US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

07/11/2025

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?

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.

No changes since the last PIA.

Describe the purpose of the system.

The Registration for Technical Assistance Portal (REGTAP) website was created by the CMS Center for Consumer Information and Insurance Oversight (CCIIO) to provide stakeholder training and outreach for organizations involved in federal and state Healthcare Insurance Marketplaces, under the Affordable Care Act (ACA) and other policy including the No Surprises Act.

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

REGTAP collects and stores user account 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.In accordance with ARS requirements, individual user accounts expire after 60 days without accessing the system. Email

address is added for login by the user at registration, along with a password created and maintained by the user. No other person, including system administrators, have access to user passwords. Name and telephone are stored and used to contact users for system support service desk tickets. Telephone and email address may be used for multi-factor authentication (MFA) at login. Names are required to properly account for training and outreach inquires, attendance records and reporting, while other user demographics are used for determining if a user should be confirmed for a training event. Stakeholder registration and attendance data are shared with CMS only. This information is collected in the REGTAP database and stored permanently.

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, training and communication related to ACA Marketplace, Consolidation Appropriations Act of 2021 (CAA), including the No Surprises Act. REGTAP provides a secure, public, website for registered users from organizations such as health plan issuers, insurance agents and brokers, third party administrators, regulators, and other healthcare-related organizations. We were notified on February 26, 2015, that a CMS Records Freeze in relation to Marketplace Enrollment data supersedes NARA requirements. No PII is available publicly. Types of Personally Identifiable Information REGTAP Collects includes Email address, Full Name, Organization Name, State, Organization Type, Title, Role in Organization, Work Phone, and Mobile Phone. REGTAP reports are available only to CMS and REGTAP staff who need this information to perform their duties. The website includes the following services: training event registration, a library of CMS-cleared 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. All user account information and PII, including the system support staff user credentials, is retained indefinitely. 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.The PII collected by the REGTAP system is used for the purpose of REGTAP account creation, access to the REGTAP platform, user support, and training event confirmation. The REGTAP support staff (direct CMS contractors) regularly uses PII to retrieve system records including using the name, email, organization name, and/or phone number of users and help users with training event registration or other application assistance. All demographic information may also be retrieved by CMS or REGTAP support staff for determining if a user should be confirmed for a training event. This information is not shared or used for any other activities.

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 information includes Organization Name, State, Training event registration history, Password, Organization Type, Title, and Role in Organization.
The type of information that is collected and retained is the same for all users, including those of CMS employees and/or contractors.

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

Employees
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors

ACA Marketplace Stakeholders which consist of health plan issuers, insurance agents and brokers, third party administrators, regulators, and other healthcare-related organizations.
REGTAP organization types include the following: Agents and Brokers, Assisters, Plans/Issuers/Third Party Administrators (TPAs)/Pharmacy Benefit Managers (PBMs), Providers/Facilities, States and Other.

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

PII is used for user account management (system access and account updates). PII is also collected and stored for the purpose of identifying the stakeholder organization type to ensure they receive the appropriate training and outreach information from CMS so they may comply with regulatory rules. CMS also uses PII of users to determine if a user should be confirmed for training events. REGTAP never collects PII for purposes of commercial marketing nor does it share information for any purpose unrelated to the CMS mission and goals.

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 1414.5 USC Section 301 Department RegulationsConsolidated Appropriations Act, 2021 (CAA) including the No Surprises Act.

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

Identify the OMB information collection approval number and expiration date

Government Sources
- Within OpDiv
- State/Local/Tribal

Non-Governmental Sources
- Public
- Private Sector

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 to create an account. REGTAP support staff are advised as part of the general onboarding 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.

All REGTAP users must accept the CMS terms of use to gain access to the system.

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

REGTAP has several methods for notification and to obtain consent if required including the REGTAP Home page before login, the REGTAP Dashboard after login, and email notification to registered REGTAP 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 to registrar@regtap.cms.gov. The REGTAP Registrar will then contact the office of the CMS 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, use of multi-factor authentication (MFA), role-based access and encryption layers. REGTAP users of the system and REGTAP administrators maintain data accuracy and relevancy. Users can correct their own PII data within their own REGTAP account, or administrators can correct this for them if they are alerted to necessary changes. Administrators also run quarterly reports to determine if there are any anomalies (i.e. name change, or mismatch) with REGTAP user information. If found, the error is addressed and resolved by contacting the user and either modifying their user data or removing their access to REGTAP, if no longer required/desired.

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

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 temporarily 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 quarterly. 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 contractors that support REGTAP. Contractors receive this training as part of their initial training and annually thereafter. 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.

On February 26, 2015, CMS notified our team of a records freeze for any records associated with enrollment in the Marketplace which superseded all other requirements. Records are maintained in accordance with the National Archives and Records Administration (NARA) Disposition Authority, DAA-0440-2012- 0016-0001 which indicate the CMS business requirement is that Outreach and Training records are to be stored “Permanently” in accordance with https://www.cms. gov/Regulations-and-Guidance/Guidance/CMSRecordsSchedule/Downloads/Bucket-8-Public-Outreach-and-Engagement.pdf. 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. Any removal of historic information must be approved by its corresponding Government Task Lead.

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 REGTAP users and deactivation of non-active REGTAP accounts. The technical controls in place include firewalls that prevent unauthorized access, encrypted access when users log into REGTAP, security vulnerability scans, annual penetration testing and ongoing intrusion detection and prevention technologies. There is also active penetration testing and a tiered system architecture which means REGTAP users can only log into the production/live application but not into any test (non-production) environment considering the non-production testing and active production applications (environments) are not joined together. Access to the REGTAP database is restricted by CMS EUA account and job codes, CMS CloudTamer access, and CMS Virtual Private Network (VPN). There is no physical system as REGTAP exists solely in the CMS Amazon Web Services (AWS) Cloud through CMS controlled accounts.

Identify the publicly-available URL:

https://regtap.cms.gov/

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.

Does the website have any information or pages directed at children uner 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