US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/10/2016

OPDIV:

CMS

Name:

Amazon Web Services

PIA Unique Identifier:

P-9660184-315057

The subject of this PIA is which of the following?

General Support System (GSS)

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.

Amazon Web Services (AWS) is a cloud service provider (CSP) that provides Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) for the Centers for Medicare & Medicaid Services (CMS). AWS will be used as a cloud infrastructure environment to support CMS web hosting.

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

AWS collects and maintains employee and contractor credentials to include; user first and last name, cell phone number and email address. The PII (user first and last name, cell phone number and email address) is collected and maintained in order to grant users access to AWS.

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

AWS is a General Support System (GSS) that provides the infrastructure to host CMS Major Applications. AWS does not directly collect, maintain, or disseminate information, but rather provides cloud support infrastructure for other CMS Major Applications to perform these functions.

This PIA only considers the AWS. Separate PIAs will be evaluated for each of the Major Applications hosted by AWS. The Major Applications hosted by AWS include Exchange Consumer Web Services (ECWS), Market Place Lite (MPL), Finder, External Data Gathering Environment (EDGE), and Assister Help Resource Center Support System (AHRCSS). AWS collects and maintains employee and contractor credentials to include user first and last name, cell phone number and email address.

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

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

Employees

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

AWS collects and maintains employee and contractor credentials to include; user first and last name, cell phone number and email address. The PII (user first and last name, cell phone number and email address) is collected and maintained in order to grant users access to AWS.

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

There are no other uses for the PII collected outside of the primary use.

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.

09-70-0560, Health Insurance Exchanges (HIX)

Identify the sources of PII in the system.

Other

Government Sources

Within OpDiv

Non-Governmental Sources

Private Sector

Other

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.

No prior notice is given as the system doesn't directly collect any personal information. The information is provided by EIDM. Individuals requesting access to AWS must sign an account request form. The account request form must also be filled indicating name, email, phone number and access level needed. This form is reviewed and approved by the System information Security Officer (ISSO) prior to account creation.

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 that is collected in a separate application, which is the EIDM application, therefore there is no ability to opt-out. Potential user cannot 'opt-out' of providing his or her PII (email, name and phone number). The PII is needed to create a user account in order to access AWS.

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

Notification is not provided by AWS, because the PII is not directly collected from the individual.The PII that is collected in a separate application, which is the EIDM. However individual requesting access to AWS must sign an account request form prior to account creation.

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 data is obtained from another CMS system, therefore, there is no process in place by AWS to address an individuals' concerns. However, complaints regarding the use of a system user PII can be sent to any of AWS system administrators .These complaints will be given a corresponding ticket to ensure that the system administrators practice due diligence to review the issue, question or concerns of the individual. Data collection practices, privacy and security safeguards are of the utmost importance to the AWS system management and any concerns raised will be reviewed.

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

In order to maintain the integrity, availability, accuracy, and relevancy of the PII, System Administrators review user accounts annually. Any anomalies are addressed and resolved by contacting the user, and modifying their user data, or by removing their access if no longer required. Under this process, outdated, unnecessary, irrelevant, and inaccurate PII is identified and deleted. The PII is available as needed, and is sufficient (minimum required) for the purposes needed. Only system administrators can create or modify PII. Activities of all users including system administrators are logged and reviewed by System Information System Security Officer (ISSO) to identify abnormal activities if any.

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

Administrators:

Administrators create the accounts for the users and modify account information if necessary.

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

Individual requesting access to AWS must sign an account request form. The account request form must also be filled indicating minimal access required to perform one's tasks. Prior to granting access, review and approval is required by the System Information System Security Officer (ISSO).

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.

AWS 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" commensurate with their assigned duties. System Administrators review user accounts at least annually. Any anomalies is addressed and resolved by contacting the user, and modifying their user data, or by removing their access if no longer required. Activities of all users including system administrators are logged and reviewed by AWS 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 AWS users are required to take the CMS Information Security and Privacy training on an annual basis, or whenever changes to the training module have been made. This training includes details on the handling of PII.

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

CMS employees and contractors with privileged access 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.

In addition to the CMS provided trainings, AWS contractors take the following courses from their company; Rules of Behavior, HIPAA Privacy, and Culture of Responsibility.

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.

Records Association (NARA), General Records Schedule (GRS) 20 states that AWS 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 AWS will delete/destroy when agency determines they are no longer needed for administrative, legal, audit or other operational purposes. 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.

AWS is located at a secured facility. Physical controls are in place such as security guards to ensure access to the buildings is granted to only authorize individuals. Identification of personnel is checked at the facility. AWS uses the principle of least privilege as well as a role based access control to ensure system administrators are granted access on a "need-to-know" and "need-to-access" commensurate with their assigned duties. The information is protected using Access Control Lists (ACLs) defined for allowing only administrator access to the PII. This access is further protected by the system controls which enforce two-factor authentication into the AWS system. Furthermore, the information is maintained in an encrypted manner by ensuring the databases are encrypted. Access is provided based on an approved request by the Information System Security Officer (ISSO). Lastly, audit logs are reviewed for suspicious activity by the ISSO on regularly basis.