US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/28/2016

OPDIV:

CMS

Name:

Enterprise User Administration

PIA Unique Identifier:

P-2722934-005075

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?

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 Enterprise User Administration (EUA) system is the primary application that CMS uses to create and manage CMS employee, Federal, state, and local/tribal agency employee and CMS direct contractor "user credentials" which provide the access and use of many CMS information systems and applications. It is also the system that tracks and manages the Computer Based Training (CBT) certification process that must be completed annually by CMS employees, Federal, state, and local/tribal agency employees and CMS direct contractors to retain access to CMS information systems and applications.

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

The information that may be collected and stored is the following: name; business address, telephone number, email and company name; Social Security Number; password; CMS user ID; organizational affiliation, contract information (if applicable); and assigned job codes for authorized access to CMS systems.

This system also contains internal administration information, such as assigned job codes, system access history, workflows, and approvals necessary to grant various types of access, To log into the EUA system, every user must input their user ID and password.

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

The EUA system manages access to other CMS information systems and applications. EUA allows each user to manage their account information and request job codes for access to other CMS information systems and applications. EUA users are CMS employees and direct contractors primarily. However, for access to certain other CMS systems, there are other authorized users from states, tribal/local agencies, other HHS departments and other Federal agencies. Requests for job codes are approved by authorized CMS Access Administrators (CAA). The EUA system also tracks and manages the Computer Based Training (CBT) certification process that must be completed annually to retain access to other CMS systems.

The information included in EUA identifies the user with information such as name, business address, telephone number, email address, mailing address, employment status, date of birth, company name, CMS user ID and passwords, and organizational affiliation.

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

Yes

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

Social Security Number

Date of Birth

Name

E-Mail Address

Mailing Address

Phone Numbers

Employment Status

Other: Passwords; Job Codes; company name, CMS user ID and passwords, and organizational

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

Employees

Business Partner/Contacts (Federal/state/local agencies)

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

The PII is used to assign, control, track, and report authorized access to and use of CMS information systems and applications.

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

None

Describe the function of the SSN.

The SSN is used to identify the system users.

Cite the legal authority to use the SSN.

Executive Order 9397.

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

Title 5 U.S. Code, Section 552a(e)(10), Executive Order 9397, the Debt Collection Improvement Act, 31 United States Code (U.S.C.) § 7701(c)(1), and 5 U.S.C. 552a(b)(1) and 5 U.S.C 301 Departmental Regulations

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.

Individuals Authorized Access to CMS Computer Services, published 7/26/2002 as 09-70-0064 and

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Email

Government Sources

Within OpDiv

Other HHS OpDiv

State/Local/Tribal

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.

Individuals are notified that their personal information is being collected when they apply for access to CMS systems. The Application for Access to CMS Systems (form CMS -20037) is completed and on page 3 there is a Privacy Act notice that informs individuals that their personal information is being collected. The EUA system does not directly notify individuals.

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.

Because an individual's PII (user ID and password) is required for access to and use of the EUA system, there is no 'opt out' method.

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

If there was a major change to the EUA system that affected the use and/or disclosure of system users' PII, the individuals would be notified by normal CMS methods: user-wide email alerts and notification within the EUA system welcome page. However, obtaining 'consent' isn't part of the process, because PII is required to access the EUA system.

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.

If an individual has concerns about their PII in the system, then the person would contact the CMS IT Service Desk, by telephone or email, to request their PII be updated. Then the EUA administrators would update PII, as approved by the EUA Government Technical Lead (GTL).

If the concern was about inappropriate use, or disclosure, then the individual would also contact the CMS IT Service Desk by telephone or email to report the issue. The CMS IT Service Desk will log the concern in the CMS Issue Tracking System. The issue would be investigated and further action would be taken as necessary.

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 accuracy and relevancy of the PII, EUA users may update their own accounts, and administrators can delete or de-activate accounts. Data integrity and availability is ensured by employing security technologies including firewalls, and encryption and system access logs.

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

Users:

CMS system users may have access to their own PII within EUA in order to verify their information and to manage their account information and passwords.

Administrators:

Database administrators, system administrators and CAAs will have various access levels to PII to perform system functions or manage other EUA user accounts.

Developers:

Developers may have access to PII for database migration and reporting activities. This access window will be time-controlled and monitored to ensure data integrity.

Contractors:

CMS direct contractors may fill the roles of administrators, developers or the CMS IT help desk and would have access to PII in accordance with those roles.

Others:

While not administrators, the CMS IT help desk staff has minimal access to PII in order to reset accounts when a user locks themselves out

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

EUA uses role-based assignments to allow access to PII. The access is limited by a 'need to know and need to access' basis.

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.

Access to PII is limited by the principle of least privilege, where most system users may only see their own PII and authorized users may have access to certain levels of PII. Information is redacted and only certain aspects of the system are accessible.

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.

The CMS Security Awareness and Privacy training is provided to each user on an annual basis. Users acknowledge successful training after passing a test at the end of training and the system verifies completion. This training is mandatory and is required for continued access to CMS systems.

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

Administrators and those with privileged access to the system receive additional training regarding the appropriate and ethical use of privileged accounts. Additionally, rules of behavior for privileged users and acceptable use policies are acknowledged by privileged users.

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 following processes and guidelines are adhered to in the retention and destruction of PII data: National Archives and Records Administration (NARA) Record Control Schedules N1-GRS-87-005, N1-GRS-92-002, N1-GRS-95-002, DAA-GRS-2013-0005, DAA-GRS-2013-0006. CMS retains records to facilitate the review of PII disclosures/access records for five (5) years. CMS ensures that audit information is archived for six (6) years to enable the recreation of computer related accesses to both the operation system and the application wherever PII is stored. CMS retains PII inspection reports, including a record of corrective actions, for a minimum of three (3) years from the date the inspection was completed. CMS retains electronic records for 1 year to provide support for after-the-fact investigations of security incidents and to meet regulatory and CMS information retention requirements. CMS record retention requirements are updated to meet the requirements of The National Archives and Records Administration (NARA) General Records Schedules.

When PII is destroyed, CMS follows the guidance of NIST Special Publication 800-88 Rev. 1. CMS will disintegrate, pulverize, melt, incinerate, and/or shred PII data once it is no longer necessary to retain. Certificates of destruction are completed and retained whenever PII data is destroyed.

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

The administrative controls in place to secure the PII include role-based access and permissions, periodic review of users and deletion or revoking of user accounts. Only authorized administrators can approve job code requests and there is a multi-tier process for some types of access.

The technical controls in place are firewalls that prevent unauthorized access, encrypted access at log on, security scans, penetration testing, and intrusion detection and prevention systems (IDS/IPS) and computer system controls that prevent users without administrative or developer access to long into a test environment and the test environment and usable application are not joined together.

EUA is hosted in a secure data center that employs physical controls and monitoring to restrict physical access and ensure the security of doors with the use of security cards and pass codes; environmental controls that ensure the efficacy of heating, ventilation and air conditioning; smoke and fire alarms, and fire suppression systems; and by employing cameras, fencing and security guards.