US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/10/2016

OPDIV:

CMS

Name:

Premium Estimation Tool

PIA Unique Identifier:

P-4781243-233826

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 Premium Estimation Tool (PET) system, also called the Window Shopping System (WSS), has two subsystems: Premium Estimation Tool (PET) and Public Facing Tax Tool (PFT).

The subsystem PET enables consumers to get cost and eligibility estimates and browse available health and dental plans on Healthcare.gov, also known as the Federal Facilitated Marketplace (FFM) or Health Insurance Marketplace. The second subsystem PFT assists consumers with determining tax exemption eligibility and premium tax credit eligibility.

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

The subsystem PET gives consumers a chance to see what Qualified Health Plans (QHP) and Stand-alone Dental Plans (SADP) they may be eligible for in the FFM before creating an account and filling out the eligibility application on healthcare.gov. The PET subsystem lets the consumer enter a few details about themselves. The information is not saved/stored by the PET subsystem .

The requested information includes: zip code, gender, household income, ages of household members, tobacco usage, pregnancy, and status/existence of current healthcare coverage. Responses are optional.

Based on that information, the consumer is directed to the next screen where the available plans are listed. The consumer can then select plans and view the description of the insurance plan coverage and see the estimated monthly premiums.

Users of the PFT application enter the zip code and county where each household member lived each month of the previous year, their ages, the months they were eligible for employer coverage, and the months during which they didn't have another coverage exemption. In return, they are provided with the following information: potential premium tax credits, tax exemptions and links to tax related information.

System administrators log into main PET system to support and administer the application/system. To access the system they enter the following login credentials: a User ID and password. The creation of the User ID and password are done in the CMS Enterprise User Administration (EUA) system and not within the main PET system.

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

Login credentials are used by administrators to access systems which support the programming of WSS. The creation of the User ID and password are done in the CMS EUA system.

Information that a consumer enters/selects into the PET webpage is collected temporarily by the webpage but is not stored. When a person exits the screen, the information is not retained for another use. The same user would need to re-enter/select information each time. The information entered by the user/person is: zip code, household income, and ages of household members and whether they use tobacco, are pregnant, and whether they already have health coverage from an employer, Medicaid/ Children’s Health Insurance Program (CHIP), or Medicare. In response, users of the PET application are presented with insurance plan information such as: plan names, copays, deductibles and estimated monthly premiums. The insurance plan information is stored in the Marketplace/Healthcare.gov database to support the PET system and updated monthly by that system's administrators.

Information entered by the public into the PFT webpage is collected temporarily by the webpage but is not stored. When a person exits the screen, the information is not retained for another use. The same user would need to re-enter information each time. The information entered by the user/person is: zip code and county where each family member lived each month of the previous year, the months they were eligible for employer coverage, and the months during which didn't have another coverage exemption. In return, they are presented with tax information. The insurance plan information is stored in the Marketplace/Healthcare.gov database to support the PET system and updated monthly by that system's administrators.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Other: Login credentials (userID and password), zip code, household income, ages of household

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?

1,000,000 or more

For what primary purpose is the PII used?

Login credentials (user ID and password) is collected to support and administer the application/system. To access the system, they enter login credentials. The creation of the User ID and password are done in the CMS EUA system and not within the main PET system.

Temporarily collected PII (zip code, household income, ages, etc.) is used to present the public/consumers with insurance plan information (plan names, copays, deductibles and estimated monthly premiums), and tax 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.

Affordable Care Act. Title 42 U.S.C. 18031, 18041, 18081, 18083, and sections 2723, 2761of the Public Health Service Act (PHS Act).

5USC 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.

SORN 09-70-0560, Health Insurance Exchange (HIX) Program

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Government Sources

Within OpDiv

Other

Non-Governmental Sources

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.

The consumer user community entering information on the main PET system website has a link to the Privacy Policy that contains information about the privacy and use of information collected.

The collection of CMS employee and contractor user credentials being saved by CMS systems is inherent to employment. Individual requesting access to WSS must sign an account request form. Prior to granting access, review and approval is required by the main PET System Information System Security Officer (ISSO).

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.

For the consumers whose PII is temporarily collected, if a consumer decides not to provide this information he or she will not be able to know what Qualified Health Plans (QHP) and Stand-alone Dental Plans (SADP) he or she may be eligible for in the FFM before creating an account and filling out the eligibility application on healthcare.gov. He or she will not know his or her potential premium tax credits, and tax exemptions before creating an account and filling out the eligibility application on healthcare.gov. However, entering this information is optional in order to learn of thier consumer choices.

An option for users to opt-out of having their login credentials stored within the main PET system is not available because it is fundamental to the function of the system. Potential user cannot 'opt-out' of providing his or her PII .The PII is needed to create a user account in order to access the main PET system.

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

Only CMS employees and contractors credentials are accessed/stored by the system. The expectation of user credentials being saved by CMS systems is inherent to system access. Individual requesting access to WSS must sign an account request form. Prior to granting access, review and approval is required by the WSS system owner.

The other collected PII (zip code, household income, ages, etc.) is used to present the public/consumers with insurance plan information (plan names, copays, deductibles and estimated monthly premiums), and tax information. This information is collected temporarily by the webpage but is not stored. When a person exits the screen, the information is not retained for another use.

The same user would need to re-enter information each time. Changes to the use or the disclosure of the PII would be made in the HIX SORN and published for a 60 day public comment period.

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.

The credential information used by the main PETsystem is from the CMS EUA system. If the information (name and company e-mail) is inaccurate such that a name is misspelled or a company e-mail is incorrect, then a simple e-mail to the CMS Access Authority (CAA) with the details of the change would be sufficient to correct the problem and amend the record within EUA.

If an employee has reason to believe that their personal information has been compromised they can create a ticket with the CMS IT Service Desk at a 1-800 number. Potentially, the CMS Cyber Information Center (CCIC) may be notified and they would investigate the matter to determine the severity of the compromise.

The other collected PII are used to present the public/consumers with insurance plan information (plan names, copays, deductibles and estimated monthly premiums), and tax information. This information is collected temporarily by the webpage but is not stored. When a person exits the screen, the information is not retained for another use. The same user would need to re-enter information each time.

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

The other collected PII are used to present the public/consumers with insurance plan information (plan names, copays, deductibles and estimated monthly premiums), and tax information. This information is collected temporarily by the webpage but is not stored. When a person exits the screen, the information is not retained for another use. The same user would need to re-enter information each time.

The credentials information used by the PET system is from the CMS EUA systemThe EUA system is initially responsible for the review for integrity, availability, accuracy and relevancy.

The information is initially entered into EUA via a request form, to allow access to CMS system. The form must be approved by the employee’s manager and COR (Contracting Officer Representative). The EUA system automatically requires users to review their access information annually and confirm that it is accurate. Further, when an employee or contractor is terminated, their access to CMS systems is terminated and their EUA information is deleted.

The PET Administrators will review and update the current users of the PET system to ensure that only the approved users are allowed access to the system.

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

Administrators:

Administrators of the main PET system, may be contractors or CMS employees, will be able to generate a list of local system administrators by login User ID. This is necessary to perform their job as administrators of applications or local systems and have the ability to add, edit or delete userIDs. The only information that is accessible is the User name/User ID.

Local Administrators of PET systems, may be contractors or CMS employees, may have access

to a list of local system administrators by login UserID. This is necessary to perform their job as administrators of applications or local systems.

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

Prospective system administrators must sign an account request form. The account request form must also be filled indicating the minimal access required to perform one's tasks. Prior to granting access, review and approval is required by the system owner.

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.

The main PET system uses the principle of least privilege as well as a role based access control to ensure system administrators, and users are granted access on a "need-to-know" and "need-to-access" commensurate with their assigned duties. System Administrators review user accounts at least annually. Any anomalies are addressed and resolved by contacting the user, and modifying their user data, or by removing their access if no longer required. Activities of all users including system administrators are logged and reviewed by the main PET system ISSO to identify abnormal activities if any.

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 contractors with privileged access are required to complete role-based training and meet continuing education requirements commensurate with their role. Other training avenues such as conferences, seminars and classroom training provided by CMS/HHS is available apart from the regular annual training.

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

None

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.

National Archives Records Association (NARA), General Records Schedule (GRS) 20 states that WSS will 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 and GRS 24 states that WSS will delete/destroy when agency determines they are no longer needed for administrative, legal, audit or other operational purposes. System Administrators review user accounts at least semi-annually to remove user PII if access is no longer required.

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

The main PET system is located at a secured facility. Physical controls are in place such as security guards to ensure access to the buildings is granted to only authorize individuals. Identification of personnel is checked at the facility.

The main PET system uses the principle of least privilege as well as a role based access control to

ensure system administrators are granted access on a "need-to-know" and "need-to-access" commensurate with their assigned duties. The information is protected using Access Control Lists (ACLs) defined for allowing only administrator access to the PII. This access is further protected by the system controls which enforce two-factor authentication into the PET system. Access is provided based on an approved request by the system owner. Lastly, audit logs are reviewed for suspicious activity by the information security officer on regularly basis.

Identify the publicly-available URL:

https://www.healthcare.gov/find-premium-estimates/ , and
https://www.healthcare.gov/taxes/

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.

Session 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