US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/25/2016

OPDIV:

CMS

Name:

Contractor Administrative Budget and Financial Management System

PIA Unique Identifier:

P-5631180-054466

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.

Agency

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 Administrative Budget and Financial Management (CAFM) system is used by authorized Centers for Medicare & Medicaid Services (CMS) and Medicare Administrative Contractors (MAC) to manage their administrative budget and expenses. CAFM also has the capability to track payments to the contractors, and banking, and financial reporting data of MAC. CAFM provides CMS with a mechanism to set and approve contractor budgets within limits of congressionally appropriated funding. CAFM is used to monitor expenditures to ensure funds are spent in accordance with the approved budget. The CAFM system provides CMS with the capability to monitor contractor compliance regarding budgeting, banking, and payment activities of Medicare contractors. In addition, CAFM provides CMS with a mechanism to track benefit payments by provider type and to detect significant shifts in program expenditure, monitor implementation of new programs, and identify operational problem areas for resolution. There are four CAFM categories are: budget, cash, benefit payments, and settlement reports. These categories are used to accommodate reporting requirements for the Medicare contractor community.

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

Contractor Administrative Budget and Financial Management (CAFM) contains aggregated reporting data entered by the Medicare contractor or the CMS analyst. Data entered into CAFM is stored indefinitely, and can be browsed or queried to create reports. The Personally Identifiable Information (PII) collected within CAFM provides access to four CAFM categories, which are: budget, cash, benefit payments, and settlement reports. These categories are used to accommodate reporting requirements for the Medicare contractor community. The budget category allows the CMS analyst to set and approve contractor budgets within the limits of Congressionally appropriated funds, as well as the ability to monitor each contractor's compliance with their individual budget.

The cash category is used to monitor the financial and banking operations of the Medicare contractor. The benefit category system serves as a mechanism to track benefit payments by type of provider to detect shifts in program expenditures, monitor new program implementation, and to identify operational problems for resolution. The settlement reports category allows the analyst to develop budgeted and incurred costs for contractor audit and settlement functions by type of activity and type of provider or reporting entity. The CAFM system maintains the user's ID, name, email address, and contact phone number.

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

The CAFM system is the main vehicle for planning, administering and monitoring the administrative expenses for the Medicare contractor community. The PII elements maintained in the CAFM system are User ID, Name, Address, and Contact number. These data elements can only be accessed by the File Manager or System Administrator for user activity reporting.

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

Phone Numbers

Other - User ID

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 Personally Identifiable Information (PII) is used to identify an authorized user's history.

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

There are no secondary use for the PII collected.

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

Title 5 U.S. Code, Section 301

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.

09-70-0538

SORN is In Progress

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Persion

Government Sources

Within OpDiv

Non-Governmental Sources

Other

Identify the OMB information collection approval number and expiration date

Not Applicable- OMB collection approval number not required for information required to gain system access.

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.

The PII is collected by another system for authorized use and access to the CAFM system. Users are notified through security audit alerts for all system activity when the system is accessed by their user ID. CAFM only stores user IDs, name, email address and contact phone number for users for file and system management only.

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.

Users may opt-out of data collection of PII (user ID, name, address and contact number) within CAFM when completing the application for gaining initial access to the system. However, without user consent, an individual may not gain access to the system.

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

No process is in place within CAFM, however, in accordance with the Privacy Act, a new system of record notice (SORN) would be published with a 60-day comment period to notify individuals of a change in use and/or disclosure of data by the IACS.

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.

CAFM distributes daily security audit alerts to individual users when the system is accessed with their PII (user ID). If the user feels his/her information has been used inappropriately or the user has not accessed the system at the time of notice they may contact the system administrator for mitigation. Only the necessary PII is maintained for access purposes and users who no longer require access are removed through synchronization.

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 CMS Access Administrator (CAA) assigned to the user or contractor are responsible for ensuring the integrity and availability of user's information on behalf of CMS. The Business Owner completes a quarterly audit review. A job code report is generated by (Enterprise User Administration (EUA) every 90 days, and sent to the Business Owner for review. During the review, the Business Owner verifies that job code and system security level assigned to CAFM users corresponds with their job responsibilities. The four levels are File Manager, Central Office, Region, and Contractor. File Managers are system administrators, and can access the PII of another user in the event a formal request is received to confirm or update system access. Central Office, Regional, and Contractor users cannot access the PII of another CAFM user. All users have the capability to update their own PII in the user routing section of the system (for location, phone number, etc.). Data integrity is preserved and maintained because users can only access their own PII, or other data that they have entered into the system.

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

Users:

Authorized CAFM users will have access to view/update their own personal profile information, i.e. Name, address, telephone number & e-mail address. User IDs cannot be modified.

Administrators:

Administrators, i.e. File manager will have access to User Profile information to deactivate or mitigate access issues, run user job code roles, and activity reporting for quarterly auditing purposes. Additionally, Administrators have the capability to update a user's name, addresses, phone number, and access for all users.

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

CAFM job responsibilities (job code) are entered by the CMS Access Administrator (CAA) and determined by user responsibilities by Role Based Access Control (RBAC). The only individuals who may access PII are the file manager and system administrator.

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.

CAFM users are granted specific access based on their job responsibilities (job code) and granted through Role Based Access Control (RBAC) to ensure access is on a need-to-know basis for users in the region, central office, or contractor. However, PII is only accessed by the file manager and system administrator.

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 system users are required to recertify access annually and must complete online CMS System Security and Privacy Computer Based Training (CBT) prior to gaining access to the system.

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

Users receive training via Standard Operating Procedures (SOPs) when systems access is granted. AdHoc training is also offered for system reporting. Standard Privacy Awareness Training is provided by CMS for each user to maintain access and for training on handling access to PII in order to perform job 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.

General Records Schedule (GRS) 20 applies to management of electronic records created or received by Federal agencies including those managed for agencies by contractors. It covers records created by computer operators, programmers, analysts, systems administrators, and all personnel with access to a computer. GRS 24 provides disposal authorization for certain files created and maintained in the operation and management of information technology (IT) and related services as defined in the Information Technology Management Reform Act of 1996 (now the Clinger-Cohen Act), "information technology" including computers.

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

The PII is secured through the Baltimore Data Center (BDC) where the application is housed and is responsible for the physical and environmental security controls. The system adheres to the administrative and technical controls established by CMS such as annual training requirements, assigned job codes/role based job codes, multifactor authentication, firewalls, and encryption. Entry into the Baltimore Data Center is controlled by both security personnel and physical authentication devices. Physical Authentication devices require smart card for entry. The Contract Security Officer controls visitor access to the BDC only. The Officer ensures the visitor is properly signed in and escorted into the BDC. Access into the BDC is monitored and recorded utilizing both the CMS Physical Access Control Systems (PACS) and manual forms for visitors. Access to the CMS complex as a whole is restricted. Only authorized personnel are permitted to enter the buildings within the CMS central office complex. The system controls are reviewed on an annual basis to ensure that the system continue to adhere to CMS' information security practices.