

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/04/2016

OPDIV:

CMS

Name:

Small Business Health Options Program - Enrollment Portal

PIA Unique Identifier:

P-4257499-211763

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 Small Business Health Options Program (SHOP) Marketplace was established as part of the Affordable Care Act (ACA), for small businesses to be able to offer affordable healthcare coverage to their employees and for their employees to sign up for healthcare coverage. The SHOP Marketplace is part of the Federally-Facilitated Marketplaces (FFM) website, Healthcare.gov, and is accessible on that website.

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

The SHOP collects information about the small business employer such as: Full name; personal email address, address, telephone, Social Security Number (SSN)(optional); a password; answers to 'challenge questions' to establish their identity; the business name, mailing and physical addresses, Federal Tax ID, telephone, and email. The small business owner must also provide the employee's name(s) and SSN(s) for those employees that will be offered healthcare insurance.

The SHOP also collects information about the small business' employees such as: their name,

address, email, telephone, SSN and tobacco usage. They create a password and answer 'challenge questions' to establish their identity. The employee may provide the following optional information: race, ethnicity and preferred language.

The SHOP displays available health insurance information (plan name, identification number, description and premiums) of Qualified Health Plan (QHP) issuers participating in the SHOP Marketplace. The QHP information is available for viewing indefinitely.

The SHOP system support personnel (CMS employees and contractors) access SHOP with user credentials, a user ID and password.

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

The SHOP allows small business employers and their employees to purchase healthcare coverage from QHPs. The SHOP is accessible on Healthcare.gov. and small business owners may view and compare various healthcare insurance plans and select the plan they want to offer to their employees. Then, their employees can then create an account and sign up for the selected healthcare plan.

The SHOP collects personally identifiable information (PII) from small business employers and employees for determining eligibility and enrolling in a QHP during the application and enrollment process, and this PII is maintained throughout the lifecycle of this process.

Specifically, SHOP requires that each small business owner set up an on-line account. They input their information to create the account. This information is stored for the length of time the small business participates in the SHOP and is updated by the small business as necessary. Each time the small business owner wishes to access SHOP, they will input their email address and a password.

For the small business employee to purchase the coverage being offered to them by their employer, the employee must create an online account and sign up. They input all of their information to create the account. This information is stored for as long as the small business employee purchases the insurance coverage or is employed by their current employer.

The QHP insurance information (plan name, identification number, description and premiums) is available for viewing indefinitely and is updated outside the SHOP program by the QHP.

CMS system user credentials are collected and maintained by the Enterprise Identity Management system (EIDM). EIDM is external to SHOP and the PII within EIDM is covered by a separate PIA. This information is used in order to provide customizable services and provide account support.

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

Employment Status

Taxpayer ID

Other: Employer, Race, Ethnicity, Tobacco usage, User Credentials (user name and password),

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

Employees

Public Citizens

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

PII is used to establish an individual's identity and for determining eligibility for the healthcare plan offered by the small business employer.

The PII collected from CMS employees and contractors is used to create user accounts, which provide a customizable application and a means of contacting users regarding account maintenance or issues.

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

Not applicable.

Describe the function of the SSN.

The SSN is used to determine citizenship and eligibility for healthcare coverage.

Cite the legal authority to use the SSN.

42 U.S.C. Section 18081 requires CMS to collect the SSN for use in determining citizenship and immigration status.

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

42 U.S.C. Section 18081

Affordable Care Act (ACA), Section 1411

Affordable Care Act (ACA), Section 1414

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.

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Online

Government Sources

Within OpDiv

Other Federal Entities

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

OMB Control Numbers:

CMS Form Number: CMS-10400

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

OMB control number: 0938-1191

Expiration Date: 04/30/2016

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 the SHOP small business employer and employee create an account, they are presented with the Healthcare.gov Privacy Policy and must click a checkbox acknowledging that they understand the Privacy Policy before an account is created. PII is required to create an account and obtain healthcare coverage.

There is also a link to the Privacy Policy at the bottom of the website.

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 method for individuals to opt-out of providing their PII because it is required to purchase healthcare coverage in the SHOP.

There is no method for individuals to opt-out of providing their PII because for the system support personnel, user credentials are necessary to access the system to perform their job functions.

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

Should a major change occur, the privacy statement on healthcare.gov will be updated. The System of Record Notice (SORN) will also be updated and posted to the Federal Register to inform the public and provide a means to comment.

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 a concern about their PII, they can contact the SHOP call center at 1-800-706-7893 or the Health Insurance Marketplace call center at 1-800-318-2596 and describe their concerns. The SHOP call center or the Health Insurance Marketplace call center would investigate and work with the individual to resolve their concern.

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

CMS has a National Institute of Standards and Technology (NIST) compliant continuous monitoring program to ensure system integrity, availability, and confidentiality. As a part of CMS, SHOP is included within that monitoring program.

The SHOP online enrollment application is designed with logic checks to verify data accuracy and integrity. CMS Center for Consumer Information and Insurance Oversight (CCIIO) established an Enrollment Resolution and Reconciliation program to provide services necessary to resolve errors and reconcile discrepancies in enrollment data between the SHOP, the QHPs and CMS.

Yearly, CCIIO is required to review and update the enrollment process to verify data collected is relevant to the health insurance enrollment process.

The availability of the user credentials is managed by cross-checks with the EIDM system for current, authorized users. For the PII of consumers, the availability is also managed by the CCIIO's reconciliation process.

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 the perform their maintenance and support activities they may have access to PII.

Developers:

System developers do not specifically access or use PII but because of the type of work they do, they might have incidental access to PII by working on the system updates, improvements, or changes to the system.

Contractors:

Contractors may have a role as SHOP Eligibility Support staff and would assist the small business owner or employee with the enrollment process and may need to access PII. Contractors may also have Administrator and Developer roles and do not specifically access or use PII as part of their system maintenance support activities. However, because they need to have administrator access to the perform their maintenance and support activities they may have access to PII.

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

Access is to PII is granted based on the user's role following the principles of minimum necessary and least privilege. Managers must approve all system access and re-certify that access within every 365 days.

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.

User interfaces limit the display of PII to only those elements needed to perform specific tasks. Also, PII is transmitted to validate information rather than copying or pulling information from another source. Lastly, SHOP implements role-based access controls and auditing to ensure those with access have a "need-to-know" and a "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.

Federal and Contractor personnel who access or operate a CMS system are required to complete the annual CMS Security Awareness Training provided annually as a Computer-Based Training (CBT) course. Contractors also complete their annual corporate Security Awareness Training.

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

Users are also required to complete IRS Security Awareness Training for safeguarding Federal Tax Information (FTI). Personnel with privileged access must also complete role-based security training commensurate with their assigned duties and receive additional job related training by attending conferences, forums, and other specific training on an annual basis.

Contractors implement Security and Privacy Awareness training programs providing general security and privacy awareness training at the time they are hired, before accessing the SHOP Portal system, and annual refresher training thereafter. In addition, periodic reminders are sent via email, as well as items in a weekly contractor newsletter.

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 will be maintained until they become inactive, at which time they will be retired or destroyed, which is ten years. These procedures are in accordance with published records schedules of the Centers for Medicare & Medicaid Services as approved by the National Archives and Records Administration General Records Schedule 20 (GRS 20) for electronic records.

DISPOSITION: Delete/destroy when agency determines they are no longer needed for administrative, legal, audit or other operational purposes (Disposition Authority: GRS 20, item 1).

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

Administrative controls such as written policy, procedures and guidelines have been established. Administrators of the system are vetted prior to hiring and are required to receive annual Security and Privacy awareness training. Third-party assessment validated the implementation of the logical or technical controls that have been implemented to prevent unauthorized access, to safeguard the data in the event of a disaster, and to audit activity within the application

The technical controls in place are firewalls that prevent unauthorized access, encrypted access when users access PAS and computer system controls that prevent users without administrative or developer access to log into a test environment and the test environment and usable application

are not joined together.

SHOP is hosted by a qualified Data Center that employs physical controls and monitoring to restrict physical access and ensure the security of doors; the efficacy of heating and air conditioning, smoke and fire alarms, and fire suppression systems; and by employing cameras, fencing and security guards.

Identify the publicly-available URL:

<https://www.healthcare.gov/small-businesses/>

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?

No