US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/26/2025

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?

Existing

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

Significant System Management Change

Describe in further detail any changes to the system that have occurred since the last PIA.

Since last approved PIA, the system has added a Cloud component in addition to the hosted data center.

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 other CMS information systems and applications. It is also the system that tracks 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 or PIV. External users also must enter a second factor, such as one-time PIN via text message or email.

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. In addition, 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 track the Computer Based Training (CBT) certification process that must be completed annually to retain access to other CMS systems. EUA uses PII to retrieve system records, including the CMS user ID, password, email address and a password hint. This allows an authorized EUA user (described above) to access the system. The information collected and stored in EUA is used to identify/authenticate the users. The information collected includes a user's name, SSN, business address, telephone number, email address, business 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: Company name and address, CMS user ID and password, Federal Agency affiliation, contract information, job codes, and internal administration information.

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

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

Title 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 (IACS), published 7/26/2002 as 09-70-

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Email

Online

Non-Applicable

Identify the OMB information collection approval number and expiration date

Government Sources

Within OpDiv

Other HHS OpDiv

State/Local/Tribal

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

The CMS Enterprise Infrastructure & Operations Group (EIOG), Division of Operations Management (DOM), establishes and maintains MOUs, ISAs, and related documents to ensure information sharing and disclosure agreements adequately address information security concerns. The EUA system has appropriate MOUs for sharing information to the following systems: HighGlass, CMS Active Directory, CMS Health Care Financing Administration, CMS MainFrame (RACF), CMS Enterprise Lightweight Directory Access Protocol (LDAP), CMS Portal LDAP, CMS Legacy LDAP, CMS Unix LDAP, CMS Administrative Technology Solutions, Comprehensive Acquisition Management System, CMS Computer Based Training DataBase, Smart Card Management System (Personal Identity Verification - PIV), and the CMS Issue Tracking System.

Describe the procedures for accounting for disclosures.

The information stored within the EUA system is only disclosed to the business owner, or first approver associated with the user whose information was requested. The CMS Government Technical Lead must approve a specific service request routed to EUA administrators in order for this information to be furnished. All requests for disclosures are tracked in a separate system, the CMS Issue Tracking System. Any inappropriate disclosures are handled as information security PII incidents which are reported to the CMS IT service desk and tracked in the CMS Issue Tracking system. Inappropriate disclosures are handled by the CMS Information Security and Privacy Group and reported on in accordance with CMS and

HHS requirements.

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 advised 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.

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, and explain the concerns. The CMS IT Service Desk creates a service/investigation ticket and routes it to the CMS Incident Management Team (IMT), who would investigate and determine if any additional action by the user or CMS is required. If a user believes their PII is inaccurate they can either correct it in their account or the EUA administrators would update PII, as approved by the EUA Government Technical Lead (GTL).

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 review and update their own accounts (at will). System administrators review access and are authorized to delete or de-activate accounts. Data integrity and availability is ensured by reviewing accounts quarterly and deactivating dormant accounts. In addition, the access to user information is limited to a specified group of privileged users. EUA also implements various access and system logs that monitor user activity and alerts system administrators of anomalies.

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.

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

Access to PII is limited by the principle of least privilege, where most system users can only access their own PII and can only access a limited view of the system. Privileged users, such as administrators or developers have access to PII to perform their job functions and maintain the system. For those users, 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 Information Security and Privacy Awareness Training is required to be completed by all users on an annual basis. This training is mandatory for continued access to CMS systems.

In addition, the direct contractor organizations required their staff to take company-sponsored annual security and privacy training. In both scenarios, users acknowledge successful training after passing a test at the end of training and the system verifies completion.

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.

EUA follows the CMS Records Control Schedules located on the cms.gov website and the National Archives and Records Administration (NARA) website.

For CMS and the information systems that support its missions, the NARA Transmittal 29 includes the General Records Schedules (GRS) that are followed. GRS 3.2 provides the requirements for the retention and destruction of PII handled by EUA. For System Access Records (GRS 3.2 Item 030), EUA retains records for up to six (6) years to enable the recreation of computer related accesses to both the operation system and the application wherever PII is stored.

EUA follows the guidance of National Institute of Standards and Technology (NIST) Special Publication 800-88 Rev. 1 as part of the implementation of the Media Protection Security controls. EUA 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 to authorize 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.