US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/18/2016

OPDIV:

CMS

Name:

Contractor Reporting of Operational and Workload Data

PIA Unique Identifier:

P-1795216-473029

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?

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.

N/A

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 Contractor's performance in processing claims. Core Functions:
CROWD provides the capability for Medicare Contractors to electronically enter workload data on a large variety of functional areas (as collected by the shared systems).

CROWD is a mechanism that provides CMS with a timely way to monitor each Medicare Contractor's 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.

The type of information within CROWD is counts of Medicare Contractor workload activity that is collected by the Shared Systems and/or by the Medicare Administrative Contractor (MAC) in-house systems and then submitted to CROWD, either by keypunch or upload. This data is maintained on direct on-line storage for Fiscal Year 1990 through the current fiscal year. 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 (i.e. beneficiary or provider identifiers).

In order to be granted access to the application, the user must provide his or her user ID, name and phone number. These are the three (3) PII identifiers required by the security module within CROWD. 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 Medicare Contractor's performance. Medicare Contractor workloads, submitted on a monthly, quarterly, or annual basis, are permanently maintained in the database.

User credentials (Name, User ID, Phone Number) stored within CROWD, is used to gain the system user access to CROWD in order to perform job duties.

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

Yes

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

Name

Phone Numbers

System User ID

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?

The User ID, Name, and Phone Number are the elements required to create a user account within CROWD which allows the user to access the application.

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

The User ID (PII) 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.

Government Sources

Within OpDiv

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 contacts their CMS component's CMS Access Administrator (CAA) via email, providing the CAA with their Name, User ID, and Phone Number. The CAA, in turn, enters the data into the Enterprise User Administration (EUA) system, requesting approval for access to Jobcode CROWD_P_User. This action initiates an email to the CROWD System Administrator (SA), requesting his/her approval in EUA. Upon approval, EUA notifies the individual, that their request has been granted. In turn, the SA builds the new user record in CROWD, which permits the individual access.

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 EUA, therefore there is no ability to opt-out.

If the user requires access to CROWD, they cannot 'opt-out' of providing their PII to EUA, as the User ID, Name and Phone Number are the identifiers used to create the user within the 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 recieves the PII via another CMS application, EUA .

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 EUA. Individual's concerns involving their PII (user credentials), are addressed by the Enterprise Administration User team (a function of the maintenance contractor, Lockheed Martin).

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

In order 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 EUA listing of individuals with the jobcode CROWD_P_User and CROWD's listing of active users. 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 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 (EUA) system. The process to ensure PII is available when needed is by having nightly updates run between the EUA sytems and CROWD; the process to ensure that PII is sufficiently accurate for the purposes needed is ensured when the nightly updates are sync. Users, can at any time, request that their PII (access) be deleted, by contacting their CAA, who in turn, would take the corresponding action via EUA.

Identify who will have access to the PII in the system and the reason why they require access.

Administrators:

The System Administrator (CROWD File Manager) is assigned the responsibility (privilege) for adding, updating, browsing and/or deleting users.

Developers:

The Developer (System Maintainer) has access to PII in order to assist users in data uploads and for researching anomalies/issues as identified.

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

Only the System Administrator and the Developer have access to PII. All other users (Central Office or Regional Office personnel, CMS Contractors) do not have access to PII, only to the counts data stored in CROWD. User Privileges (role based) are defined within the Security Module. The initial EUA 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 the Security Module. The initial EUA 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 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.

The EUA initiates a notification email to the System Administrator when a user no longer requires access to the application. Correspondingly, EUA also deletes Jobcode CROWD_P_User from the individuals profile. Upon receipt by the SA, the users record (comprising the User ID, Name and Phone Number) is deleted from the CROWD database. Specifically, National ArchivesRecords Association (NARA), General Records Schedule (GRS) 20 states that CROWD will destroy/delete when 7 years 6 months, 10 years 6 months, or 20 years 6 months old, based on the maximum level of operation of the Certification Authority, or when no longer needed for business, whichever is later.; and GRS 24 states that CROWD will delete/destroy when agency determines they are no longer needed for administrative, legal, audit or other operational purposes.

The EUA system that provides the database with PII to CROWD destroys the data. When the nightly updates sync with the CROWD, than the data that is no longer needed is removed from EUA and does not appear in CROWD.

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 Data Center manages remote access, equipment ordering/testing, and has responsibility for the EUA 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 Host on Demand (HOD) and EUA, 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 responsibiltiy (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, bythe System Administrator, of a System Security Plan (SSP), Information Security Risk Assessment (IR RA), Contingency Plan (CP), completion of the Privacy Impact Assessment (PIA), and adherence to the Security Controls.