US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/28/2024

OPDIV:

CMS

Name:

Contractor Reporting of Operational and Workload Data 2.0

PIA Unique Identifier:

P-8791131-727831

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Initiation

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?

New

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

The Contractor Reporting of Operational and Workload Data system (CROWD) provides the Centers for Medicare and Medicaid Services (CMS) with the tool to monitor each Medicare Administrative Contractor's (MACs) performance in processing claims, as well as other activities required under contract.

CROWD provides the capability for the MACs to electronically enter workload data on a large variety of functional areas (as collected by the CMS Shared Systems). CROWD is a mechanism that provides CMS with a timely way to monitor each MACs performance in processing claims, and paying bills, processing appeals, handling beneficiary over payments, answering beneficiary and provider inquiries, fraud and
abuse, and Medicare Secondary Payer. CROWD contains workload reporting capabilities that allow the data collected to be used for estimating budgets, defining operating problems, comparing performance among contractors, and determining regional and national trends.

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

CROWD collects count of MAC workload activity that is collected by the CMS Shared Systems and/or collected by the MACs in-house systems and then submitted to CROWD by file upload. This data is maintained on direct on-line storage through the current Fiscal and Calendar years, and goes back historically for 10 years. The data collected and stored in CROWD is used to monitor the performance of the MACs, who process all the referenced activity under contract to CMS.

Types of activities counted and, in turn, submitted to CROWD as informational data includes number of claims receipts; number of claims processed; number of inquiries received; claims processing timeliness; Medicare Secondary Payments (MSP) savings; number of Remittance Advices sent; number of Redeterminations pending; number of Requests cleared; number of Claims affirmed; number of
Affirmations; and number of Administrative Law Judge (ALJ) decisions. As noted, CROWD only contains counts of activity. It does not collect, store or share any Beneficiary or Provider identifiers.

In order to be granted access to CROWD, the user must obtain a valid CMS-issued Enterprise Identity Management (EIDM) account,, which requires him/her to provide credentials (ie. Name, Email, Date of Birth, Phone Number and Mailing Address) to the external CMS IDM application, which manages all access requests to CROWD. Of these, only the User ID, Name and Phone Number Personally Identifiable Information (PII) identifiers are stored within CROWD's internal security module. The CROWD user base is comprised of CMS employees and CMS contractors.

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

The CROWD application maintains counts of contractor activity and provides CMS with a timely way to monitor each MACs performance. MAC workloads, submitted on a monthly, quarterly, or annual basis, are permanently maintained in the database. User credentials (Name, Email, Date of Birth, Phone Number and Mailing Address) are collected by an external application (CMS Identity Management (IDM) Portal) in order to establish an initial EIDM account for the user to gain access to CROWD. Of these, only the User ID, Name and Phone Number are stored within CROWD's internal security module in order for the user to be able to perform his or her appropriate job duties.

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
E-Mail Address
Phone Numbers

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

Employees
Vendor/Suppliers/Contractors
CMS Contractors and CMS employees only

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

To register and create a CMS Enterprise Identity Management (EIDM) user account to access the application.

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

The user's EIDM User ID allows the System Administrator to identify the user who entered the counts informational data in order to research and resolve issues reported with the application.

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

5 USC 301, Departmental Regulations

Are records on the system retrieved by one or more PII data elements?

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within the OMB

Identify the OMB information collection approval number and expiration date

Not Applicable

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.

No prior notice is given by CROWD, as the PII is collected by another CMS application. The individual requesting access to CROWD uses the CMS Identity Management (IDM) Portal to register and create a new Enterprise Identity Management (EIDM) user account, providing their First Name, Last Name, Date of Birth, Home Address, Email, desired User ID, and Phone Number as required fields. Upon receiving an email confirmation of the successful creation of his or her User ID, the user then logs into the CMS Enterprise Portal and requests access to the CROWD application, indicating his or her desired user role within the system. The user is then taken through the CMS Remote Identity Proofing (RIDP) process and, upon completion, enters an appropriate justification for his or her user role request. This then triggers an email to the authorized CROWD approver to approve his or her role-based access request to the system.

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 PII that is collected is in a separate application, which is the CMS IDM Portal, therefore there is no ability to opt-out. If the user requires access to CROWD, they cannot 'opt-out' of providing their PII to the CMS IDM Portal, as the User ID, Name and Phone Number are the identifiers used to create the user within the CROWD application's security module.

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

The collection of PII (user credentials) is not done by CROWD so there is no notification process. CROWD receives the PII via another CMS application, CMS IDM Portal.

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.

There is no process in place to resolve an individual's concerns by the CROWD system as the PII within CROWD is provided by the CMS IDM Portal. Individual's concerns involving their PII (user credentials), are addressed by the CMS IDM Portal Team (via the IDM Tier 1 Help Desk).

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

To maintain the integrity, availability, accuracy, and relevancy of the PII stored within the database, the System Administrator, semi-annually, performs a crosswalk between the CMS IDM Portal's listing of User IDs associated with the various CROWD User Roles and CROWD's listing of active User IDs. Any anomalies (i.e., name change, or mismatch) is addressed and resolved by contacting the user, and modifying their user data, or by removing their role-based access to CROWD, if no longer required under their current job description. Under this process, outdated, unnecessary, irrelevant, and inaccurate PII is identified and deleted from CROWD. The PII is available as needed and is sufficient (minimum required) for the purposes needed. The PII fields are locked and cannot be changed; The process to ensure that individuals who provide or modify PII cannot repudiate that action is done within the source (CMS IDM Portal) system. The process to ensure PII is available when needed is by having regular periodic updates run between the CMS IDM Portal systems and CROWD; the process to ensure that PII is sufficiently accurate for the purposes needed is ensured when the updates are sync. Users, can at any time, request that their PII (access) be deleted by logging into the CMS IDM Portal and indicating so within its self-service "My Profile" or "Manage My Roles" modules.

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.

Only the System Administrator, Developer, and Help Desk user have access to PII. All other users (Contractor or Government) do not have access to PII, only to the counts data stored in CROWD. User Privileges (role-based) are defined within CROWD's security module. The initial CMS IDM Portal request for approval for access to the CROWD application describes the level of access (need to know) required by the individual.

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.

User Privileges (role-based) are defined within CROWD's security module. The initial CMS IDM Portal request for approval for access to the CROWD application describes the level of access (need to know) required by the individual.

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 CROWD users must annually complete CMS User ID Certification (which involves a review of all applications to which they have access) through the CMS Information Systems Security and Privacy Awareness Training and Cyber Awareness Training, and Records Management Training.

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

New users may receive one-on-one training from the System Administrator. They are also provided with Help Cards (document guides) associated with the specific type of role-based user they are that provide screen prints of the logon process, screen print examples of the location and types of data stored within the application, a User's Guide, and the location of the CROWD write-up within the Internet-Only Manual (IOM). Other training avenues such as conferences, seminars and classroom training provided by CMS/HHS is available apart from the regular annual 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.

This is a new system, CMS websites keep data collected long enough to achieve the specified objective for which they were collected. The data generated from these activities falls under the National Archives and Records Administration (NARA) General Records Schedule (GRS) 5.1 – Common Office Records. Item 010 Administrative records maintained in any agency office.

Records accumulated by individual offices that relate to routine day-to-day administration and management of the office rather than the mission-specific activities for which the office exists. Disposition Instruction states that Temporary destroys when buisness use ceases. Disposition Authority DAA-GRS 2016-0016- 0001.

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

Physical controls such as the security of the physical plant, which include such items as providing long term power supply, emergency lighting, and fire protection; Technical controls are in place such as the IDM Tier 1 Help Desk manages remote access, equipment ordering/testing, and has responsibility for the CMS IDM Portal system (management of user accounts), which defines the privileges for each user of the information system(s); OCISO coordinates compliance with security controls and the artifacts that document compliance by each application; and GSS manages, among others, telecommunications, remote access, and transmission confidentiality. As the physical and technological aspects are managed by other organizations within CMS, and as access to CROWD is a function of the CMS IDM Portal, the duties of the System Administrator are solely, that of administration. Administrative controls are at the application level, although CROWD has built-in internal controls to enforce role-based access to datasets and functions, it is the responsibility of the System Administrator to enforce the Segregation of Duties Policy to ensure that each role has limited responsibility (user roles are defined to only allow access to specific functions of the application. PII is secured on the system level, through compliance with the policies in place, developed to accomplish that task. This involves the annual submission, by the System Administrator, of a System Security Plan (SSP), Information Security Risk Assessment (ISRA), Contingency Plan (CP), completion of the Privacy Impact Assessment (PIA), and adherence to the Security Controls.