US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/30/2016

OPDIV:

CMS

Name:

Enterprise Electronic Change Information Management Portal

PIA Unique Identifier:

P-5937966-283529

The subject of this PIA is which of the following?

General Support System (GSS)

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.

None

Describe the purpose of the system.

The Enterprise Electronic Change Information Management Portal (ECHIMP) automates the change management process for Fee For Service and Medicare Part D processes. It also automates the Technical Direction Letter process. The Fee For Service change management process uses business requirements to communicate instructions to the Medicare Administrative Contractors (MACs) for the processing of Medicare claims. The Medicare Part D change management process also uses business requirements to communicate instructions to the Medicare Part D maintainers for system changes. The Technical Direction Letter process communicates technical direction to the MACs for time sensitive instructions. In addition, the ECHIMP has added the Award Fee Evaluation Process. This process automates the Award Fee Evaluation Process for calculating MACs awards and award fees. Each of these processes (Fee For Service, Technical Direction Letter, Medicare

Part D and Award Fee Evaluation Process) is managed and conducted by the Medicare Contractor Management Group.

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

ECHIMP collects and maintains information about the Medicare Administrative Contractors (MACs) (Hours estimates, policy information and Change Request numbers)

ECHIMP collects the Award Fee Evaluation information for Medicare Contractor Management Group (computations of award fees for the Medicare Administrative Contractors contracts)

ECHIMP also collects usernames, CMS user IDs, work emails, and work telephone numbers. These are collected to identify and provide users with access to ECHIMP.

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

ECHIMP collects and maintains information about the Medicare Administrative Contractors (MACs). This information and data elements they collect are Hours estimates (dollar and number of hours), policy information (statutory mandates) and Change Request numbers. Also, ECHIMP collects the Award Fee Evaluation information for Medicare Contractor Management Group. This information and data elements include the computations (unique equations that use dollar amounts, hours estimates, labor categories, etc.) of award fees' for the Medicare Administrative Contractors contracts. User names, and CMS user IDs, work emails and work telephones numbers are collected to identify and provision user's access in Enterprise ECHIMP.

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: CMS User IDs and work telephone numbers.

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?

500-4,999

For what primary purpose is the PII used?

The PII collected is strictly CMS user IDs, work email addresses and work telephone numbers. The collection of this information is used for user authentication. This authentication and data is maintained by Enterprise User Administration and Lightweight Data Access Protocol (EUA/LDAP).

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

There is no other secondary uses of PII.

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

5 U.S.C. 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

In-Person

Government Sources

Within OpDiv

Other

Non-Governmental Sources

Private Sector

Other

Identify the OMB information collection approval number and expiration date

N/A

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.

Before users are allowed to logon to Enterprise ECHIMP, they are prompted to select "I agree" to the terms of the application. This "I Agree" button notifies the user their PII (CMS user ID, work email and work telephone number) is being collected.

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 method for users to opt-out. Users are not allowed to log on if they do not select the "I agree" button (to agree to terms) when signing on.

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

If there were a major change, the Enterprise ECHIMP team would notify users using their work emails addresses via a disclosure.

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.

We would work with the ECHIMP Chief Information Security Office (CISO) immediately if a user's PII is obtained, used or disclosed inappropriately. Enterprise ECHIMP users who are deemed inactive receive email notifications regarding their inactive access. This notification instructs users to login to ECHIMP or request to have their ECHIMP job code removed via EUA.

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

ECHIMP contractor maintains the data integrity and availability by employing security procedures including firewalls and encryption layers. The users of the system and CMS administrators maintain data accuracy and relevancy. Users can correct their own PII data within their own account, or administrators can correct this for them if they are alerted to changes. Administrators also run monthly reports. They note discrepancies or problems with data integrity, availability or accuracy and take necessary action to remediate.

Users PII is not editable after users do not access ECHIMP anymore. User's name, work email and work telephone numbers are kept in ECHIMP for record keeping purposes only (audit trail). The data is protected by a role based provisioning system that only allows the ECHIMP system administrators to make edits. The Enterprise ECHIMP also receives nightly reports of the users who access needs to be terminated. Once a user access is no longer needed it is removed in EUA.

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

Users:

Users are able to see other users PII (name, work email address and work telephone number) to communicate and collaborate with other users.

Administrators:

Administrators are able to see users PII (CMS user ID, name, work email address and work telephone number) because they are the stewards for the application. Administrators are responsible for ensuring the system is operating and being used appropriately.

Developers:

Developers can see users PII (CMS user ID, name, work email address and work telephone number) for testing purposes only.

Contractors:

Contractors can see users PII (CMS user ID, name, work email address and work telephone number) for testing and continuity purposes only.

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

ECHIMP has a Role Based Access system. The roles are defined by the ECHIMP system

administrator and business owners. There are job codes that define user's access. These job codes are authenticated/provisioned through CMS' Enterprise User Administrative System (EUA).

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.

Only the system administrators and developers (contractors) have access to PII (CMS users ID, name, work email address and work telephone number) in Enterprise ECHIMP. We run 14-day checks on what administrators and developer (contractors) have access to. If a user does not have the proper job code they are not allowed to see other users PII. This access is provisioned (through EUA/LDAP) upon a user logging into ECHIMP.

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 users (system owners, managers, operators, contractors and/or program managers) must complete the CMS annual security awareness computer based training. In addition, the Information System Security Officer (ISSO) and contractors (security consultant) attended and received the CMS ISSO certification. The ISSO certification consists of a two day (16 hours) training course and written exam. This certification is maintained via annual trainings and training hour requirements.

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

The contractors (security consultant) have a Certified Information System Security Personnel (CISSP) certification. The CISSP certification training consists of asset security, security engineering, software development security, etc. The training and certification process for the CISSP is conducted on an annual basis.

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.

User's PII (CMS user's ID, name, work email address and work telephone number) is retained indefinitely by the application. This information is only retained for the purpose of authentication and/or Enterprise ECHIMP system records (as a audit trail). After a user does not login for a period of 60 days their user credentials are deemed inactive in Enterprise ECHIMP. This means the users are removed from all active user lists until they log back into Enterprise ECHIMP. Enterprise ECHIMP users who are deemed inactive receive email notifications regarding their inactive access. This notification instructs users to login to ECHIMP or request to have their ECHIMP job code removed via EUA. Also, please see the NARA records retention schedule, sections GRS 20 and 24, they apply to ECHIMP.

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

For administrative controls, a CMS staff member is not approved as an administrator with access to PII unless it is determined by the Lead Administrator and Technical Lead that the access is necessary for the employee to complete their job duties. Multi-factor authentication is also in process for administrators that will further protect access to this information. Technical controls include the firewall and encryption protections in place within the system to secure PII. Physical controls include security and monitoring of the servers and data center at our system contractor's site.