

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/21/2017

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?

New

Does the system have Security Authorization (SA)?

No

Indicate the following reason(s) for updating this PIA.**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. Invoices 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 to a third party payment processing service (ProfitStars Enterprise Payment Solutions (EPS)) for transmitting Automated Clearinghouse (ACH) transactions to the respective 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 publically 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 contain Health Insurance Claim Number (HICN) information 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 publically accessible TPA website, www.tpadministrator.com.

Format layouts provide descriptions of each field included in the reports. The Contract Dispute File (Effective February 8, 2015) 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 collects CGDP program participant usernames and passwords, but does not store passwords. CGDP also collects usernames of system backend support users.

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

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 HPMS has its own PIA.

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.

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. 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 later time, or to defer the payment because it is too small for their bank to issue an ACH transaction.

Each payment initiation transaction is sent to a third party payment processing service (ProfitStars) who sends the ACH transactions to the respective banks. The settlement status of those transactions is reported back from ProfitStars in order 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, on the CGDP Portal.

The bank account information for the sender of payments is stored on the 3rd party payment processor's system, rather than the Portal. It is 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.

Other - HICN, service provider ID, bank account information (token identifier, routing and account

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?

As a function of facilitating CGDP payments between pharmaceutical drug manufacturers and Part D health plan sponsors, the TPA provides reports to detail CGDP payment amounts due, facilitate the dispute of CGDP PDE data by manufacturers, and disseminate reports to detail the dispute resolution/disposition determination. The PII, HICN, is not used in the facilitation of payments between drug manufactures and Healthcare Insurers/plan Sponsors. The HICN is only present in dispute disposition reports received from the CMS contractor, GDIT, as part of routine use for fulfilling the TPA contract and providing dispute disposition reports to Health Insurer/plan sponsor to assist in proper adjustment of PDE claims included in the CGDP.

Reports are partitioned based on the contractual agreements in HPMS. The system does not use the HICN at all.

The username and password are used in conjunction with the directory server to authenticate the users.

Once authenticated, the username is also used to determine the role of the user in the CGDP DPP Portal application.

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.

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 as 1860D–12(b)(3) (D) and 1106 of the Act, as described in 42 CFR 423.505(b)(8), (f), (l), and (m).

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."

5 U.S.C. 301, Departmental Regulations

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.

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

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.

Private Sector

Health Care Insurers/Plan sponsors.

Dispute disposition files contain HICN information to allow a health plan sponsor to track and review disputed PDE files for subsequent adjustments.

Data is partitioned based on HPMS contractual agreements so that Drug Manufacturer or Sponsor specific data is only accessible by the contracted entity.

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 HICN 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 HICN is not managed by this system or the TPA contract. The TPA is not the source of the information, but individuals can refer back 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 HICN 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.

In regards to the collection of credentials, options to opt-out are not available. Collection of PII (credentials) is required in order 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 HICN 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.

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 manufacturers 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.

In regards to 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 HICN included in the Dispute Disposition reports forwarded to applicable sponsors is provided by the DDPS Contractor, GDIT, and is transmitted as is to the designated end users.

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

In regards to credential reviews, the TPA performs comparisons of the data listed in HPMS to the information issued to manufactures and sponsors to validate that authorized users match the information listed in HPMS. In the event that 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.

Administrators:

To perform tasks to maintain the system.

Developers:

Test new code and correct programming errors encountered in production.

Others:

Drug Manufacturers and Sponsor companies are involved in related Coverage Gap Discount claim activity.

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 NARA 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.tpadadministrator.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.

Session Cookies that do not collect PII.

Persistent Cookies that do not collect PII.

Does the website have any information or pages directed at children under 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