US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/05/2024

OPDIV:

CMS

Name:

Drug Data Processing System

PIA Unique Identifier:

P-2911720-675947

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.

The Drug Data Processing System (DDPS) is going through V3 (legacy) to V4 (Greenfield) migration. V3 (Legacy) to V4 (Greenfield) migration is part of a CMS initiative to standardize all accounts to modern cloud architecture. DDPS is moving our existing AWS V3 and migrating to AWS V4. Ultimately, AWS V3 will be going away and DDPS will be in AWS V4. All settings will remain the same outside of the differences and benefits of the AWS V3 vs. AWS V4.

Account to Virtual Private Cloud (VPC) mapping more aligned to business processes and needs

Flexibility in VPC-to-Account Mapping

Fewer accounts to manage (i.e. One Production and One Non-Production Account) and ability to apply variations based on business needs.

Improved cost savings

New AWS account (Non-prod and Prod)

Mapping of EUA users to pre-existing CloudTamer/Kion roles

Name of new VPCs to be created (e.g. DEV, TEST, IMPL)

VPC peering requirements.

Describe the purpose of the system.

The Centers for Medicare & Medicaid Services (CMS) implemented the Drug Data Processing System (DDPS) to support CMS' implementation of a new prescription drug benefit program for Medicare mandated by the Medicare Prescription Drug Improvement and Modernization Act (MMA) of 2003. This system processes all Medicare covered and non-covered prescription drug events (PDEs) and related data, including non-Medicare drug events as necessary, to validate/authenticate Medicare payment of covered drugs made by plans for Medicare beneficiaries enrolled in Part D.

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.

This system processes data that is collected from other CMS systems, which have validated data and each of these systems have their own respective Privacy Impact Assessments (PIA). The CMS systems that provide data to DDPS are covered under individual Privacy Impact Assessments (PIA). Source System input files come from Prescription Drug Front End System (PDFS), Medicare Advantage Prescription Drug System (MARx) or Medicare Beneficiary Database (MBD), Health Plan Management System (HPMS), National Plan and Provider Enumeration (NPPES), and the Provider Enrollment, Change and Ownership System (PECOS), Non-PII pharmacy information externally comes from the National Council for Prescription Drug Programs (NCPDP), Medispan, Preclusion Data, and First Data Bank (FDB). The data those systems collect includes: name, phone number, mailing address, detailed and summary beneficiary prescription drug claim data, health insurance claim number (HICN)/Medicare Beneficiary Identifier (MBI), card holder identification number, mailing address, date of service, gender and, optionally, the date of birth, provider characteristics, prescriber identification number, assigned provider number (facility, referring/servicing physician), national drug codes, in addition to beneficiary, plan, and supplemental payment amounts. System users access DDPS 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.

The Drug Data Processing System processes, validates, authenticates, and maintains/stores all covered and non-covered drug transaction events, including payments, for covered drugs made by plans on behalf of enrolled Medicare beneficiaries; it includes detailed and summary beneficiary prescription drug claim data, health insurance claim number (HICN)/Medicare Beneficiary Identifier (MBI), card holder identification number, mailing address, date of service, gender and, optionally, the date of birth, provider characteristics, prescriber identification number, assigned provider number (facility, referring/servicing physician), national drug codes, in addition to beneficiary, plan, and supplemental payment amounts. It also supports fraud, waste, and abuse analysis; risk adjustment; drug utilization analysis; auditing; trends analysis; payment reconciliation; benefit adjustment analysis; and general Prescription Drug Event reporting. The Drug Data Processing System does not collect information directly from beneficiaries, but receives it from the following CMS systems:

Prescription Drug Front End System (PDFS) on a daily basis, Medicare Advantage Prescription Drug System (MARx) on a monthly basis, Medicare Beneficiary Database (MBD) on a daily basis for beneficiary information, Health Plan Management System (HPMS) on a monthly basis, National Plan and Provider Enumeration (NPPES) on a weekly and monthly basis, and the Provider Enrollment, Change and Ownership System (PECOS), Non-PII pharmacy information comes externally from the National Council for Prescription Drug Programs (NCPDP) on a weekly and monthly basis, Medispan on a daily basis (Monday through Friday), Preclusion Data on a monthly basis, and First Data Bank on a weekly basis. In order to access DDPS, system users, CMS employees and CMS direct contractor support, enter their user ID and password.

DDPS retrieves beneficiary, demographic, and plan enrollment information daily from the Common Medicare Environment (CME), which houses the enrollment data. The DDPS Operational Data Store (ODS) retrieves this data via the Medicare Beneficiary Database Application Program Interface (MBD/API) by sending requests by submitting Health Insurance Claim Number (HICN)/Medicare Beneficiary Identifier (MBI) and date of service.

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
Medical Records Number
Medical Notes
Other: detailed and summary beneficiary prescription drug claim data, health insurance claim number (HICN)/Medicare Beneficiary Identifier (MBI), card holder identification number, date of service, gender, date of birth, provider characteristics, prescriber identification number, assigned provider number (facility, referring/servicing physician), national drug codes, beneficiary, plan, and supplemental payment amounts. System user credentials: user ID and password.

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

Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors
Patients

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The primary purpose of this system is to maintain/store and process information on all Medicare covered, and as many non-covered drug events as possible, for people with Medicare who have enrolled into a Medicare Part D plan. In order to access PRS, system users such as CMS employees and CMS direct 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.

This system is mandated under provisions of the Medicare Prescription Drug, Improvement, and Modernization Act, amending the Social Security Act by adding Part D under Title XVIII (§§ 1860D–

15(c)(1)(C) and (d)(2)), as described in Title 42, Code of Federal Regulations (CFR) 423.301 et seq. as well as1860D–12(b)(3)(D) and 1106 of the Act, as described in 42 CFR 423.505(b)(8), (f), (l), and (m).

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)

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within the OPDIV

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

Data used in the Drug Data Processing System has already been collected and validated from other CMS systems and are covered under individual Privacy Impact Assessments. Therefore, no OMB information collection approval number is required. The information collected in person online is system user credentials for CMS employees and CMS direct contractor support personnel.

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.

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.

DDPS is a batch processing system. There is no process in place by DDPS to notify individuals that their personal information will be collected because it is not collected by DDPS. 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. CMS Enterprise User Administration (EUA) and Amazon Web Services (AWS) Identity Access Management (IAM), which maintains user credentials for CMS employees and CMS direct contractors, notifies CMS and direct contractor staff via the application for Access to CMS Computer System and AWS of collection of PII when requesting a CMS or AWS IAM user ID.

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.

Although voluntary, individuals must provide their information in order to receive Medicare Part D. Part D Sponsors and Providers are required to have a disclaimer agreement with the beneficiary allowing them to collect required information in support of Medicare Part D. Data processed by DDPS is received from other CMS systems and NCPDP that has already been collected from plan sponsors and drug providers. This data does not involve direct collection from the beneficiary; therefore, DDPS does not maintain nor support a method for users to opt out of data processed by DDPS. In order to obtain a CMS or AWS user ID, CMS employees and direct contractors provide their PII to CMS EUA. CMS employees and direct contractors may opt out of providing their PII to CMS EUA or AWS IAM, in effect not obtaining a CMS or AWS user ID in support of their job

function.

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

DDPS receives PII information from the source system Prescription Drug Front-End System (PDFS). PDFS provides Prescription Drug Events (PDEs) records of beneficiaries covered under the Part D benefit. Therefore, DDPS does not directly communicate, nor notify individuals of system changes. The process to notify and obtain consent from the individuals whose PII is used in the system when major changes occur is through the Privacy Act System of Records Notice (SORN) and the Medicare & You handbook. The handbook is used to annually notify individuals of their right to ask Medicare to limit how their PII is used to run the Medicare program. The SORN is used to notify the public of what information is being used, for what purpose and with whom it will be shared or disclosed. If changes to the system occur, a revision will be made to the SORN and published to the Federal Register for public comment for a 60 day period. CMS staff and direct contractors will be notified via EUA notifications, if there is a change to a staff user profile affecting system access.

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 DDPS does not collect the data it processes, it does not maintain a method to resolve individual concerns. However, participants in the Part D Drug program may complain to their Plan sponsors to whom they provided their information. Plan sponsors will report the issue to the proper programs and take appropriate action. Individuals are also notified annually in the Medicare & You handbook of their right to complain about any alleged violation of their privacy rights and provides step by step instructions to follow in the event of a privacy concern. CMS and direct contractor staff may contact the CMS IT Service Desk to report any potential concern about their CMS EUA user credentials which are used to support the DDPS 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.

Data validation is conducted prior to DDPS processing; therefore, a review of data integrity is not performed by DDPS. DDPS relies on other CMS systems to perform data validation and to ensure PII is timely, accurate, and relevant before the files make it to DDPS for processing. DDPS does perform file integrity checks each time flat files are received from the other CMS systems; these checks ensure that the data integrity performed by the other CMS systems remains accurate and relevant for DDPS processing. CMS employees and direct contractors ensure DDPS availability and the PII within the system. DDPS also participates in annual security audits, which test the administrative and technical safeguards configured in DDPS to continue rigorous protection of the data confidentiality, integrity, and availability. As CMS EUA and AWS IAM maintains job codes for DDPS to support role-based access to CMS’s computer systems, DDPS performs quarterly and semi-annual account reviews, to ensure CMS employees and contractors maintain appropriate system access.

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.

CMS employees and direct contractors follow the CMS EUA and IAM guidelines and procedures to request access to the system. The guidelines include conducting a background check (conducted by

CMS); identifying required job codes for system access; and multiple levels of review and approval by the requesting user's manager, and CMS stakeholders before access is granted. After adhering to the CMS EUA and IAM guidelines and multiple levels of approval, appropriate role based access is granted by CMS EUA and AWS IAM system administrators. Approved users are assigned relevant 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.

Access is always based on least privilege and is explicitly denied unless otherwise granted. 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.

CMS 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, general security awareness, notations of conflict of interest, and import/export restrictions. A separate training for Records Management is also completed annually.
Personnel with significant security roles take role-based trainings in addition to the CMS Security Awareness and Records Management training. This additional training is also conducted annually, and is tailored to an individual's role within the program and varies depending on the desired role.

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.

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

There is no DDPS specific user training that is above and beyond the general CMS Information System Security and Privacy Awareness (ISSPA) 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.

Outputs of the DDPS, which provide summary data of all annual prescription approvals, are temporary and cut off annually; the outputs are then deleted and destroyed 20 years after cutoff. (Disposition Authority: N1-440-09-4, Item 1d). The records disposition is permanent and to be cut off annually. Pre-accession files to the National Archives are 5 years after cutoff. DDPS will legally transfer individual files in an acceptable format (following current CFR guidelines) to the National Archives annually, 20 years after cutoff and will include an electronic copy of the system documentation (i.e., code books, record layout, user guides and any other technical specifications) with the transfer. (Disposition Authority: pending NARA approval).

Per the Office of Strategic Operations & Regulatory Affairs (OSORA) standards, DDPS also retains the following data criteria in addition to the above NARA disposition authority: Financial Records, Beneficiary Records, Compliance and Integrity. Financial Records retention states, "Destroy no sooner than 7 year(s) after cutoff but longer retention is authorized." Beneficiary Records retention

states, "Destroy no sooner than 10 year(s) after cutoff but longer retention is authorized." Compliance and Integrity retention period states, "Destroy no sooner than 7 year(s) after cutoff but longer retention is authorized." DDPS is compliant with all the record retention requirements derived from OSORA, and documented in NARA per DDPS retaining system data indefinitely.

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

Access to the database where PII is stored is not available to anyone outside the CMS Infrastructure support team. Administrative security controls in place consist of a quarterly and semiannual account reviews conducted by EUA with input from DDPS. Technical security requirements include, but are not limited to: unique user IDs, passwords that must be changed every 60 days for CMS employees and contractors; 60 days for system/process accounts unless otherwise documented in the System Security Plan SSP, access based on least privilege, and auditing procedures. Records are housed in both active and archival files in an encrypted format to protect data confidentiality and integrity. Role Based Access is also employed to limit access to PII based on role function and least privileges. For phycial controls, this is inherited by AWS. All policies relating to the information security of DDPS are addressed in the CMS organizational policies and procedures, including the CMS Policy for Information Security Program and CMS Acceptable Risk Safeguards (ARS).