US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/28/2024

OPDIV:

CMS

Name:

CMS Analysis, Reporting, and Tracking System

PIA Unique Identifier:

P-1810626-760471

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.

Centers for Medicare & Medicaid Services (CMS) Analysis, Reporting, Tracking (CMS ART) application utilizes CMS Identity Management (IDM) Application Programming Interfaces (APIs) for user authentication and authorization.

Describe the purpose of the system.

The CMS ART system maintains business and contract related information about contractors that work with CMS. It tracks contractor cost reports, all deliverables, and estimated versus actual costs for contracts awarded. CMS ART also serves as a repository for contract deliverables, and it collects contract workload information.

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

The CMS ART system is the CMS system of record for tracking Contractor Business Proposals, Cost Reports, Deliverables, and Workload Information for various departments within the agency.

CMS ART captures only federal and contractor contact information which related specifically to a contract and does not store any other Personally Identifiable Information (PII). This data is considered to be contract-specific in nature and has official work contact information only.

The system collects information regarding contracts, including contract-specific dates and financial information. CMS ART maintains contractor cost reports and tracks estimated verses actual costs for contracts awarded by CMS. The system also keeps track of contract deliverables and contract performance data. Contract deliverables are specific requirements per contract and may include documentations per contract requirement. Additionally, there is a point of contact (POC) associated with each contract entry. The POC information includes name, official work address, email address and phone number as well as the user's title. This information is collected directly from official contract documentation.

Contractors in CMS ART consist of the following groups: Comprehensive Error Rate Testing Contractors (CERT/DAVE), Durable Medical Equipment Medicare Administrative Contractors (DME MAC), Medicaid Integrity Contractors (MIC), Medicare Administrative Contractors (MAC), Medicare Drug Integrity Contractors (MEDIC), Program Safeguard Contractors (PSC), Qualified Independent Contractors (QIC), Railroad Retirement Board Contractors (RRB), Retiree Drug Subsidy – Collection of Benefits Contractors (COB), Retroactive Processing Contractors (RPC), and Zone Program Integrity Contractors (ZPIC).

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

CMS ART's business purpose is to provide a consistent means for CMS staff to track detailed financial activity, deliverables, and performance on contracts. CMS ART maintains contractor cost reports and tracks estimated versus actual costs for contracts awarded by CMS.

CMS personnel establish contractors, task orders (a.k.a. contracts), specific tasks associated with each task order, and deliverables associated with each task order. Contract deliverables are specific requirements per contract and may include documentations per contract requirement. A task order is assigned to a contractor, and from that point forward, the contractor defines business proposals for each applicable period of performance. On a monthly basis, cost reports are entered against the business proposal by the contractor to allow for tracking and analysis of actual versus estimated costs. Additionally, files containing deliverables are uploaded by the contractor to satisfy the requirements of those deliverable items that have been defined by CMS.

Contracts in CMS ART are in following groups: Comprehensive Error Rate Testing Contractors (CERT/DAVE), Durable Medical Equipment Medicare Administrative Contractors (DME MAC), Medicaid Integrity Contractors (MIC), Medicare Administrative Contractors (MAC), Medicare Drug Integrity Contractors (MEDIC), Program Safeguard Contractors (PSC), Qualified Independent Contractors (QIC), Railroad Retirement Board Contractors (RRB), Retiree Drug Subsidy – Collection of Benefits Contractors (COB), Retroactive Processing Contractors (RPC), and Zone Program Integrity Contractors (ZPIC).

In order to authenticate users, the system collects user ID and password at the time of logon. The user ID is used throughout the user's session to ensure only authorized data is viewable. Other PII that system will collect or maintain includes e-mail address, mailing address, phone numbers, name, and job role/title.

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

Yes

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

Name
E-Mail Address
Mailing Address
Phone Numbers
Other: Job role/title; User ID; Password/password history

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

Employees
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

The purpose of PII is to identify key personnel that support the contracts that are supported and tracked by CMS ART. These elements cannot be searched directly and show up only as a description of the specific contract. Users can only view those contracts that have been explicitly granted access to them.

The user ID is used throughout the user's session to ensure only authorized data is viewable.

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

N/A. No secondary purposes for PII. PII acts only as information stored about a specific contract.

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

3 USC 501, 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 OPDIV
Other

Identify the OMB information collection approval number and expiration date

N/A. PII only lists POC information about specific contracts. PII is not collected as it pertains to a specific person. POC information is collected through CMS ART user interface.

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 process in place for notification. All POC information is retrieved from official contracts documentation. These documents are not uploaded into the system, rather the POC information is collected manually through the CMS ART user interface.

Users accept the CMS warning banner at the time of logon. This acts as notification to users that user ID/password will be collected by 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.

There is no option to opt out, as only approved POCs for contracts are entered into CMS ART. Contracts are required to have a POC identified. If a POC did not want their work information to be collected, they would not be able to be identified as the contract's POC.

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

Major system changes are communicated to all CMS ART users when they occur, either via phone call and system communication emails and would also go through an internal SIA process. Additionally, major changes are communicated through system messages on the logon page.

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.

POCs would discuss concerns with local CMS Contracting Officer Representative (COR) assigned to their contract. Additionally system users will contact their CMS ART supervisor if they feel their credentials have been inappropriately used. They would also report any unauthorized system use with their credentials to the CMS IT Services 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.

Accuracy and Relevancy: All (and only relevant) POC PII is retrieved from official contracts documentation. As POCs change, the CMS contracts department must first reflect the change within the contract before changes are made to the system. At that time, the CORs maintain the responsibility to update the POC information in CMS ART. The CORs are required to login to the system to update the information, ensuring non-repudiation as it relates to the PII data being entered. This ensures a proper workflow and authorization/purpose of the PII being added to the system. This also ensures the information is accurate.

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 administrator role is restricted to only approved CMS personnel. CMS COR identifies personnel with a need to have administrative access.

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.

Users only have access to a limited subset of contracts. Users are granted read access to those contracts which they support. Administrators grant access to specific contracts based on need to know. These are enforced through Role Based Access Control (RBAC).

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.

CMS users complete annual Enterprise User Administration (EUA) required training. Contractors complete security training in accordance with annual training, as defined by CMS.

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

CMS ART users complete annual security training in accordance, as defined by CMS.

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.

DAA-GRS-2013-0006-0003: Destroy 1-year(s) after system is superseded by a new iteration or when no longer needed for agency/ IT administrative purposes to ensure a continuity of security controls throughout the life of the system.

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

Administrative Controls include but are not limited to: Policies and Procedures; Information Security, Badge, Incident Response, Information Security and Privacy Rules of Behavior, Physical and Environmental, Record Retention, Initial, Annual and Role based security training, and Background checks.

Technical Controls that are in place, include, but are not limited to: USERID/Passwords, 2-Factor Authentication, Access Control Lists (ACL), Data and Internet Encryption, Network and Host Based Firewalls, Network Intrusion Detection/Prevention Systems (IDS/IPS), 3-Tier architecture, De-Militarized Zone (DMZ), Network Antivirus/Spam, Endpoint Security (Antivirus/Malware), Security Content Automation Protocol (SCAP) Monitoring Tools that include; Vulnerability, Configuration, Asset and Patch Management

Physical and Environmental Controls include, but are not limited to (inherited from Amazon Web Services (AWS) mostly): Access Controls; Electronic Key Cards, Numbered Keypad Locks. Fire and Emergency Controls: Emergency Power/Shutoff, Fire Alarms, Smoke Detectors, Emergency Lighting, Lighted Exit Signs, Fire Suppression Systems, Cameras/Electronic Surveillance Systems, Visitor Badges and logs.

Note: web address is a hyperlink.