US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/29/2016

OPDIV:

CMS

Name:

Marketplace Lite

PIA Unique Identifier:

P-9175612-272177

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 Center for Medicare & Medicaid Services (CMS) Office of Communications (OC) designed Marketplace Lite (MPL) to provide an easy-to-use application process for individuals with simple life situations to enroll for health insurance coverage on the Federally Facilitated Marketplaces (FFM) website, healthcare.gov. Just as the IRS offers a 1040-EZ form for taxpayers with a simple financial situation, MPL offers a simplified application process for users that have “less complex” life situations.

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

The MPL application process collects the following information from consumers as they create an account and apply for healthcare insurance: full name; date of birth; email address; address; phone number; gender; Social Security Number (SSN); whether they are part of a Federally-recognized Tribe; pregnancy information and tobacco usage. If there are additional household (dependents) members included on the application, some of the above information is collected about them.

The individual creates a user name, answers to ‘challenge questions’ to establish their identity, and a password.

Additional information obtained is citizenship, employment information, dependent information, annual income (financial account information in item 15 below), and current healthcare coverage. Optional information that a consumer may also provide is ethnicity, race and preferred language.

For the MPL system support personnel (administrators, developers) to access the system, they must present 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.

MPL is part of the overall application process within the healthcare.gov website. It provides an easy-to-use application process for consumers with “less complex” life situations. Consumers are redirected to the MPL process, behind the scenes, and answer questions to determine if their household situation is non-complex to qualify for applying through the MPL. If they meet the criteria within the MPL parameters, they complete the application process through MPL. With the streamlined application flow, users can progress through easily to selecting an insurance plan in less time and with less use of computing resources. If the consumer doesn’t meet the non-complex criteria, they are redirected back to the basic FFM application process. The consumer is not aware of the determination process.

The information collected during the MPL application process is retained for as long as the consumer elects to purchase coverage through the FFM.

The individual inputs the information listed in item 12 above to create an account and apply for healthcare insurance. After the application process, the individual is redirected to the FFM to select insurance plans and complete the process. This is an invisible process to the consumer.

The SSN is used to check for registrant uniqueness within the system. The "challenge questions" are used for account creation. Individuals voluntarily provide answers to these questions as well as a user name and password, which are used to identify and authenticate each user.

To access MPL for system support purposes, user ID and password are collected. These user credentials are maintained for the length of time access to the system is necessary.

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

Financial Accounts Info

Employment Status

Other: Income, Healthcare coverage, User ID, Password, Challenge questions, Dependent

Tax Filing Status

User ID, Challenge questions

Dependent Information

Race and Language Preference, Sex (M or F)

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

Employees

Public Citizens

Vendor/Suppliers/Contractors

Other: Health insurance agents and brokers

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

PII is collected and used to validate an individual's identity and eligibility determination for enrollment in a Qualified Health Plan. For system support personnel, it is used to access the system.

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

This is not applicable to MPL.

Describe the function of the SSN.

SSN is used to check for registrant uniqueness within the system and verify citizenship.

Cite the legal authority to use the SSN.

42 U.S.C. 18081 and Affordable Care Act (ACA) sections 1411 and 1414

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

ACA 42 U.S.C. sections 1411(c),1411(d) and 1414; 18031, 18041, 18081—18083

45 CFR 155.200

5 U.S.C. 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.

09-70-0560, Modification to the Health Insurance Exchange (HIX) SORN, October 23, 2013

09-70-0560, Health Insurance Exchanges (HIX) Program SOR, May 27, 2013

09-70-0560, Health Insurance Exchanges (HIX) Program, 2/6/2013 and updated 5/29/2013 and

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

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

OMB Control Number: 0938-1156
Title: Establishment of Qualified Health Plans and American Health Benefit Exchanges.
Expiration Date: 6/30/2019

OMB Control Number: 0938-1191
Title: Data Collection to Support Eligibility Determinations for Insurance Affordability Programs and Enrollment through Health Benefits Exchanges, Medicaid and Children's Health Insurance Program Agencies

Expiration Date: 06/30/2019

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.

As part of the application process and creating an online account, an individual is presented with the Healthcare.gov Privacy Policy and must click a checkbox to acknowledge that they understand it. There is a link to the Privacy Policy at each stage of the application process.

If an individual elects to apply by mail, the 2015 Marketplace Application form has a privacy notice on it.

Users who register by phone or in person are also notified that their personal information will be collected for registration purposes.

MPL system support staff are notified via email when they receive their account login details about the collection of their 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 option for consumers to opt-out of providing PII, since it is necessary for to register for health insurance. It is also necessary that the system collect PII of system support staff for identification and authentication as well as tracking/auditing purposes.

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

Since MPL is part of the FFM website, healthcare.gov, any changes or updates to the system would be posted on the FFM website.

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.

Individual who have concerns about their PII can contact the Health Insurance Marketplace call center at 1-800-318-2596.

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 with regularly scheduled system audits, at least annually, and monthly/quarterly scanning to ensure system integrity and availability. As part of CMS, MPL is included within that monitoring system.

To ensure the integrity, availability, accuracy and relevancy of the PII in MPL, the following methodologies are used. MPL users can manage their own PII by editing their profile after they have registered with the system for data integrity, accuracy and relevancy. MPL does a cross-check with FFM for data integrity and account management purposes. MPL is designed with encryption and role-based access controls to ensure data accuracy and integrity. Encryption is applied to data in transit and data at rest.

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

Administrators:

Administrators may have incidental access to PII in the performance of their duties to support the MPL application process.

Developers:

Developers may also rarely have incidental access to PII in the support of the MPL application.

Contractors:

Contractors may be in a role of administrator or developer, and would have incidental access to PII as described within those roles.

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

The MPL user interfaces limit the display of PII to only those elements needed to perform specific tasks. Role-based access controls to ensure system support staff are granted access on a "need-to-know" and "need-to-access" basis which their assigned duties. The CMS System Owner determines who has an administrative account on this system and reviews all accounts periodically.

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.

There are three methods for restricting access. First, is to program user interfaces to limit the display of sensitive information, such as Personally Identifiable Information (PII) to only those elements needed to perform specific tasks. Second, PII is only transmitted to validate information rather than copy or pull information from another source. Third, role based access controls and auditing ensure those with access have a "need-to-know" and "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.

Both CMS employees and contractor staff who access or operate MPL are required to complete the annual CMS Security Awareness training provided annually as computer based training (CBT) course. Contractors also complete their annual corporate security training.

Individuals with privileged access must also complete role-based security training commensurate with the position they are working in.

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 retention guidelines are specified in the CMS Records Schedule, April 2015, which cites the National Archives and Records Administration (NARA) General Records Schedule (GRS) 20 and 24. GRS 20 and GRS 24 states that MPL authentication files are retained for as long as necessary and destroyed as necessary or after 10 years.

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

This system is located in a network data center which provides physical control protections such as security guards responsible for physical access, the use of security cards for access and video monitoring.

There are intrusion detection and prevention systems, a web application firewall, and encryption of information at rest and in transmission are the technical controls being applied.

CMS uses role-based access controls to ensure system support staff are granted access on a "need-to-know" and "need-to-access"; periodic review and deletion of inactive accounts and access based on "minimum necessary" are the administrative controls in place.

Identify the publicly-available URL:

https://www.healthcare.gov/marketplace/b/app

https://www.cuidadodesalud.gov/marketplace/b/app

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.

Persistent Cookies that do not collect PII.

Other technologies that do not collect PII:

Siteshield,WAF; Third-party web tools: Third-party tools are being used to gain visibility into when website traffic is building during busy (peak) periods.
Third-party tools have access to the following limited information:

Domain from which consumers

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?

No

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

null