US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/29/2024

OPDIV:

CMS

Name:

Medicare Part D Coverage Gap Discount Program Direct Payment Process Portal

PIA Unique Identifier:

P-3045406-382417

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.

New Medicare Beneficiary Identifier (MBI) replaced social security number (SSN)-based Health Insurance Claim Number (HICN)

Addition of multifactor authentication (MFA) token to access the Medicare Part D Coverage Gap Discount Program Direct Payment Process Portal (CGDP DPP Portal). Requires validated e-mail address for delivery.

Removal of ProfitStars Enterprise Payment Solutions (EPS). Replaced with Direct to PNC Bank Automated Clearinghouse (ACH) processing.

Describe the purpose of the system.

The Affordable Care Act (ACA) of 2010 initiated the need for a Coverage Gap Discount Program (CGDP) Third Party Administrator (TPA) contract, per Section 3301 (PL 111-148) as amended

through May 1, 2010, to facilitate payments between Pharmaceutical Manufacturers and Part D Health Plan Sponsors.

The CGDP TPA facilitates payments between drug manufacturers and Healthcare insurers/plan sponsors Invoice and other reports are received from the CMS' Division of Durable Medical Equipment, Prosthetics, Orthotics and Supplies (DMEPOS) Policy (DDP) Drug Data Processing System (DDPS) contractor, General Dynamics Information Technology (GDIT). The data and reports are loaded into Palmetto's CGDP web-based portal, the CGDP DPP Portal, for report download and retrieval and payment initiation. Any payments that are initiated have transactions that are sent as an Automated Clearinghouse (ACH) transaction to PNC Bank for processing and transmitting ACH funds to and from the respective entity's banks.

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

The system stores report and invoicing information received from the DDPS contractor, GDIT. DDPS is another CMS system that has its own PIA.

Report information consists of CGDP-qualified prescription drug event (PDE) data in detail, summary formats, and payment invoice formats.

The PDE data consists of drug attributes such as the ingredient price of the drug, whether the drug is brand or generic, the patient pay amount, the covered plan paid amount, the drug name, the service provider ID, and the Coverage Gap Discount amount.

Format layouts for the CGDP-qualified PDE data provided to manufacturers and sponsors are located on the publicly accessible TPA website, www.tpadministrator.com.

Format layouts provide descriptions of each field included in the reports. The Invoice Report and Data Report provide the file layout format of the Manufacturer Invoice and Detail (Data) reports.

The Contract Data and Contract Summary Reports provide the file layout format for the Sponsor Invoice and Detail (Data) reports.

CGDP-qualified PDE invoice data is included in dispute files submitted by manufacturers, and dispute resolution/disposition reports that note the upheld/denied status of disputed CGDP-qualified PDE invoice data.

Dispute disposition files no longer contain Health Insurance Claim Number (HICN) information. It has been updated with the Medicare Beneficiary Identifier (MBI), which replaced social security number (SSN)-based Health Insurance Claim Numbers (HICN), to allow a health plan sponsor to track and review disputed PDE files for subsequent adjustments.

Format layouts for the dispute disposition file are located on the publicly accessible TPA website, www.tpadministrator.com.

Format layouts provide descriptions of each field included in the reports. The CGDP Contract Dispute File (2/4/ 2018) provides the file layout format for the dispute disposition file.

The CGDP DPP Portal also stores bank account information (routing and account numbers) for CGDP Program participants (drug manufacturers and health plan sponsors) receiving payment as well as a token representation of the bank account information used for sending payments. It also stores usernames but not passwords.

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

Quarterly invoice and report data are received from the DDPS contractor GDIT, which is transmitted via CMSNet. The data files are loaded into the CGDP DPP Portal so that invoice data can be reformatted into a browser-based user interface and individual supporting reports are available for download.

Access to the portal is limited to drug manufacturers and health plan sponsors authorized to do so based upon their Health Plan Management System (HPMS) role and contact information. The TPA utilizes HPMS to verify contractually obligated CGDP manufacturer and sponsor entity authorized associates prior to providing access to the CGDP DPP Portal.

The HPMS fields of TPA Liaison and Coverage Gap Discount Program (CGDP) Payment Initiator must be populated with authorized manufacturer or sponsor personnel, who will then be provided with access to the CGDP DPP Portal by the TPA.

The authorized user login is based upon their CGDP contract identifier derived username and their user defined password, which is stored on a directory server, separate from the application server used by the CGDP DPP Portal application. The PII element, UserName, determines the type of data that is available for access by a Manufacturer or Sponsor (view and pay vs. view only) in the CGDP DPP Portal application. Authorized users can retrieve stored records 365 days a year if the UserName is in an active status. In addition to the username and password, authorized users require a multifactor authentication (MFA) token sent to an authorized user's validated email (PII). User's email addresses must be verified to securely receive MFA tokens as part of the CGDP Portal login procedure. Once a user validates their email address, an MFA token is generated to complete the login process.

This MFA, once generated, is valid for only 15 minutes.

Once logged in, users can download any reports available to them and initiate payments for any or all line items presented in the current invoice, with the correct role assignment. The amounts and payee for each line item is pre-determined by the invoice data received from the DDPS contractor. The options the user has is to make the payment for the current date, schedule the payment for a future date, or to defer the payment because it is too small for their bank to issue an ACH transaction.

Each payment initiation transaction is sent as an ACH transaction to the bank of record (currently PNC Bank) who receives and processes the ACH payments to the respective payee banks. The settlement status of those transactions is retrieved from PNC Bank to update the CGDP DPP Portal.

Bank accounts associated with each sender and receiver of payments is established by a separate maintenance process. Bank account change forms are available on the CGDP DPP Portal. The bank account information (bank accounts and routing numbers) for each receiver of payments is stored, encrypted, and cross-referenced as a token identifier, which is stored on the CGDP DPP Portal.

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

Yes

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

E-Mail Address
Financial Accounts Info
Other: Service provider ID, Medicare Beneficiary Identifier (MBI), bank account information (token identifier, routing, and account numbers), Username and passwords

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

Employees
Patients
Drug Manufacturers and Health Plan Sponsors

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The dispute disposition report contains the MBI. The original HICN data is no longer passed directly from the DDPS contractor, GDIT, through the CGDP DPP Portal to the sponsor entity with authorized access to the CGDP DPP Portal.

Reports are partitioned based on the contractual agreements in the CMS' HPMS. The system does not use the MBI data at all.

The username is used in conjunction with the directory server to authenticate the users. Once authenticated, it is also used to determine the role of the user in the CGDP DPP Portal application.

E Mail is utilized to provide an MFA token to the authorized user to complete the login process for accessing the CGDP Portal.

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.

The Privacy Act permits the disclosure of information without an individual's consent if the information is to be used for a purpose that is compatible with the purpose for which the information was collected. Any such disclosure of data is known as a "routine use."

This system contains Protected Health Information as defined by HHS regulation "Standards for Privacy of Individually Identifiable Health Information" (45 CFR Parts 160 and 164,

65 FR 82462 (Dec. 28, 00), as amended by 66

FR12434 (Feb. 26, 01)). Disclosures of Protected Health Information authorized by these routine uses may only be made if, and as, permitted or required by the "Standards for Privacy of Individually Identifiable Health Information."

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

Email

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

Identity Verification Services

Not Applicable

Not applicable for collection of user credentials to log into the system.

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 TPA Contract Statement of Work calls for the reports to be distributed to Drug Manufacturers and Sponsors.

Describe the procedures for accounting for disclosures.

The process of collecting the MBI is not managed by this system or the TPA contract.

The TPA discloses PII data received from information collected and transmitted from the CMS DDPS contractor, GDIT, to the specific sponsor that will utilize the data to perform adjustments on CGDP-qualified PDE claims. Per the DDPS SORN # 09-70-0553, “These routine uses specify circumstances, in addition to those provided by statute in the Privacy Act of 1974, under which CMS may use and disclose information from the DDPS without consent of the individual to whom such information pertains."

TPA "shares" by allowing a designated Drug Manufacturer or Sponsor to Download reports, which contain this data. Report download activity is logged which accounts for the tracking of the disclosure of PII and provides the ability to perform periodic log reviews, as necessary.

Manufacturers and sponsors have access to the CGDP DPP Portal via authorized access. Authorized access is based on information listed in HPMS for the CGDP. The HPMS TPA Liaison and CGDP Payment Initiator fields provide the entity with the ability to designate authorized individuals for the access to the CGDP DPP Portal.

One set of credentials is issued per TPA Liaison and/or CGDP Payment Initiator. Users are discouraged from sharing access.

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 process of collecting the MBI is not managed by this system or the TPA contract. The TPA is not the source of the information, but individuals can refer to the source of the data for notification.

Collection of credentials: the HPMS memo dated March 20, 2015, titled “Updates on the new Medicare Part D Coverage Gap Discount Program Direct Payment Process” states that “Additional instructions on the enrollment steps will be supplied by the Third-Party Administrator (TPA) at a later time.”

To meet this enrollment step listed in the HPMS memo, the TPA notifies drug manufacturers and health plan sponsors during the onboarding process, via Welcome letter, that credentials will be provided for access to the CGDP DPP Portal once the Welcome packet data is received and processed. As stated in the Welcome letter for manufacturers and sponsors “Login credentials will only be provided to the TPA Liaison contact. Login credentials will not be provided if the TPA Liaison Contact differs from the TPA Liaison contact listed in HPMS.”

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.

The process of collecting the MBI is not managed by this system or the TPA contract.

The TPA is not the source of the data, therefore cannot provide an opt-out function. Individuals must contact the maintainer of the source data to submit an opt-out request.

Regarding the collection of credentials, options to opt-out are not available. Collection of PII (credentials) is required to allow authorized access to the CGDP DPP Portal.

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

The process of collecting the MBI is not managed by this system or the TPA contract.

The TPA is not the source of the data.

Manufacturers and sponsors have access to the CGDP DPP Portal via authorized access. Authorized access is based on information listed in HPMS for the CGDP. The HPMS TPA Liaison and CGDP Payment Initiator fields provide the entity with the ability to designate authorized individuals for the access to the CGDP DPP Portal.

One set of credentials is issued per TPA Liaison and/or CGDP Payment Initiator.

The TPA notifies drug manufacturers and health plan sponsors during the onboarding process, via Welcome letter, that credentials will be provided for access to the CGDP DPP Portal once the Welcome packet data is received and processed. As stated in the Welcome letter for manufacturers and sponsors “Login credentials will only be provided to the TPA Liaison contact. Login credentials will not be provided if the TPA Liaison Contact differs from the TPA Liaison contact listed in HPMS.”

The TPA provides notification to CGDP drug manufactures and health plan sponsors of major changes via communications approved by CMS, using listserv, outreach, and HPMS memo communication methods.

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.

The systems involved in this contract are not the primary source of obtaining consent from individuals whose PII is in the system. As a result, other organizations are responsible for notifying individuals of their right to file a complaint if they believe their privacy rights have been violated.

Regarding the recourse for inappropriately obtained, used, or disclosed credentials, drug

manufacturers and health plan sponsors may contact the TPA, via email at TPAOperations@tpadministrator.com or toll free at 1-877-534-2772 option 1, to request review of the possible credential PII disclosure in question. TPA will disable the account and review system logs to determine activity associated with the PII disclosure.

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

The MBI passes directly from the DDPS contractor, GDIT, through the CGDP DPP Portal, and transmitted as is to the designated end users.

Data integrity processes are not applicable for the MBI, because the information is not collected by the TPA, and the data has no relevant use in the CGDP DPP Portal processes.

Regarding credential reviews, the TPA performs comparisons of the data listed in HPMS to the information issued to manufacturers and sponsors to validate that authorized users match the information listed in HPMS. If data does not match, the account is disabled.

Conditions that require TPA to compare data listed in HPMS:

password reset requests, accounts unlock requests, and any other access-associated activity questions received.

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 systems is given based on need to know and job responsibilities to process CGDP data using a user ID and role-based access. Access is obtained using a request form which must be approved by the designated approvers prior to access being granted.

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 systems is controlled using security software. The user is given the least amount of access required to perform their job duties and is explicitly denied access by the security software unless otherwise granted.

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 Palmetto GBA (direct) contractors and employees are required to take annual training regarding the security and privacy requirements for protecting PII. In addition, role-based training is provided to individuals with significant access or security responsibilities. This annual role-based training is required by the CMS Chief Information Officer Directive 12-03. All training is modeled on and is consistent with training offered by the Department of Health and Human Services and CMS.

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

In addition to the general security and privacy awareness training, users must sign rules of behavior. Also, throughout the year, users are provided with newsletters, list serve messages and security bulletins to provide ongoing awareness of their security and privacy responsibilities.

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 the National Archives and Records Administration (NARA) Records Control Schedule (RCS) Job Number N1-440-04-003, records are maintained in a secure storage area with identifiers. Records are closed at the end of the fiscal year, in which paid, and destroyed after 6 years and 3 months. All claims-related records are encompassed by the document preservation order and will be retained until notification is received from Department of Justice.

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

Access to the systems is given based on need to know and job responsibilities to process CGDP data. CM - Customer Support system maintainers use security software and procedural methods to provide “least privilege access” to grant or deny access to data based upon need to know. External audits also verify these controls are in place and functioning. Technical controls used include user identification, passwords, firewalls, virtual private networks, and intrusion detection systems. Physical controls used include guards, identification badges, key cards, cipher locks and closed-circuit televisions.

Identify the publicly-available URL:

https://apps.tpadministrator.com/tpacgdp/

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?

Yes

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

No