US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/16/2016

OPDIV:

CMS

Name:

Enterprise Identity Management

PIA Unique Identifier:

P-9873401-033331

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?

Yes

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.

In support of the American Recovery and Reinvestment Act (ARRA), the Health Information Technology for Economic and Clinical Health Act (HITECH), and the Patient Protection and Affordable Care Act of 2010, also known as Affordable Care Act (ACA), Centers for Medicare & Medicaid Services (CMS) has implemented an Enterprise Identity Management (EIDM) system. EIDM is an identity management system that provides the means for users needing access to CMS applications to identify themselves, apply for and receive credentials in the form of a User Identifier (User ID) and Password, and apply for and receive approval to access the required system(s). EIDM manages the life cycle of User IDs, passwords and the supporting data collected from the user, from issuance to archive. EIDM supports at least-fifty five (55) CMS applications.

EIDM is grouped into four functional areas:

Registration Service: Verify users' identity through the Accessible New User Registration (NUR) process invoking Remote Identity Proofing (RIDP). EIDM uses the Experian RIDP web service to authenticate users. The RIDP service is offered by Experian Information Solutions, Inc.

Authorization Service: Extract relevant identity attributes and support users who already have credentials issued by trusted organizations

Access Management Service: Manage access to CMS applications through the use of roles and groups to assign Level Of Access (LOA) to users

Identity Lifecycle Management Service: Self-service access to forgotten user ID, forgotten password, enable temporarily disabled account, and the ability to restore access to a revoked account, reset password, and update user profile.

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

EIDM collects, maintains and stores the following information on external and internal CMS system users: First Name, Last Name, Date of Birth, E-mail Address, Phone Number, Social Security Number, User Identifier (User ID) and Password, Challenge Questions and Answers, and Organization Name.

The Social Security Number is used to check for registrant uniqueness within the system. The First Name, Last Name, Date of Birth, Phone Number, and Organization Name are used by the approver to approve the user’s request for access.

The User Identifier (User ID) and Password are used to grant access to applications users have been authorized to access. Challenge Questions and Answers are used to validate a user in the event of a forgotten User ID or password.

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

EIDM is an identity management system that provides the means for users needing access to CMS applications to identify themselves, apply for and receive credentials in the form of a User Identifier (User ID) and Password, and apply for and receive approval to access the required system(s). EIDM manages the life cycle of User IDs, passwords and the supporting data collected from the user, from issuance to archive.

EIDM collects, maintains and stores the following information: First Name, Last Name, Date of Birth, E-mail Address Phone Number, Social Security Number, User Identifier (User ID) and Password, Challenge Questions and Answers, and Organization Name.

The Social Security Number is used to check for registrant uniqueness within the system.

The First Name, Last Name, Date of Birth, Phone Number, and Organization Name are used by the approver to approve the user’s request for access.

The User Identifier (User ID) and Password are used to grant access to applications users have been authorized to access. Challenge Questions and Answers are used to validate a user in the event of a forgotten User ID or password.

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

Phone Numbers

Other: User ID, Password, Organization Name, Challenge Questions and Answers

Organization Name

Challenge questions and Answers

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

Employees

Public Citizens

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

Vendor/Suppliers/Contractors

Patients

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The primary purpose of the system is to collect and maintain individually identifiable information to assign, control, track, and report authorized access to and use of CMS' computerized information and resources, for those individuals who apply for and are granted access across multiple CMS systems and business contexts. Information in this system is also used to: (1) Support regulatory and policy functions performed within the Agency or by a contractor, consultant, or CMS grantee; and (2) Support litigation involving the Agency related to this system. The Social Security Number is used to check for registrant uniqueness within the system. The First Name, Last Name, Date of Birth, and Phone Number are used by the approver to approve the user's request for access.

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

None

Describe the function of the SSN.

Social Security Number is used to check for registrant uniqueness within the system.

Cite the legal authority to use the SSN.

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)

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

U.S.C. § 7701(c)(1), Appellate procedures
U.S.C. 552a(b)(1), Records Maintained on Individuals
5 U.S.C. Section 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.

09-70-0538, Individuals Authorized Access to CMS Computer Services

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Email

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

OMB No.0938-1236 Expiration Date: 04/30/2017

Is the PII shared with other organizations?

Yes

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

Private Sector

Experian Information Solutions, Inc. provides Remote Identity Proofing (RIDP) services. PII is sent to Experian over a secure channel using Federal Information Processing Standards (FIPS) 140-2 compliant encryption. Experian enables EIDM to prove the identity of users.

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

Information Sharing Agreement (ISA) with Experian, January 2013: Experian provides Remote Identity Proofing (RIDP) web services for EIDM to remotely identity proof its users.

Describe the procedures for accounting for disclosures.

The disclosure of any PII is documented via the ISA with Experian, as well as, the CMS Incident Management process. A Remedy ticket is created to record the incident and all relevant information to the incident (i.e. What was disclosed, when, how, by whom). An incident investigation will be initiated and the results documented in the Remedy ticket and a report provided to the data owner for all involved systems. Appropriate remediation actions will be taken based on nature of the incident.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

There is a Privacy Act Statement that users must accept during initial registration and again on a yearly basis. The privacy act statement is included in the Terms and Conditions that the user accepts.

The Privacy Act Statement describes how EIDM will use the information the user provides. It further describes that the collection of Personal Identifiable Information (PII) is necessary for the identity proofing services being requested which are regulated by the Fair Credit Reporting Act and that a user's explicit consent is required to use these services.

Users must accept the Privacy Act Statement included in the Terms and Conditions on initial registration and at login.

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 must accept a Privacy Act Statement included in the Terms and Conditions on initial registration and at login. Users may opt out of providing their information, however, if a user chooses not to accept the terms and Conditions during the initial registration then a user account cannot be created for the users. Therefore the user will not be able to access CMS applications that require login credentials.

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

Users must accept a Privacy Act Statement which provides users with the uses of data, this is included in the Terms and Conditions on initial registration and at login. A warning banner is also displayed that describes that the system is a government operated system, and that individuals can opt out of usage of EIDM at any time.

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.

Any concerns of inappropriate gathering or use of an individual's PII should be directed to the EIDM Help Desk or sent in writing to Medicare following the complaint process outlined in Medicare’s Notice of Privacy Practices. A Remedy ticket is created to record the incident and all relevant information to the incident (i.e. What was disclosed, when, how, by whom). An incident investigation will be initiated and the results documented in the Remedy ticket and a report provided to the data owner for all involved systems. Appropriate remediation actions will be taken based on nature of the incident.

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

Each application supported by EIDM is responsible for verifying the accuracy of PII collected on their behalf. EIDM supports at least fifty five (55) CMS applications. PII data is protected in transit and storage using FIPS 140-2 approved encryption. An annual Security Controls Assessment is conducted to ensure compliance with the CMS Acceptable Risk Safeguards. EIDM uses role-based access controls to ensure that administrators and users are granted access on a ‘least privilege’ basis commensurate with their assigned duties (only those with the "need" to access the system are granted access for their assigned task/duties). EIDM system administrators and contractors ensure system availability and the PII that is within EIDM.

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

Users:

EIDM account users have access to only their PII. This information is used to identify the user and allow them to manage their EIDM user account.

Administrators:

Administrators/Contractors have access to PII to facilitate the process of managing user accounts, creating new user accounts and disabling inactive user accounts. Administrators also have access to PII in order to maintain and test EIDM.

Contractors:

Administrators/Contractors have access to PII to facilitate the process of managing user accounts, creating new user accounts and disabling inactive user accounts. Administrators also have access to PII in order to maintain and test EIDM.

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

EIDM uses role-based access controls to ensure that administrators, and users are granted access on a 'least privilege' basis that is commensurate with their assigned duties (only those with the "need" to access the system are granted access for their assigned task/duties). Individuals requesting access to a CMS application through EIDM must submit a request indicating the level of access. The request is reviewed and approved by the business owner before access is granted to the application.

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.

EIDM uses the principle of least privilege as well as role based access control to ensure system administrators and users are granted access on a "need-to-know" and a "need-to-access" basis that commensurate with their assigned duties. Individuals requesting access to a CMS application through EIDM, must submit a request indicating the level of access. The request is reviewed and approved by the business owner before access is granted to the application.

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 EIDM users are required to take the CMS Information Security and Privacy training on an annual basis, or whenever changes to the training module are made. This training includes details on the handling of PII.

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

System administrators are required to complete role-based training and meet continuing education requirements commensurate with their role. Other training avenues such as conferences, seminars and classroom training provided by CMS/HHS is available apart from the regular annual training.

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.

National Archives and Records Administration (NARA), General Records Schedule (GRS) 20 states that EIDM will destroy/delete all records that are 7 years 6 months, 10 years 6 months, or 20 years 6 months old, based on the maximum level of operation of the Certification Authority, or when no longer needed for business, whichever is later. GRS 24 states that EIDM will delete/destroy all records when the agency determines they are no longer needed for administrative, legal, audit or other operational purposes. The following are all NARA approved records schedules for EIDM:

1. Master Files

a. Registration - username/password and challenge question/answers, allows users to prove their identify by associating federate credentials as well as use these credentials for subsequent authentication

DISPOSITION: Destroy/delete when 7 years 6 months, 10 years 6 months, or 20 years 6 months old, based on the maximum level of operation of the Certification Authority, or when no longer needed for business, whichever is later.

(Disposition Authority, GRS 24, item 13a1)

b. Authorization - manages applications as well as entitlements within applications as requested items to end users; integration of CMS applications into EIDM; connects with application stores specific to Federal Exchange using the database connector

DISPOSITION: Destroy/delete when 7 years 6 months, 10 years 6 months, or 20 years 6 months old, based on the maximum level of operation of the Certification Authority, or when no longer needed for business, whichever is later.

(Disposition Authority, GRS 24, item 13a1)

c. ID Management – Self-service for forgotten user IDs and passwords to enable temporarily disabled accounts, to rest -passwords, to update user profiles, to allow for step up authentication, for Federated user ID matching, and allow helpdesk service to view users, enable/disable users, unlock user IDs and rest passwords.

DISPOSITION: Delete/destroy when agency determines they are no longer needed for administrative, legal, audit or other operational purposes.

(Disposition Authority: GRS 20, Item 1)

d. Access Management - can extract relevant identify attributes; users enter credentials (e.g., one-time password); native integration point to call an external web service for validation of collected multi-factor credentials.

DISPOSITION: Delete/destroy when agency determines they are no longer needed for administrative, legal, audit or other operational purposes.

(Disposition Authority: GRS 20, Item 1)

2. Inputs

DISPOSITION: Destroy/delete data when entered into the master file or database and verified, or when no longer required to support reconstruction of, or serve as backup to, a master file or database, whichever is later

(NARA Disposition Authority: GRS 20, item 2(4)b, Input Source Records).

5. Outputs

DISPOSITION: Destroy/delete when no longer needed for Agency business. (NARA Disposition Authority: GRS 20, Item 16)

System Administrators review user accounts at least semi-annually to remove user PII if access is no longer required

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

EIDM uses the principle of least privilege as well as a role based access control to ensure system administrators, and users are granted access on a "need-to-know" and "need-to-access" basis that commensurate with their assigned duties. Individuals requesting access to a CMS application through EIDM must submit a request indicating the level of access. The request is reviewed and approved by the business owner before access is granted to the application.

EIDM is located in a Tier-1 (Hewlett-Packard Enterprise (HPE)) data center which provides premier physical control protections. Physical controls are in place such as security guards to ensure that access to the buildings is granted to authorize individuals. Identification of personnel is checked at the data center.

EIDM is built using industry best practices and independently reviewed against Federal Information Security Management Act (FISMA) and National Institute of Science and Technology (NIST) Security and Privacy controls to ensure technical, operational, and management controls are properly applied.

Identify the publicly-available URL:

https://portal.cms.gov/

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Session Cookies that do not collect PII.

Persistent Cookies that do not collect PII.

Does the website have any information or pages directed at children under the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

Yes

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

No