US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/29/2016

OPDIV:

CMS

Name:

Scalable Login Systems

PIA Unique Identifier:

P-7035478-489646

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.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Describe the purpose of the system.

The Scalable Login Systems (SLS) is an internal CMS web application that supports the Federally-Facilitated Marketplaces (FFM) website, healthcare.gov. SLS provides the identity management of consumers that create accounts on healthcare.gov.

It is a database application that manages the lifecycle of consumers' User IDs, passwords and the supporting data collected from the consumer, from initial creation until the account is archived.

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

SLS collects the following information from consumers and sends the data over an encrypted connection, Secure Socket Layer (SSL), to the FFM system for eligibility and enrollment in a healthcare plan. The FFM maintains its own PIA that outlines the security and privacy controls in place for the information collected and maintained in it.

The list of information that SLS receives from FFM includes the following:

Full name

Employer

Mailing address

Social Security Number

Sex

Race

Marital status

Date of birth

E-mail address

Phone number

Tax filing status

Financial information (e.g., Household income/sources)

Number of Dependents

Each household member information (if applicable): first name, middle name, last name, suffix, address, phone number, email address, preferred language, relationship to applicant

Current health insurance coverage

Citizenship status

Race

Ethnicity

User ID and Challenge questions are generated from the above to create a user account on healthcare.gov.

Additionally, system administrators and developers have user credentials (user ID and password) to access SLS.

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

The SLS is a database applications that provides the identity verification and account management of online accounts that consumers create on the FFM, healthcare.gov. Consumer-users do not have their own local SLS accounts; instead they create an account in the FFM, on healthcare.gov and are marked as a SLS user. The FFM has its own PIA for the information collected and maintained within that system.

SLS services are grouped into two functional areas: the Registration Service verifies each user's identity through the New User Registration (NUR) process using Remote Identity Proofing (RIDP). Experian Remote Identity Proofing (RIDP) web service enables SLS to remotely verify the identity of the consumer applying for insurance. The Identity Lifecycle Management Service provides self-service for the consumer-user, allowing the consumer-user to: change a forgotten ID or password, enable a temporarily disabled account, restore access to a revoked account, and update their profile.

To accomplish these services, SLS collects and shares personally identifiable information with FFM to establish a consumer's primary online account. This information includes a broad list of information such as the consumer's name, address, telephone, employer, SSN, gender, ethnicity, citizenship status, household income, identifying information about any dependents or household members, and preferred language.

The SSN is used to check for registrant uniqueness within the system. The consumer's name, date of birth, and telephone number are used for identity proofing. Information is kept for as long as the consumer purchases healthcare coverage through the FFM on healthcare.gov.

To access the SLS for system support services, SLS collects and uses user credentials (user ID and password). The SLS system support staff are CMS employees and direct contractors. SLS system support user credentials are maintained for the length of employment or length of job position requiring access to SLS.

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

Mailing Address

Phone Numbers

Financial Accounts Info

Employment Status

Taxpayer ID

Other: Employer name, sex, race, marital status, tax filing status; citizenship status; household

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

Employees

Public Citizens

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

PII is collected and used to validate an individual's identity. PII for system administration is used for access to the system for maintenance and other support functions.

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

Not applicable.

Describe the function of the SSN.

Per the Affordable Care Act (ACA), Section 1411; if a consumer has one, CMS must collect the SSN for use in determining citizenship and immigration status. The SSN is also used for validating an individual’s identity prior to enrollment in a qualified health plan.

Cite the legal authority to use the SSN.

ACA 42 USC, Sections 1411 and 1414 and 45 CFR 155.305(f)(6)

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

45 CFR 155.200

ACA, 42 USC Sections 18031, 18041, 18081—18083 and Section 1414, Section 1411

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 Exchanges (HIX) Program, 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

Email

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

CMS Form Number: CMS-10433

Title: Establishment of Qualified Health Plans and American Health Benefit Exchanges.

OMB Control Number: 0938-1156

Expiration Date: 6/30/2019

OMB Control Number 0938-1086

Expiration Date is 12/31/2020

OMB Control Number 0938-1191

Expiration: 6/30/2019

Is the PII shared with other organizations?

Yes

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

Private Sector

To perform the initial identity verification of a consumer creating an account, PII is shared with the Experian RIPD (Remote Identity Proofing Data) to verify the consumer's identity.

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

There is a CMS and Experian Information Sharing Agreement (ISA) in place and authorizes information sharing for the purpose of authenticating consumers.

Describe the procedures for accounting for disclosures.

The SLS system does not disclose PII outside of what is permissible for the system to function and use PII. The SLS maintains an audit record of what information is disclosed to any third parties and for what specific purpose.

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

Because the SLS system is a database system supporting healthcare.gov, the consumer-user is notified by the Privacy Policy posted on the FFM healthcare.gov website that their personal information is being collected. The healthcare.gov website privacy notice is outside the SLS system boundary control. Posted notices on the website are controlled by FFM. Individuals who elect to apply by mail by downloading the 2015 Marketplace Application PDF file are notified by language on the application.

For the SLS system support staff, when they log into the system there is a notice that they are accessing a government computer system and must provide their user ID and password.

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.

SLS doesn't directly provide an option to opt-out of providing PII because it is a database system that supports the functions of healthcare.gov. In order to apply for healthcare coverage via healthcare.gov, whether online, by mail or over the telephone, there is no option for consumers to opt-out of providing PII information if they want to participate in buying health insurance.

For SLS system support staff, their user credentials (PII) are required to access the SLS system and perform their tasks, so there is no option to opt-out of providing PII.

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

The SLS system would not directly notify consumers of major changes. The primary webpage on the FFM website will be updated as necessary and consumer-users that elected for email notifications would be notified by an email notice. In addition, customer service personnel will inform the applicant on the telephone, prior to the enrollment process. Posted notices on the website are controlled by FFM.

For SLS administrators and developers, when they log into the system it is on the CMS intranet and would be notified via internal CMS communications, in the form of email alerts and workplace meetings.

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.

If an individual has concerns about their PII, they can contact the Health Insurance Marketplace call center at 1-800-318-2596. If an individual reports that their PII has been misused or disclosed, an incident report will be filed with the Marketplace Security Operations Center (MSOC) and the CMS Privacy Office will be notified.

The SLS support staff may contact the CMS Information Technology (IT) Help Desk by telephone or email. A help desk ticket is created and the Help Desk will investigate. If necessary, an incident report will be filed with the Marketplace Security Operations Center (MSOC) and the CMS Privacy Office will be notified.

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

To ensure the integrity, availability, accuracy and relevancy of the PII in SLS, the following methodologies are used.

SLS users can manage their own PII by editing their profile after they have registered with the system for data integrity, accuracy and relevancy. SLS does a cross-check with FFM for data integrity for login and account management purposes. SLS sends an email alert notification after a user has modified their login credentials to ensure that users are aware of account changes. The SLS is designed with logic checks to ensure data accuracy and integrity.

For SLS system users, the system maintains the data integrity and availability by employing security technologies including firewalls, and encryption and system access logs. The system users and administrators maintain data accuracy and relevancy by correcting/updating their own PII data within their own account. User account isn’t validated but is monitored for activity and audited for usage. Accounts can be disabled for non-activity or terminated .those accounts that have not been used at least once every 366 days are deleted.

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

Administrators:

System administrators do not specifically access or use PII as part of their system maintenance support activities. However, because they need to have administrator access to perform their maintenance and support activities they may have access to PII.

Developers:

System developers do not specifically access or use PII as part of their support activities. However, because of their support activities, they may be allowed incidental access to PII. Access is only by CMS approval on extremely rare occasions while investigating an incident.

Contractors:

Direct contractors may be either Administrators or Developers, so they may have incident PII access in those roles. Experian staff assists consumers with identity proofing and are provided with a minimum necessary system access to PII for the performance of required tasks.

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

CMS uses role-based access controls to ensure administrators and direct contractors are granted access on a "need-to-know" and "need-to-access" commensurate with their assigned duties. The CMS Business Owner determines who should have access to the system. Additionally, CMS Information System Security Officers (ISSOs) conduct quarterly account reviews to determine which accounts are still active and need to be maintained on the system.

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.

There are three methods for restricting access. First, is to program user interfaces to limit the display of PII to only those elements needed to perform specific tasks. Second, is to limit the transmission of PII to validate information rather than copy or pull information form another authoritative source. Third, is to implement role based access controls and auditing to ensure those with access have a "need-to-know" and "need to access".

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 direct contractor staff who access or operate a CMS system are required to complete the annual CMS Security Awareness training provided annually as Computer-Based Training (CBT) course. Direct contractors also complete their annual corporate security training.

Individuals with privileged access must also complete role-based security training commensurate with the position they are working in.

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.

SLS follows the records retention guidelines are specified in the National Archives and Records Administration (NARA) General Records Schedule (GRS) DAA-0440-2014--0003, which states that records will be destroyed after 10 years of the calendar year when the records were created; and GRS 3.2, which states that records will be destroyed after a maximum of six years.

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

The administrative, technical and physical controls for securing PII in SLS are as follows. Users must obtain CMS user IDs and passwords and are granted access to only those SLS functions and issuer IDs required by their job functions; Direct contractor staff undergo background investigations and security checks; Direct contractor staff undergo security awareness training.

From a technical standpoint, SLS employs the use of a multi-zone security architecture, the operating system is monitored and there are firewalls, host and network based intrusion detection services, and all internet communication is encrypted.

This system is located in a CMS Data Center with strong physical control protections. The Data Center has exterior security controls - security access cards with passwords and security guards to verify identity. The SLS system support users access the system by CMS authentication and access controls by using security tokens and user credentials.