US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/28/2025

OPDIV:

CMS

Name:

Part D Transaction Facilitator

PIA Unique Identifier:

P-5669962-082309

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.

Not applicable.

Describe the purpose of the system.

The purpose of the Medicare Part D Transaction Facilitator (PDTransFac) system is to meet the statutory requirement outlined in the Medicare prescription drug benefit, authorized in the Medicare Prescription Drug, Improvement, and Modernization Act (MMA) and ensures routing of claim information so that Medicare Part D Plans can accurately calculate True Out of Pocket (TrOOP) expenditures and non-Medicare Payer payments.

Non-Medicare payments do not count toward the Medicare Beneficiary’s TrOOP expenditures. Therefore, the PDTransFac system is used to determine, capture, and route claims data at the beginning of the process (when a Medicare Beneficiary fills the prescription) which minimizes errors and adjustments.

NDCHealth Corporation DBA RelayHealth, as the PDTransFac Contractor, supports the TrOOP Facilitation Process by:

Providing Medicare Part A, B, or D Beneficiary Plan eligibility information to the pharmacy in real-time using the HIPAA mandated National Council for Prescription Drug Programs (NCPDP) Eligibility Inquiry (E1) transaction standard.

Capturing supplemental claim data for routing to the appropriate Medicare Part D Plan in real-time using the HIPAA mandated NCPDP Information Reporting (Nx) transaction standard.

Determining when a Medicare Beneficiary has been enrolled into a new plan and requests the TrOOP balance information from the previous plan(s) and provides this data to the new plan using the NCPDP Financial Information Reporting (FIR) transaction standard.

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

The Medicare Part D Transaction Facilitator (PDTransFac) system receives Medicare Beneficiary enrollment data files that include the following data elements: Medicare Beneficiary ID (MBI), Social Security Number (SSN), date of birth, gender, name, mailing address, entitlement status and coverage dates in Medicare Part A, Part B and Part D, and plan coverage information (including plan ID number and supplemental plan information). The Medicare Beneficiary enrollment data file is received daily via a secure electronic file transfer from the Medicare Beneficiary Database (MBD), without direct user input.

PDTransFac passes or transfers Medicare beneficiary enrollment information in the form of

Financial Information Reporting (FIR) transactions
Eligibility Inquiry (E1) transactions
Information Reporting (Nx) real-time standard transactions

There are no external users of the system; PII is used only in HIPAA named NCPDP transactions. External users cannot access the system.

Part D sponsors receive mandatory compliance reporting from RelayHealth for FIR and Nx rejections via CMS required secure emails.

PDTransFac passes or transfers Medicare beneficiary enrollment information in the form of National Council for Prescription Drug Programs (NCPDP) HIPAA standard financial information reporting (FIR) real-time transactions. The enrollment information is provided to pharmacies via NCPDP HIPAA standard eligibility inquiries (E1) transactions and NCPDP HIPAA standard information reporting (Nx) real-time standard transactions to Part D Sponsors. There are no external users of the system, just transactions. Part D sponsors receive mandatory compliance reporting for FIR and Nx rejections via CMS required secure file transfer protocol (SFTP). External users cannot access the system.

Access to the PDTransFac Systems is only granted to RHP Support Administrators. All access to the PDTransFac Environment is conducted through the PDTransFac Virtual Private Network (VPN) which ensures communication integrity. The VPN is used to access the PDTransFac system and utilizes a native access control software solution. The VPN collects administrator usernames, password, and email information.

RHP maintains PII internally via a limited group of credentialed users with multi-factor authentication. Medicare beneficiaries' PII in the form enrollment information only is maintained and transferred to

Medicare Part D plans as CMS direct contractors. Enrollment information is shared with Pharmacies who are under contract with Medicare Part D plans via NCPDP HIPAA standard real-time transactions.

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

The purpose of the Medicare Part D Transaction Facilitator (PDTransFac) system is to meet the statutory requirement outlined in the Medicare prescription drug benefit, authorized in the Medicare Prescription Drug, Improvement, and Modernization Act (MMA) and ensures routing of claim information so that Part D Plans can accurately calculate True Out of Pocket (TrOOP) expenditures and non-Medicare Payer payments. Personally Identifiable Information (PII) is provided to the contractor and is used to create and respond to transactions required for Part D coordination of benefits. The data is maintained for 10 years. All information is passed via HIPAA mandated NCPDP transaction standards.

Relay Health Plan (RHP) maintains Personally Identifiable Information (PII) that is accessible internally via a limited group of credentialed users with multi-factor authentication.

Enrollment information is shared for processing of:

Financial Information Reporting (FIR) transactions between Part D plans

Eligibility Inquiry (E1) transactions with contracted pharmacies
Information Reporting (Nx) real-time standard transactions sent to Part D plans

The system also checks user credentials- username, passwords, and emails for users who access the system.

Plans can accurately calculate True Out of Pocket (TrOOP) expenditures and non-Medicare Payer payments. Personally Identifiable Information (PII) is provided to the contractor and is used to create and respond to transactions required for Part D coordination of benefits. The data is maintained for 10 years. All information is passed via National Council for Prescription Drug Programs (NCPDP) Health Insurance Portability Act (HIPAA) transactions only.

Relay Health Plan (RHP) maintains Personally Identifiable Information (PII)is retrieved by internally via a limited group of credentialed users with multi-factor authentication. Medicare beneficiaries' PII in the form enrollment information only is maintained and transferred to Medicare Part D plans as CMS direct contractors. Enrollment information is shared with Pharmacies who are under contract with Medicare Part D plans via NCPDP HIPAA standard real-time transactions. PII is retrieved based on the beneficiary's last name, date of birth, Medicare Beneficiary ID and home address, HICN, MBI, Plan coverage information including plan ID number. The system also checks user credentials- username, passwords, and emails for users who access the system.

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
Other: MBI, Plan coverage information including plan ID number. User credentials- username, passwords, and emails.

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

Medicare Beneficiaries

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

Personally Identifiable Information (PII) is used to: respond to pharmacy transactions to ascertain enrollment in Medicare and to create transactions for transfer of Part D drug spend balances and records of supplemental coverage.

User credentials are used for authentication into the system to support operations and maintenance.

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

Not applicable.

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

The Medicare Modernization Act (MMA), Section 1860D-23(a)(4) of the Social Security Act.

The statutory authority for this system is given under Part D of Title XVIII of the Social Security Act, as amended by the Medicare Prescription Drug, Improvement, and Modernization Act of 2003.

Medicare, Medicaid, and State Child Health Insurance Program (SCHIP) Extension Act of 2007 (Section 111 of P.L. 110-173), E.O. 9397.

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.

09-07-0536, Medicare Beneficiary Database (MBD)

09-70-0557, True Out-of-Pocket (TrOOP) Expenditures System

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

N/A

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.

The Information Sharing Agreement (ISA) is between Relay Health Plan (RHP) and the Centers for Medicare & Medicaid Services (CMS). Data Use Agreement-21471, Contract-HHSM-500-2011-0006C (between CMS and RHP) has specific statements of work related to information sharing or disclosure necessary to conduct coordination of benefit activities required under regulation and the CMS Part D manual chapter 14.

Describe the procedures for accounting for disclosures.

Disclosure information is maintained as part of the transaction process. Each National Council for Prescription Drug Programs (NCPDP) HIPAA standard financial information reporting (FIR) real-time transaction and NCPDP HIPAA standard eligibility inquiries (E1) transaction is maintained for 10 years by Relay HealthPlan (RHP). Each transaction is equivalent to a disclosure. Data disclosures are accounted for by approval of DUAs which track who data is disclosed with, for what purpose, and what date.

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

There is no process to notify individuals that their personal information is collected because the Medicare Part D Transaction Facilitator (PDTransFac) system does not collect Personally Identifiable Information (PII) directly. Data provided to RHP is from another CMS system, Medicare Beneficiary Database (MBD), which has its own PIA.

Relay Health Plan (RHP) maintains PII internally via a limited group of credentialed users with multi-factor authentication. Medicare beneficiaries' PII in the form of enrollment information only is maintained and transferred to Medicare Part D plans as CMS direct contractors. Enrollment information is shared with Pharmacies who are under contract with Medicare Part D plans via NCPDP HIPAA standard real-time transactions.

When an individual enrolls in Medicare Part D their PII is recorded in MBD so that CMS can administer the benefit.

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.

None – Beneficiaries must submit this information to be enrolled in the Part D benefit. Sharing of this information with pharmacies is mandatory for Part D benefit administration to accurately track beneficiary costs and copayments.

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

There is not a process to obtain consent from individuals as maintenance of their data required to administer the benefit. The notice would not be needed because the data uses are only those required by HHS law. Neither CMS nor the contractor can change the system purposes.

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.

Beneficiaries would contact medicare.gov or 1-800-Medicare and report the complaint. If it is a privacy issue it will get referred to the CMS Privacy officer who would send the complaint to the system COR for investigation. The COR would obtain details of the beneficiary complaint and work with the contractor to resolve. We have not had such a complaint since the process was implemented in 2006.

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

Relay Health Plan (RHP) has implemented a policy that limits the use and disclosure of Personally

Identifiable Information (PII) to the minimum necessary to accomplish the purposes for which PII is needed. RHP conducts an annual Part D Transaction Facilitator (PDTransFac) System Protected Health Information (PHI) and PII Holdings review which involves an examination of data received by, stored in, or generated by the system to ensure data integrity. This review involves discussion and decisions regarding appropriateness of storage of the data considering data use and contractual obligations to maintain system integrity. The data must be available to pharmacies who need it when the patient presents to them for a prescription. Pharmacy responses are returned as required by the national standards organization, (NCPDP). These standards are real-time transactions, and the infrastructure employed (high availability) supports the real time mandate. As for relevancy, the NCPDP standard is used in transactions to ensure that the system supplies relevant (standard) use cases.

RHP maintains Personally Identifiable Information (PII) internally via a limited group of credentialed users with multi-factor authentication. Medicare beneficiaries' PII in the form enrollment information only is maintained and transferred to Medicare Part D plans as CMS direct contractors. Enrollment information is shared with Pharmacies who are under contract with Medicare Part D plans via the National Council of Prescription Drug Programs (NCPDP) Health Insurance Portability Accountability Act (HIPAA) standard real-time transactions.

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.

The contractor has procedures in place pursuant to which the contractor determines what roles have job functions that require access to PII. The level of access or privilege of a user or administrative role is based on the minimal amount of information necessary to perform the authorized job roles by the individual. Individuals in authorized roles are required to complete training prior to accessing 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 Medicare Part D Transaction Facilitator (PDTransFac) Systems is only granted to RelayHealth (RHP) Support Users and Administrators. Access to the PDTransFac Environment is granted after successful authentication with a virtual private network (VPN) that utilizes native access control software to validate the identity of the user. Using restrictive least privilege principles enforced by procedures and tools, access to the RHP information system is granted based on: (a) a valid need-to-know that is determined by assigned duties and satisfying all personnel security criteria, and (b) intended system usage. Proper identification and approval are required for requests to establish information system accounts. Each user or process is assigned the most restrictive set of privileges needed for the performance of authorized tasks.

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.

The contractor's parent organization, McKesson, organizational Security awareness training occurs for all employees at the point of new hire and with annual refresher training. This training is specific to the roles of the individuals and there is training associated with the CMS contracts specifically. The contractor is required to complete annual CMS Security Awareness and Privacy training.

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

N/A

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 the data resides on the server database that is still in use and the data needs to be purged, the information which is encrypted is deleted off the database. When servers are decommissioned or if data is stored on tapes, there is an on-site shredding service that provides a certificate of destruction for tapes and server hard drives that are shredded.

According to the Medicare Advantage and Rx Plan Operations (MARPO) disposition authority N1-440-09-04, Item 1b1, beneficiary enrollment records must be cutoff annually and deleted/destroyed 6 years and 3 months after cutoff.

According to the Medicare Advantage and Rx Plan Operations (MARPO) disposition authority N1-440-09-04, 1b3, prescription drug records must be cutoff annually and deleted/destroyed 10 years after cutoff.

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

Administrative

Relay Health Plan (RHP) has policies and procedures designed to manage development, implementation, and maintenance of the security measures designed to protect Protected Health Information (PHI) and the conduct of those with access to the PHI. These information security policies provide an essential and coherent framework for protection information resources.

Technical

RHP Systems reside within multiple levels of boundary security controls. The network boundaries around RHP Systems are protected by firewalls configured to meet control requirements at each egress point in addition to an intrusion detection system (IDS). The RHP WAN is mainly comprised of private point-to-point connections. Two-factor authentication is required to remotely access RHP Systems.

Physical

There are diverse protect-in-depth physical controls in place to validate the identity of everyone which include perimeter and access controls.

Identify the publicly-available URL:

https://medifacd.mckesson.com/

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?

null