US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/23/2016

OPDIV:

CMS

Name:

Registration for Technical Assistance Portal

PIA Unique Identifier:

P-4726151-323081

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 Registration for Technical Assistance (REGTAP) website was created by the CMS Center for Consumer Information and Insurance Oversight (CCIIO) to provide educational events and communication for organizations involved in federal and state
healthcare insurance marketplaces, exchanges and Premium Stabilization programs under the Affordable Care Act (ACA).

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

REGTAP collects and stores user registration information which includes the following: email address, name, password, organization name, state, organization type, role in organization, position title, telephone number and training event registration and attendance history.

System support staff, CMS employees and direct contractors, provide user credentials, user name and password to access the system.

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

REGTAP supports the CMS commitment to providing technical assistance, education and communication related to healthcare insurance and Premium Stabilization programs under the ACA. REGTAP provides a secure, public, website for only registered users from organizations such as health plan issuers, insurance agents and brokers, third party administrators, regulators, and other healthcare- related organizations.

The website includes the following services: training event registration, a library of CMS- published resource materials, a frequently asked questions (FAQ) database and an inquiry submission module to submit questions to CMS.

The information collected and maintained in REGTAP includes user account information and the CMS library of resources. The user account information, including the system support staff user credentials, is retained for as long as the user retains their account or as long as the user needs access to the system. The library material is considered ‘public’ as it is informational about healthcare marketplace and Premium Stabilization program topics. Both categories of information are retained indefinitely on an ‘as necessary’ or ‘as applicable’ basis and is updated periodically.

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 - Organizational role and title; Organization Name; State; Training event registration history;

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

Employees

Public Citizens

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

Vendor/Suppliers/Contractors

Health Plans/Issuers

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

Email address, Phone number, organizational role and title, organization name, state, training event, and registration history are used to provide educational events and communication for organizations involved in federal and state healthcare insurance marketplaces, exchanges and Premium Stabilization programs.

User name and password are used to access REGTAP.

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.

Affordable Care Act 42 USC Sections 18031, 18041, 18081-18083 and Section 1414.

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) Program, published 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

Email

Online

Government Sources

Within OpDiv

State/Local/Tribal

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

OMB 0938-1185, expiration 4/30/2019

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.

REGTAP advises individuals on the main log-on page and on the new user registration page that personal information will be collected. As part of the registration, a user must accept the REGTAP terms of use and privacy policy in order to create an account. System support staff are advised as part of the general on-boarding process of CMS employment or gaining access to CMS systems.

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 to 'opt out' of providing PII because it is necessary for the creation of a user account and system access.

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

REGTAP has three methods for notification and to obtain consent if required: 1) on the REGTAP Home page - publicly accessible information (login not required); 2) on the REGTAP Dashboard messaging - available to all registered users; and 3) by email notification to all registered users.

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 believes their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate, they may report this to REGTAP Registrar by telephone at 1-800- 257-9520 or E-mail registrar@regtap.info.

The REGTAP Registrar will contact the office of the Chief Information Security Officer (CISO) and/or the Information System Security Officer (ISSO) within one (1) business hour of issue identification for investigation, and resolution.

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

REGTAP maintains the data integrity and availability by employing security procedures including firewalls, requiring complex passwords, role based access and encryption layers. The users of the system and REGTAP administrators maintain data accuracy and relevancy. Users can correct their own PII data within their own account, or administrators can correct this for them if they are alerted to changes. Administrators also run quarterly reports to determine if there are any anomalies (i.e. name change, or mismatch) with user information. If found, the error is addressed and resolved by contacting the user, and modifying their user data, or by removing their access to REGTAP, if no longer required.

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

Administrators:

Administrators have access to PII to manage user accounts.

Developers:

Developers may have incidental access to PII for system development and maintenance.

Contractors:

Direct contractors may have the role of administrators, developers and the Registrar. They would have access to PII in accordance with the descriptions of those roles.

Others:

The Registrar has access to PII to manage user inquiries and respond to them.

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

REGTAP employs the concept of least privilege, allowing only authorized accesses for registered and system users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks. Based on the principles of least privilege, a role-based methodology is used to identify and validate if the existing access privileges assigned to a registered user are consistent with their job role.

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.

Registered users whose access privileges are not consistent with their job role and cannot be verified, are disabled temporally until their access privileges can be verified by their job role management authority. The REGTAP User Account Management process audit is performed as needed but not less than semi- annually. New or changed REGTAP privileged users accounts are monitored daily.

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.

Annual Security and Privacy Awareness training is required for and provided to all CMS employees and direct contractors that support REGTAP. The contractor staff receives this training as part of their initial training and annually (one year from the date a staff member completed their last security and privacy awareness training session). CMS employees take the training annually and additional REGTAP role based security and privacy training for privileged user roles.

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.

Records are maintained in accordance with the National Archives and Records Administration (NARA) Disposition Authority, DAA-0440-2012- 0016-0001, which states that records are transferred to NARA after 5 years. REGTAP also complies with General Records Schedules (GRS) 3.2, which states that records will be destroyed 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 administrative controls in place to secure the PII include role-based access and permissions, periodic review of users and deletion of non-active accounts.

The technical controls in place are firewalls that prevent unauthorized access, encrypted access when users log into REGTAP, security scans, penetration testing and intrusion detection and prevention technologies. There is alsowell as active penetration testing and a tiered system architecture which means users can only log into the application but not into any test environment and the testing and active applications are not joined together.

The physical controls in place are as follows: the use of security cards and pass codes, security guards and a separately located backup system.

Identify the publicly-available URL:

https://www.regtap.info/

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?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Web Beacons that do not collect PII.

Web Bugs that do not collect PII.

Session Cookies that do not collect PII.

Persistent Cookies that do not collect PII.

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?

Yes

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

Yes