US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/20/2016

OPDIV:

CMS

Name:

Enterprise Eligibility Service

PIA Unique Identifier:

P-8742773-975643

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 Eligibility Service (EES) is a web service that is used to determine Medicare eligibility for individuals enrolling into health insurance through the Federally Facilitated Marketplace (FFM) and State Marketplaces (SM).

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

EES receives inquiries that contain an individual's Social Security Number (SSN), Date of Birth (DOB), Name, and Gender from another CMS system which is Data Services Hub (DSH). EES does not store this information. EES processes the information contained in the inquiries and uses this information to look up in the Common Medicare Environment (CME) and determine if an individual is eligible for Medicare. EES only provides this service to the Data Services Hub (DSH) which supports the FFM and SM.

EES collects user ID and passwords and these login credentials are used to grant access to the system. Users of EES are the system administrators, maintainers and developers. The login credentials (user ID) used to access EES are provided to users by another CMS system which is Enterprise User Agreement (EUA). EUA authenticates and approves requested EES job codes.

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

The Enterprise Eligibility Service (EES) is a web service that is used to determine Medicare, Part A eligibility for individuals enrolling into health insurance through the Federally Facilitated Marketplace (FFM) and State Marketplaces (SM).

EES receives inquiries that contain an individual's Social Security Number (SSN), Date of Birth (DOB), Name, and Gender from another CMS system which is Data Services Hub (DSH). EES does not store this information. EES processes the information contained in the inquiries and uses this information to look up in the Common Medicare Environment (CME) and determine if an individual is eligible for Medicare. EES only provides this service to the Data Services Hub (DSH) which supports the FFM and SM.

EES collects user ID and passwords and these login credentials are used to grant access to the system. Users of EES are the system administrators, maintainers and developers. The login credentials (user ID) used to access EES are provided to users by another CMS system which is Enterprise User Agreement (EUA). EUA authenticates and approves requested EES job codes.

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

Other - Gender, Login credentials: User ID and Password.

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

Employees

Public Citizens

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

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

EES receives inquiries that contain an individual's Social Security Number (SSN), Date of Birth (DOB), Name, and Gender from another CMS system which is Data Services Hub (DSH). EES processes the information contained in the inquiries and uses this information to look up in the Common Medicare Environment (CME) and determine if an individual is eligible for Medicare. EES only provides this service to the Data Services Hub (DSH) which supports the FFM and SM.

Login credentials (User ID and Password) are used to grant access to EES to support system functions and operations.

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

N/A

Describe the function of the SSN.

SSN is used to identify if an individual is eligible for Medicare.

Cite the legal authority to use the SSN.

Affordable Care Act (ACA), Section 1414
Affordable Care Act (ACA), Section 1411

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?

No

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

No OMB information collection approval is required because PII in EES is not received directly from the individuals with whom the information pertains. The only PII collected directly from the individual about whom it pertains to is the user credentials of system administrators, contractors and maintainers.

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.

EES does not collect or store personal information.

EES receives inquiries that contain PII from another CMS system which is Data Services Hub (DSH).

Login credentials (User ID and Password) are provided by another CMS system which is Enterprise User Agreement (EUA).

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.

The PII within this system is not collected by EES. The PII is collected from the individual by another CMS system, which is DHS. DHS PIA describes the method for individuals to opt-out of the collection or use of their PII.

Login credentials are collected in a separate CMS system, which is the EUA, therefore there is no ability to opt-out. If the user requires access to EES they cannot 'opt-out' of providing their login credentials to EUA.

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

The PII within this system is not collected by EES. The PII is collected from the individual by another CMS system, which is DHS. DHS PIA describes the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system.

Login credentials (User ID and Password) are provided by another CMS system which is Enterprise User Agreement (EUA). EUA PIA describes the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the 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.

The PII within this system is not collected by EES. The PII is collected from the individual by another CMS system, which is DHS. DHS PIA describes 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.

Login credentials (User ID and Password) are provided by another CMS system which is Enterprise User Agreement (EUA). EUA PIA describes 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.

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

EES receives inquiries that contain an individual's Social Security Number (SSN), Date of Birth (DOB), Name, and Gender from another CMS system which is Data Services Hub (DSH). EES does not store these information. DSH PIA addresses the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

Login credentials (User ID and Password) are used to grant access to EES. Users of EES are the system administrators, maintainers and developers. The login credentials within this system are not collected by (EES). The login credentials are provided by another CMS system which is Enterprise User Agreement (EUA). EUA PIA addresses the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

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

Administrators:

Administrators have read access to database records as part of data integrity and troubleshooting efforts.

Developers:

Developers require access to enhance or make system changes to EES.

Contractors:

Direct contractors require access to maintain EES. Direct contractors are Administrators and Developers and Maintainers.

Administrators have read access to database records as part of data integrity and troubleshooting efforts.

Maintainers require access to monitor and maintain EES.

Others:

Maintainers require access to monitor and maintain EES.

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

Individuals requesting access must sign an Account request form prior to account creation. Account request form must be filed to indicate access level needed. This form is reviewed and approved by the System information Security Officer (ISSO) prior to account creation. EES uses role based access controls to ensure the administrators, maintainers and developers 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).

Activities of all users of EES are logged and reviewed by the ISSO to identify abnormal activities if any.

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.

EES 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 "need-to-access" basis commensurate with their assigned duties.

Activities of all users of EES are logged and reviewed by the ISSO to identify abnormal activities if any.

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 EES 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).

Not applicable.

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.

These records will be maintained until they become inactive, at which time they will be retired or destroyed in accordance with published records schedules of the Centers for Medicare & Medicaid Services as approved by the National Archives and Records Administration (NARA).

National Archives and Records Administration (NARA), General Records Schedule (GRS) 3.2, item 030 will destroy 1 year(s) after user account is terminated or password is altered or when no longer needed for investigative or security purposes, whichever is appropriate

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

EES is located in CMS data center, a secured facility. Physical controls are in place such as security guards, and badge reader to ensure access to the buildings is granted to only authorize individuals. Identification of personnel is checked at the facility. Visitors to the data center are escorted at all times during their visit.

Individuals requesting access to EES must sign an Account request form prior to account creation. Account request form must be filed to indicate access level needed. This form is reviewed and approved by the System information Security Officer (ISSO) prior to account creation

EES 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 "need-to-access" basis commensurate with their assigned duties.

Activities of all users of EES are logged and reviewed by the ISSO to identify abnormal activities if any.

EES 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.