US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/23/2016

OPDIV:

CMS

Name:

State Exchange Resource and Tracking System

PIA Unique Identifier:

P-3033604-743169

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?

Existing

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

Not Applicable

Describe the purpose of the system.

As part of the Affordable Care Act (ACA), the State Exchange Resource Tracking System (SERTS) was created for the CMS Center for Consumer Information and Insurance Oversight (CCIIO) to track and manage the establishment and implementation of State Based Exchanges (SBE). SBEs are alternative healthcare marketplaces for consumers to purchase insurance, other than through the Federally- Facilitated Marketplaces (FFM).

The SBEs provide information about their insurance exchanges through the SERTS web interface. SERTS is the central repository for any state with a SBE. The state SBE uploads information about the SBE's implementation details (such as an operational management plan), implementation milestones, and other program information. It also provides the SBEs with access to resources and technical assistance.

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

The SERTS is a database system for the States with health insurance exchanges. It collects and maintains SBEs' information, including: designated SBE official(s) name; State profile information - HHS region and information on any Federally- recognized Tribes; SBE contact personnel name, email address and telephone; and information about the overall SBE program. The name and contact information of the SBE official is input by the designated SBE user and not collected from the SBE official.

The SBE program information is a detailed description of the how the SBE will operate: the type of healthcare exchange model; the governing board of directors; the exchange by- laws; budget and human resources plans; a description of the consumer-related educational and outreach programs; information on whether the SBE will allow insurance agents or brokers to assist consumers apply for insurance; an explanation of the eligibility and enrollment processes; procedures to evaluate and manage the Qualified Health Plan (QHP) insurers; and the information technology and security and privacy policies and procedures in place.

Additionally, the SERTS will allow SBEs to upload the implementation progress milestones and supporting documentation; technical assistance requests (name of requestor, email address of requestor, request details, resolution details); meeting information (date, time, location, description, federal point-of-contact); interactions data (date of interaction, type of interaction, details of interaction); links to useful websites (some federal, some non-federal); SBE-related news postings; and their CMS contact person's name, email address and policy area of responsibility.

To access SERTS, an individual must input user credentials, a user ID and password. The user credentials are created in a separate CMS system, the Collaborative Application Lifecycle Tool (CALT).

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

SERTS is an informational/database-type website designed to provide states with direct access to resources and technical assistance as they implement SBEs. It is the central repository for any state with a SBE and includes information about the SBE's implementation details (such as an operational management plan), implementation milestones, and other program information. Access to SERTS is limited to only registered and approved CMS employees, contractors and designated state users.

Initially, the submitted information about the SBEs was to receive approval from HHS to operate in replacement or partnership with the FFM. After that approval, now SERTS is a place for states to update their SBE information, have direct access to federal government resources and technical assistance for the implementation and continual operation of the SBEs. It is also the place for SBE Officials and CCIIO's cross-functional team (CFT) to use as they support, track, and aggregate states' adherence to ACA regulations. The SBE information is maintained for as long as the SBE is in existence and is updated as necessary by the designated officials.

To access SERTS, a registered user must input their user credentials, user ID and password. User credentials are maintained for as long as the individual is approved as a registered user. User credentials are created within the CALT system. CALT has its own PIA to manage any PII that that system collects, maintains and stores. Users of the SERTS system include CMS employees and contractors in a support capacity and the SBE designated user(s).

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 - user credentials (user ID and password); request details, resolution details); meeting

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

Employees

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

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The PII contained within the system is for users to access the system's information.

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.

Patient Protection and Affordable Care Act as amended by the Health Care and Education Reconciliation Act of 2010, collectively the Affordable Care Act (ACA) Title 42 USC 18031,18041, 18081-18083 and sections 1311, and1414

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.

Published: SORN 09-70-0560 Health Information Exchanges (HIX) 2/6/2013 and updated 5/29/2013

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within OpDiv

State/Local/Tribal

Identify the OMB information collection approval number and expiration date

Not Applicable for CMS employee/direct contractor system user credentials.

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.

When logging into the SERTS system, there is no process to notify individuals that their personal information is being collected. When they create a user account and user credentials within the CALT system, that system notifies the individual about the use of personal information.

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 'opt out' option because all users must use PII, their user ID and password, to access the system.

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

If there were any major changes to the system, the CCIIO would notify the SBEs, which would notify their registered users. CMS employees and direct contractors with access would be notified by CCIIO as well.

Any additional documentation that a SBE may elect to upload that includes an individual's PII (name and telephone and /or email) would not be notified by the SERTS, since this information is not directly collected.

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.

All concerns regarding PII can be addressed to the FEPS (Federally Facilitated Exchange Operations Support System) helpdesk: CMS_FEPS@cms.h hs.gov, or 1-855-CMS-1515. The FEPS helpdesk investigates any issues.

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

Automated processes are in place that ensure that a user's credentials (for all system users) are matched to the CALT system for authentication by matching their user ID to
their CALT ID, email address, and name. For PII integrity, each time a user logs into SERTS, their user credentials are reviewed and authenticated by CALT. Availability is ensured through automated processes at the CMS Data Center that hosts the application, the Data Center sends emails to the administrator if there is a problem with the application or someone is unable to log on. Accuracy is ensured through the automatic data refresh with every login. Lastly, relevancy is ensured through monthly audits of user accounts and removal of any inactive accounts.

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

Administrators:

Administrators have limited access to PII to manage the access to SERTS and communicate with any users as necessary.

Developers:

Developers may have incidental access to PII to perform any updates to the system's functionality or necessary fixes to problems. It would be on a rare occasion.

Contractors:

Direct contractors, in their roles as administrators and developers, would have access to PII as described in those roles.

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

From an administrative perspective, the CMS GTL (Government Technical Lead) designates system users in certain roles. Within those roles (administrator, developer or direct contractor), the individual would be restricted to a limited set of information, 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.

Access to PII is limited by several methods: user interfaces limit the display of PII to only those elements needed to perform specific tasks; inactive accounts are disabled: and there are role-based permissions that limit the 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.

CMS employees and support direct contractors with CMS accounts must take the annual Security and Privacy awareness training provided by CMS. Users acknowledge successful training after passing a test at the end of training and the system verifies completion. Included in the training is education about how to properly handle sensitive data.

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

There is no training above and beyond the annual CMS 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.

Any records containing PII will be retained and destroyed in accordance with published records schedules of CMS as provided by National Archives and Records Administration (NARA) General Record Schedule (GRS) 20, Item 2a4, which state: Destroy/delete 1 year after cutoff, or when no longer needed for Agency business, whichever is longer; and GRS 24, Item 13a1, which states: 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.

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

The PII within SERTS is secured in the following ways. Administrative controls include using the CALT system to create user credentials; and implementation of role-based access that restricts the activities of users to specific functions.

The technical controls include firewalls that prevent unauthorized access to the system, encrypted access to the application, anti-virus and intrusion detection and prevention systems.

SERTS is hosted within the CMS virtual Data Center, Hewlett Packard Enterprises Virtual Data Center (HPE VDC1) which is protected by security guards, video monitoring and security pass cards for entry.