees; Answers to security questions may include: city you were born, name of your elementary school, father's middle name, grandmother's first name, mother's maiden name, year you graduated from high school, and user credentials- user ID and password.

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?

RDS shares PII with Federal Law Enforcement Agencies and with CMS information systems such as the Medicare Beneficiary Database (MBD) to verify retirees' ability to be claimed by an Employer Plan Sponsor as a qualifying covered retiree under the RDS program. In additional PII may potentially be shared with Federal Law Enforcement Agencies the CMS Office of Hearings, the Office of the Administrator, LexisNexis for Secure Website user (Plan Sponsors) validation, and CitiBank for payment disbursement. In addition, PII may be shared for the purposes of Congressional Requests and during audits and cost reporting.

User credentials are collected in order to access the system for system support and maintenance.

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

None

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

In accordance with requirements of the Privacy Act of 1974 and Under section 1860D–22 of the Social Security Act (the Act), employers and unions who continue to offer prescription drug coverage to their qualifying covered retirees are eligible to receive a tax-free subsidy for allowable drug costs. This amended provision of the Act is mandated by section 101 of the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) (Pub. L. 108–173). Authority for maintenance of this system is given under section 1860D–22 of the Act (Title 42 United States Code (U.S.C.) 1302, 1395w– 101 through 1395w–152, and 1395hh). These provisions of the Act are amended by section 101 of the MMA and its implementing regulations codified at Title 42 Code of Federal Regulations (CFR) Part 423, Subpart R.

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.

09-70-0550, "Retiree Drug Subsidy (RDS) HHS/CMS/CM"

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Email

Online

Government Sources

Within OpDiv

Other HHS OpDiv

Other Federal Entities

Non-Governmental Sources

Public

Commercial Data Broker

Media/Internet

Private Sector

Identify the OMB information collection approval number and expiration date

0938-0957 Expiration 11/30/2024; 0938-0977 Expiration 11/30/2024

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.

There is a CMS Information Sharing Agreement that is in place with Lexis-Nexis.

Describe the procedures for accounting for disclosures.

The RDS Program requires disclosures of PII through LexisNexis for user verification prior to access being granted. As such, all disclosures are accounted for through the end user's (Plan Sponsors) account.

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

The RDS Program has a publicly published Privacy Notice and a publicly published End User Guide detailing the steps of the collection process. Both the Privacy Notice and the RDS Users Guide are located on the RDS Public Website. For Employees, Login Banner Statements are displayed and must be agreed upon prior to access to the RDS Application. The login banner states that employees' actions are monitored while accessing RDS.

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.

This is done through Paperwork Reduction Act (PRA) notices, Outreach email, Public Website

(PWS), webinars, and system of record (SOR) notices. CMS is required to provide updated Notices of Privacy Practices. Other methods include the Secure Website User Guide, PRA, and the User Agreement. Privilege and Non-Privilege User Access to the RDS Program does not allow opt-out of collections or use of PII. Login Banner Statements must be accepted prior to gaining access RDS.

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

The information is mandatory for participation in the program. CMS is required to provide updated Notices of Privacy Practices.

RDS Program End Users (Plan Sponsors) are also notified of changes through updates to the RDS Secure Website, RDS Public Website, RDS User Guide, PRA, the User Agreement, PRA notices, Outreach email, webinars, and/or SOR notices prior to any changes implemented to RDS.

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.

Retirees follow the notification process as described in the Annual “Medicare and You” Handbook. Other users (Plan Sponsors) can contact the CMS RDS Center Help.

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

RDS interfaces with MBD, MARx and Lexis Nexis to validate the accuracy of PII provided by external entities. Inaccuracies are flagged by RDS and returned to the source for correction.

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 PII information by system users is determined utilizing role base access based on Least Privileges. RDS has created the following roles:

System Administrators containing full access to the particular systems to which they are assigned for system maintenance and support.

Application Administrators have limited access to the operating system functions, but full access to assigned application components for application maintenance enhancement and future releases.

Security auditors and analysts have access to auditing and security monitoring for security control audits and reporting in addition to monitoring environmental activity.

These roles are given least privileges to perform their duties and will have to request approval before being granted escalated privileges.

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.

Users are granted a specific level of access to the operating system on which they are working. This access is only granted after an approval process is performed via the ticket management system. After approval, access is granted for specific named role access to a system. Users with certain access can only perform specific actions on that system, such as WebSphere Application Server (WAS) administrators cannot perform administrator functions on a Unix system.

Each role has a minimum privilege need to accomplish the assigned work. Users are assigned to roles based on the concept of least privileges. Administrator roles are granted so that they can perform only the tasks which they need to while blocking them out from all other tasks. Employees

must be authorized by their manager as well as the System Security Officer to perform privileged functions. Active Directory is used to enforce least privilege in conjunction with our ticketing system and audit log reviews for escalated privileges.

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.

All Organizational Users of the RDS System must undergo yearly CMS security awareness and training as required by CMS security standards. This includes general security awareness, notations of conflict of interest, internal controls training, and import/export restrictions.

All staff that work projects that fall under HHS and its Operating Divisions must take HIPAA, and security policy training and acknowledgment. Additionally, all staff that work on HHS projects must acknowledge understanding and compliance with HHS rules of behavior (HHS-OCIO-OIS-2019-05-004)

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

The System Security Officer (SSO) is responsible for ensuring that all personnel are appropriately trained and have signed a Security Awareness and Training (SAT) acknowledgement and agreement forms. User training consists of a one-hour briefing emphasizing security awareness and policies in addition to fire and safety training. The curriculum includes the purpose of security, security contacts, the Health Insurance Portability and Accountability Act (HIPAA), IRS and privacy awareness, types of malicious activities, internal controls trainings, recognition of security incidents and the requirement to report them. Training includes Rules of Behavior, such as securing sensitive information, securing workstations, using licensed software; prohibitions against network or workstation modification, incident reporting and password management are covered in Security Awareness Training. In addition, building and physical security guidelines are stressed, and staff is encouraged to report safety issues. Corporate Code of Conduct training is given annually via web training Learning Management System (LMS). This training, which overlaps SAT, details corporate policies and procedures and how they apply to each employee. Reports are generated by the LMS. The Training department ensures that everyone takes the training and agrees to it annually.

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.

In accordance with CMS policy and the RDS Statement of Work (SOW). RDS Data is stored for at least seven (7) years and destroyed in accordance with NIST 800-88. RDS Program also abides by National Archives and Records Administration (NARA) for Financial or payment, enrollment, and beneficiary records. Financial or payment related records are governed by DAA-0440-2015-0004-0001 (Bucket 3). Destroy no sooner than 7 year(s) after cutoff but longer retention is authorized. Enrollment records are governed by DAA-0440-2015-0006 (Bucket 4). Destroy no sooner than 7 year(s) after cutoff but longer retention is authorized. Beneficiary records governed by DAA-0440-2015-0007-0001 (Bucket 5). Destroy no sooner than 10 year(s) after cutoff but longer retention is authorized. Note that disposition schedules were approved by National Archives and Records Administration (NARA). Delete/destroy when agency determines they are no longer needed for administrative, legal, audit or other operational purposes.

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

Physical Controls: N/A The RDS SYSTEM resides on the CMS AWS enclave and has no physical presents.

Technical: RDS uses CMS approved encryption algorithms (FIPS 140-3) for data at rest and in

transit. Multiple intrusion detection and prevention methodologies are employed, and the system is tested regularly (multiple times a year) for application vulnerabilities, and daily for system vulnerabilities. Role Based Access is also employed to limit access to PII based on role function and least privileges.

Administrative: Policies and Procedures have been created on securing PII in the RDS system. An example of these, there are Security Awareness and Training (SAT) policies, policies on the storage of PII, access control policies are used for login access, policies for following the NARA record retention policy. Also, RDS has policies on continuous monitoring of the system and audit log reviews.

Identify the publicly-available URL:

https://www.rds.cms.hhs.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?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

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?

No