US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/18/2016

OPDIV:

CMS

Name:

Enterprise Privacy Policy Engine

PIA Unique Identifier:

P-1681376-643150

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.

The Enterprise Privacy Policy Engine (EPPE) is a system used to track CMS Data Use Agreements (DUAs). A DUA is a binding agreement governing data usage by a User (an individual or entity). CMS provides the User with data that resides in a CMS System of Record (SOR) that is identified in the DUA. The DUA details how the CMS provided information may be used, for how long the information may be used, and how the information must be protected. The DUA is signed by the User, a Custodian (mutually agreed upon by the User and CMS), a sponsoring Federal agency and the CMS representative. The EPPE system shall allow for the more efficient tracking and adjudicating on requests for CMS Personally Identifiable Information / Personal Health Information (PII/PHI) data, while reducing security and privacy risks. Also, EPPE standardizes and automates the DUA process.

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

EPPE collects name, address, phone number, email address, CMS User Enterprise Identity Management (EIDM) ID, Enterprise User Agreement (EUA) ID for those that are entering into a DUA with CMS or those who are overseeing a Data Use Agreement as a CMS employee or direct contractor. No financial data is collected by EPPE at this time.

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

EPPE collects name, address, phone number, email address and CMS User ID and password for those that are entering into a DUA with CMS or those who are overseeing a Data Use Agreement as a CMS employee or direct contractor. This information is required in order to grant the requested DUA.

Prior to disclosing PII data, CMS policy requires the requestor to submit a formal request for data that CMS must approve. The formal request consists of completing a DUA. The DUA includes the following information: requestor name, email address, phone number, mailing address. EPPE Complies with the Federal Information Security Management Act (FISMA) by ensuring that the data is properly protected at all times.

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

Mailing Address

Phone Numbers

User ID and Password

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

Employees

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

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

The PII data in EPPE is used to track disclosures of CMS PII data through Data Use Agreements. The PII data that is collected is contact information of the data user that receives the data, as well as, the CMS employee and direct contractor data authorizer that approves the disclosure.

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

not applicable

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

Section 10332 of the Patient Protection and Affordable Care Act (ACA); 42 CFR 401.101–401.148 and sec 1106(a) of the Social Security Act, 42 U.S.C. 1306(a); 5 USC 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.

09-70-3005, Correspondence Tracking Management System, (CMTS)

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

Non-Governmental Sources

Public

Media/Internet

Identify the OMB information collection approval number and expiration date

0938-0734 Expiration: 12/31/2017

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.

There is a notice on the approved Office of Management and Budget (OMB), information collection form that informs individuals of their privacy rights and that their personal information is being collected.

The CMS employee and contractor user requesting access to EPPE contacts their CMS component's CMS Access Administrator (CAA) via email, providing the CAA with their Name, User ID, and Phone Number. The CAA, in turn, enters the data into the Enterprise User Administration (EUA) system, requesting approval for access to the job code. This action initiates an email to the EPPE System Administrator (SA), requesting his/her approval in EUA. Upon approval, EUA notifies the individual, that their request has been granted. In turn, the SA builds the new user record in EPPE, which permits the individual access.

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.

Individuals cannot opt out of the collection of their information because the notice on the OMB approved collection form informs the individual that they are not required to complete the form, indicating that doing so is voluntary. They only need to complete the form to submit a request for a DUA.

If the CMS employee and direct contractor user requires access to EPPE, they cannot 'opt-out' of providing their PII to EUA, as the User ID, Name and Phone Number are the identifiers used to create the user within the application's security module.

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

Individuals whose PII is in EPPE are notified via individual emails if major changes were to occur in the system that change the use and/or disclosure of the PII.

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.

Concerns of assigned DUA data users or custodians are addressed by the CMS Office of Enterprise Data and Analytics (OEDA) Management team and through the Enterprise ID Management (EIDM) team. However, CMS employee and contractor support user concerns involving their PII (user credentials), are addressed by the Enterprise Administration User team (a function of the maintenance contractor, Lockheed Martin).

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

Only authenticated CMS employee or direct contract support users of EPPE are able to modify or destroy the PII within EPPE. Once the PII is supplied by the requestor, it is entered into EPPE and cannot be modified by repudiated unless it is inaccurate and needs updating. The EPPE system has back up servers to ensure PII/requestor contact information is readily available. A yearly review process has been implemented where data users ensure that their DUA contact information is valid and accurate. Any outdated, unnecessary, irrelevant, and/or inaccurate PII is removed from the system during the annual review if not at the time of the contact information change such as an organization change, etc.

There’s periodic review of DUA data by (OEDA) Management team. The team is in charge of validating inaccurate information to ensure accuracy of information. EPPE has a process for archiving and extending the DUA.

EPPE has implemented segregation of roles based on the principle of least privilege. Only a few designated Administrators have access to the database.

Data is encrypted at rest and in transit thus ensuring data integrity.

There are nightly and weekly system backups thus ensuring availability of data at all times.

Old information is archived.

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

Users:

Needed in order to process data use agreement

Administrators:

Needed in order to process data use agreement

Contractors:

Needed in order to process data use agreement

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

The system administrator determines user roles which have been created in the system. As requestors come into the system, the business owner makes a determination based on the requestor's authority to receive CMS data.

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.

User Roles have been created within the system that limit access to PII within the system based on a "need to know" basis. A review of the roles and their access are conducted bi-weekly, monthly, and yearly to ensure that only the minimum PII necessary is accessed per job role.

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 CMS users are required to take annual CMS Information Security and Privacy training that make them aware of these responsibilities.

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

Any users that have specialized roles within CMS (executives, managers, ISSOs, database administrators, etc.) take role-based privacy and security training in accordance with the Federal Information Security Management Act (FISMA) of 2002 and 5 CFR 930, "Information Security Responsibilities for Employees Who Manage or Use Federal Information Systems."

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.

EPPE records will be held temporarily. They will be deleted when the related master file or database has been deleted per Disposition Authority: NARA’s General Record Schedule 20, Item 10. Additionally, DUAs are required to be retained for 5 years after they are closed by the data user (Disposition Authority: N1-440-10-4, Item 1b).

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

The administrative controls are managed through system access and system user roles. A user name and password is required from those who have access to EPPE in order in enter and search for data within the system. Those without the need to use EPPE are not granted access.

The EPPE system is secured using the following safeguards: user identification, passwords, isolated networks, encryption for data at rest and in transit, intrusion prevention systems, firewalls, security information event management (SIEM) systems, two factor authentication, operating system level and database controls, and segregation of user roles.

Identify the publicly-available URL:

https://eus.custhelp.com

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?

No

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?

No

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

null