US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/21/2017

OPDIV:

CMS

Name:

Part D Transaction Facilitator

PIA Unique Identifier:

P-5669962-082309

The subject of this PIA is which of the following?

Minor Application (stand-alone)

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.

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 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 DBA RelayHealth (RHP), 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, and capturing the claims data that is routed to the appropriate Non-Medicare Payer and also to the Medicare Part D Plan for reporting to CMS. Lastly, the PDTransFac determines when a Medicare Beneficiary has been enrolled into a new plan and request the TrOOP balance information from the previous plan(s) and provides this data to the new plan.

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 which contain the following data elements: social security numbers, dates of birth, first and last name, Health Insurance Claim Number (HICN), and plan coverage information (including plan ID number). The file is received daily via a secure electronic file transfer without direct user input from the Medicare Beneficiary Database (MBD). 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 VPN. The VPN 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.

In order to meet statutory requirements, this information is necessary to conduct transactions. 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) 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.

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

HICN, Plan coverage information including plan ID number. User credentials- user name,

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

Employees

Patients

Yes, 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 in order to support operations and maintenance.

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

Not applicable.

Describe the function of the SSN.

Pharmacies may submit the SSN number (or Health Insurance Claim Number) and other verifying information to verify eligibility for pharmacy claims submission.

Cite the legal authority to use the SSN.

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

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.

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.

Online

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

We do not directly collect data outside of user credentials.

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

State or Local Agencies

State Pharmaceutical Programs (SPAPs) and AIDS Drugs Assistance Programs (ADAPs), and other local agencies may need assistance determining why their coordination of benefit (COB) information is not being accepted by Medicare Part D plans. In this instance, the agency provides Personally Identifiable Information (PII) from within their system to compare to CMS data within the Relay Health Plan (RHP) system.

Private Sector

Pharmacies submit Personally Identifiable Information (PII) via the National Council of Prescription Drug Programs(NCPDP) eligibility transaction standard and received Medicare Part D plan enrollment in return. Medicare Part D sponsors receive NCPDP Financial Information Reporting (FIR) and Information Reporting (Nx) transactions in order to meet coordination of benefits (COB) requirements.

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.

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 –Relay Health Plan (RHP) doesn't collect this information from beneficiaries directly. Data provided to RHP is from another government system, MBD, which has it's own PIA. The MBD is where Beneficiaries must submit this information in order 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.

RHP maintains Personally Identifiable Information (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 the National Council of Prescription Drug Programs (NCPDP) Health Insurance Portability Accountability Act (HIPAA) standard real-time transactions.

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

Relath Health Plan (RHP) System receives all information from the MBD which has it's own PIA.and that system is responsible for the process to notify and obtain consent from the individuals whose Personally Identifiable Information (PII) is in the system.

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.

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. We have not had such a complaint since the process was implemented in 2006.

Relay Health Plan (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.

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. This review involves discussion and decisions regarding appropriateness of storage of the data considering data use and contractual obligations.

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.

Users:

A limited group of Relay HealthPlan (RHP) users and administrators will have access to and maintain personally identifiable information (PII), internally, via multi-factor authentication. Level of access is determined by the role of the user, which is limited to only the users who support the help desk and administrators of the system. Medicare beneficiaries' PII (in the form enrollment information only) is maintained and transferred to Medicare Part D plans as CMS 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.

Administrators:

A limited group of Relay Health Plan (RHP) users and administrators will have access to and maintain personally identifiable information (PII), internally, via multi-factor authentication. Level of access is determined by the role of the user, which is limited to only the users who support the help desk and administrators of the system. 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.

Contractors:

A limited group of Relay HealthPlan (RHP) users and administrators, direct contractors, will have access to and maintain personally identifiable information (PII), internally, via multi-factor authentication. Level of access is determined by the role of the user, which is limited to only the users who support the help desk and administrators of the system. Medicare beneficiaries' PII (in the form enrollment information only) is maintained and transferred to Medicare Part D plans as CMS 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.

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

Procedures have been developed to guide the implementation and management of logical access controls. The logical access controls and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, and are periodically reviewed, and, if necessary, updated.

Microsoft Active Directory (AD) servers reside on the Relay Health Plan (RHP) network and are utilized to provide directory and access control services to all Windows systems. Through the use of Microsoft Active Directory, comprehensive account management mechanisms have been established to: identify account types (i.e., Individual, group, and system), establish conditions for group membership, and assign associated authorizations.

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 Relay Health Plan (RHP) Support Administrators. All access to the PDTransFac Environment is conducted through the PDTransFac VPN. The VPN utilizes a native access control software solution. The VPN collects administrator usernames, password, and email information.

Through the use of Microsoft Active Directory, 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 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.

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 security awareness course includes the following topics: the importance of electronic security awareness, everyone is a security target, malicious code (viruses, Trojan horses, worms), Personally Identifiable Information (PII) and Protected Health Information (PHI) training (including minimal information necessary for performing job functions), unauthorized software, passwords, file sharing, internet security, email security, physical/Office security, and security awareness quiz.. The Centers for Medicare & Medicaid Services (CMS) employees do not have access to the Relay Health Plan (RHP) system.

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

None.

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

Physical access to the building containing RHP system components is controlled with locked doors, guards at reception desks, and key card access is required to pass the reception desk. Access to the building parking lot is restricted by a guard station at the parking lot entrance and entrance gates. Visitors check in at the guard station, directed to a restricted visitor parking lot, and are required to check in at the reception desk. A key card is required to pass by the entrance gates and enter the building parking lot.