US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/29/2016

OPDIV:

CMS

Name:

Public Website Shared Services

PIA Unique Identifier:

P-7815316-788151

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 Public Website Shared Services (PWSS) was developed to provide a single, unified source of geographical location resources to CMS and other federal systems. PWSS contains Application Program Interfaces (APIs) that are available for the geo-location services programming. Geo-location information is used by websites to assist people in finding a business at a particular location or to get directions. Sharing the geographical and zip code information eliminates the need to implement and maintain geographical lookup data by other individual CMS applications and systems. PWSS updates geographical data on regular basis and makes it available for use by CMS.

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

PWSS is an information technology (IT) service that contains and shares geographical information like zip codes, and longitude and latitude for location look-ups. It also contains 'open source' IT code for the developers of other CMS applications and systems to use.

PWSS collects the following information for system administration/access: user information (full

name, user ID, organization, email address, phone number); supervisor's
information (name, organization, email address and phone number); and CMS approver's information (name, email address, and phone number).

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

The PWSS system provides CMS with geographical and go-location data for use in other CMS applications and systems that provide directions to a location, find a location or business or find an address. PWSS is made up of APIs that developers can access and incorporate into those systems.

There are three components of PWSS: Geography (GEO) API, API Manager and Galileo.

Geography API is a shared service API. The main goal of the service is to eliminate a need to implement and maintain geographical lookup data by individual applications. This shared service updates geographical data on regular basis. The service uses the United States Postal Service (USPS) and MapBox data as its data sources. The service is built using a technology called JavaScript Object Notation (JSON). The GEO API offers city, county and/or state lookup by zip code; autocomplete or type-ahead functionality for city, county and state lookup; and GeoCode (longitude and latitude) by full address.

API Manager (KONGKong) is an open source API management platform. The benefit of API Manager is its ease of integration and use for both API creators and API users. The main goal is to allow API creators to focus on building APIs and takes the burden off of access control, rate limiting, and analytics. Kong, the underlying software, acts as a layer above the APIs, so API code doesn't need to be modified to take advantage of the features.

The PWSS also includes the Galileo performance analytics system. The Galileo system works with the Kong API manager. The Kong API manager gathers performance analytics data and transfers it to the Galileo server. The Galileo server will be accessed by the administrators to configure and view a dashboard which provides a wide array of performance analytics data. An example of performance analytics is that the frequency of use of APIs is measured against the number
of users and how many times the GEO and Kong APIs are used to create another.

To access PWSS, a user must register and create an account. PWSS will collect and use "user credentials" which consist of user ID, full name, organization name, email and phone number. This data will be contained in an encrypted flat file (e.g., spreadsheet) for account management, to register the user and check for registrant uniqueness within the system. Only the PWSS administrator will have access to the file. User credentials are retained for as long as the user requires access to PWSS. This information is not shared with anyone else or any other system internally within or externally to CMS.

Registered users may be CMS employees and contractors, non-governmental organizations, other federal government agencies, departments, or state agencies.

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

Phone Numbers

Other - Organization Name, User Credentials (user ID and password), Supervisor information and

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?

100-499

For what primary purpose is the PII used?

PII is collected and used to validate an individual's identity and access to PWSS.

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

There is no secondary use of PII for this system.

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

5 USC 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.

Health Insurance Exchange (HIX) Program, SORN 09-70-0560, published 2/6/2013 and updated

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Private Sector

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.

The PWSS registration form/email has a privacy notice that describes the collection of PII when a user registers for access to PWSS.

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.

There is no option for users to opt-out of PII information collection since it is necessary for users to register to access PWSS.

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

System administrators inform the applicant prior to the enrollment process about how they can be notified about any changes to the way their PII data is used or stored. They can contact the PWSS or GEO administrator if they have any questions about how their data is used/stored.

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.

PWSS users can contact the PWSS or GEO group administrator email account if they believe their PII has been inappropriately used or disclosed or 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.

Manual reviews of the registration spreadsheet are conducted at least annually to determine if the PII is accurate, whether the user is still active in the system and whether a user is still able to use and access the system. A continuous monitoring program is in place to ensure system integrity and availability. The PWSS is designed with system logic checks to ensure data accuracy and integrity.

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

Administrators:

Application or API administrators will have access to PII to perform their job as administrators of applications or local systems, to add, edit and delete users.

Contractors:

Application or API administrators may be contractors, and would have access to PII to perform the functions of those roles.

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

Administrators of PWSS must have a valid CMS ID, submit a request form, and have been approved through their CMS Contracting Officer's Representative (COR) and manager. After receiving approval by the COR, the administrator must then request access for specific PWSS API access. They are given access based on the principle of least privilege.

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.

Administrator access to PWSS is restricted to CMS approved system administrators. Administrators can only access it using multi-factor authentication and have been granted administrative roles. Access to PII is limited by role-based permissions. Inactive accounts are reviewed and deleted after a set time period.

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.

Both CMS employees and contractor staff who access or operate CMS systems are required to complete the annual CMS Security Awareness training provided annually as Computer-Based Training (CBT) course. This course specifically addresses what PII is and specifies privacy laws and regulations that apply to safeguarding PII. Contractors also complete their annual corporate security training.

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

There is no specific user training in addition to the general security and privacy awareness 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.

PWSS follows the CMS Records Schedule that was published April 2015 and the National Archives and Records Administration General Records Schedule (GRS) 20 and 24.

Specifically, for user credentials that are securely stored in the PWSS database, per National Archives Records Association (NARA), General Records Schedule (GRS) 20 states that PWSS will 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; and GRS 24 states that PWSS will delete/destroy when agency determines they are no longer needed for administrative, legal, audit or other operational purposes.

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 access control - request and authentication to PWSS is limited to specific users. There is also periodic review of users and deletion of inactive accounts and role-based access for administrators.

The technical controls in place are: firewalls that prevent unauthorized access;, encrypted access when users obtain the approval to log into the application; all communication are encrypted; anti-virus and intrusion prevention systems (IPS); and monthly vulnerability scans of the system.

The physical controls in place are as follows: the PWSS is hosted in a CMS Virtual data center. The data center has exterior security controls- use of security cards and pass codes and security guards. The PWSS maintenance/administrative users access by using security tokens and user credentials to access the server equipment.