US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:
02/10/2015

OPDIV:
CMS

Name:
Federally Facilitated Marketplaces

PIA Unique Identifier:
P-1710508-331195

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

Digital advertising

Describe in further detail any changes to the system that have occurred since the last PIA.
Also corrects the PIA dated 10/30/2013 by, among other things, documenting the use of web beacons and persistent cookies as of 10/30/2013

Describe the purpose of the system.
Healthcare.gov is comprised of three systems that provide the consumer with a seamless experience when inquiring and applying for health coverage:

1. The static website also known as the Learn site provides information about the healthcare law and other public information.
2. Marketplace Lite offers a simplified application process for users who can follow a simplified eligibility and enrollment path.
3. The Federally Facilitated Marketplace, the subject of this PIA.

The purpose of the Federally Facilitated Marketplace is to carry out a number of functions required by the Affordable Care Act (ACA), and other activities that support those functions. A key provision of the ACA is the implementation of Insurance Marketplaces, that help consumers and small businesses obtain health insurance in a way that permits easy comparison of available plan options based on price, benefits and services, and quality.
The Marketplaces carry out a number of business functions required by the ACA, which includes providing an easy-to-use website for individuals to determine eligibility and the enrollment for health coverage that includes support for business operations of Plan Management, Eligibility and Enrollment (including integration with Appeals), and Financial Management.

Describe the type of information the system will collect, maintain (store), or share.
Plan Management (PM) collects and stores insurer (Issuer) and plan information which includes Individual Medical plans, Dental Plans, and SHOP plans; plan information includes Plan & Benefits, Rating Table, Rating Business Rules, Service Area, AAHC, Network ID, Formulary, ECP, NCQA, URAC, Administration, and Network Adequacy.

Eligibility and Enrollment (E&E) collects consumers' demographic information to determine eligibility and enroll applicants into Qualified Health Plans (QHP). The collected information is used to verify and determine eligibility for QHP and potentially for State programs such as Medicaid and Children's Health Insurance Program (CHIP). During Open Enrollment, applications are either auto re-enrolled into the same or similar QHP, or are able to choose a new QHP.

Financial Management (FM) collects Financial Issuer data to perform financial transaction with Issuers and provide support for risk mitigation programs (Reinsurance, Risk Corridors, Risk Adjustments).

Provide an overview of the system and describe the information it will collect, maintain (store), or share,
Plan Management (PM) and Financial Management (FM) does not collect PII data as part of system or business operations.

Eligibility and Enrollment (E&E) operations does collect and store PII data (SSN, demographics) to:

• Determine Eligibility in Medicaid, Children's Health Insurance Program (CHIP), or Qualified Health Plan (QHP) based on Modified Adjusted Gross Income (MAGI) and other factors like disability
• Determine eligibility and calculate the Advance Premium Tax Credits (APTCs) and Cost Sharing Reductions (CSR); determine eligibility for individual responsibility exemption
• Facilitate QHP selection
• Process appeals and exemptions
• Monthly and Annual Internal Revenue Service (IRS) Reporting
Open Enrollment (OE):
• Process enrollment choices

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

Photographic Identifiers

Driver's License Number

Mother's Maiden Name

E-Mail Address

Mailing Address

Phone Numbers

Certificates

Device Identifiers

Military Status

Employment Status

Passport Number

Taxpayer ID

Immigration Documents

Wage Data; Certificate Numbers for Eligibility Exemptions

Federal Tax Information (FTI)

Pregnancy Inquiry

Tobacco Use

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 insurance agents, brokers and web brokers, Exchange Navigators

How many individuals' PII is in the system?
1,000,000 or more

For what primary purpose is the PII used?
Personally Identifiable Information (PII) is collected and used to validate an individual's identity and for determining citizenship, immigration status, employment status and incarceration status, in support of eligibility determinations for enrollment in a Qualified Health Plan, Medicaid, or Children's Health Insurance Program (CHIP) as well as eligibility for advance payments of the premium tax credit and cost sharing reductions. PII is also collected and used for program support for business operations of Plan Management, Eligibility and Enrollment (including integration with Appeals), and Financial Management.

Describe the secondary uses for which the PII will be used.
Limited user information is also used in generation of meta-data for Exchange; reporting, data analysis, and business intelligence. Third-party tools are being used to gain visibility into when website traffic is building during busy (peak) periods, and used to continuously measure and improve site performance and outreach efforts, and to increase outreach and assess the effectiveness of outreach tools.
Third-party tools have access to the following information, including but not limited to:
• Domain from which consumers access the Internet
• IP or MAC address (an IP or internet protocol address is a number that is automatically given to a computer connected to the Web)
• Operating system on the consumers computer and information about the browser used when visiting the site
• Date and time of visit
• Pages visited
• Address of the website that connected to HealthCare.gov (such as google.com or bing.com)
However, third-party tools do not have access through Healthcare.gov to the name, address, Social Security Number, or email address of the consumer.

Describe the function of the SSN.
Per the Affordable Care Act, Section 1411; if a consumer has one, the Centers for Medicare and Medicaid Services (CMS) must collect the Social Security Number (SSN) for use in determining citizenship and immigration status. If volunteered by the individual, the SSN will also be used for validating or Identification (ID) proofing an individual's identity prior to enrollment in a qualified health plan.

Cite the legal authority to use the SSN.
Affordable Care Act (ACA), Section 1411
Affordable Care Act (ACA), Section 1414

Identify legal authorities governing information use and disclosure specific to the system and program.
Affordable Care Act (ACA), Section 1411
Affordable Care Act (ACA), 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.
SORN 09-70-0560, Health Insurance Exchange (HIX) Program, 10/23/2013

SORN 09-70-0560, Health Insurance Exchange (HIX) Program, 05/27/2013

SORN 09-70-0560, Health Insurance Exchange (HIX) Program, 02/06/2013

SORN is In Progress

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
In-Persion

Hardcopy

Email

Online

Government Sources
Within OpDiv

State/Local/Tribal

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?
Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Within HHS
Email Outreach (GovDelivery); Medicare

Other Federal Agencies
Internal Revenue Service (IRS), Social Security Administration (SSA), Department of Homeland Security, Department of Defense (DoD), and Veterans Administration (VA) for the purpose of eligibility determination for healthcare coverage.

State or Local Agencies
State Medicaid, Children's Health Insurance Program (CHIP) programs for the purpose of eligibility determination for healthcare coverage.

Private Sector
Service Corporation (SERCO) (Eligibility Support); Experian (Remote Identity Proofing data match only); Symantec (Multi-Factor Authentication only); Insurance Providers (Enrollment information); Equifax (Current income source validation).

Describe any agreements in place that authorizes the information sharing or disclosure.
The Privacy Policy in the 'Get Started' section of the Individual Application contains information about the privacy and use of information. This is an information sharing agreement that the consumer should acknowledge for the use and disclosure of information.

CMS has Data Use Agreements (DUAs) with Office of Personnel Management and Peace Corp as titled "Data Use Agreement Between U.S. Office of Personnel Management" and "The Department of Health and Human Services, Centers for Medicare & Medicaid Services".

As appropriate Centers for Medicare and Medicaid Services (CMS) executes Interconnection Security Agreements (ISAs), Computer Matching Agreements (CMAs), Information Exchange Agreements (IEAs), and Service Level Agreements (SLAs) with all Federal, State, and Private Sector parties prior to information sharing or disclosure.

CMAs
2013-06 (CMA btw. CMS and Veteran Health Affairs)
2013-07 (CMA btw. CMS and Department of Defense)
2013-08 (CMA btw. CMS and Internal Revenue Services)
2013-10 (CMA btw. CMS and Department of Homeland Security)
2013-11 (CMA btw. CMS and State-based Exchanges)
2013-12 (CMA btw. CMS and Social Security Administration)
2014-14 (CMA btw. CMS and Office of Personnel Management) [a work in progress]
2014-15 (CMA btw. CMS and Peace Corps) [a work in progress]

IEAs
2013-01 (IEA btw. CMS and Internal Revenue Services)
2013-02 (IEA btw. CMS and State-based Exchanges)
2013-03 (IEA btw. CMS and State Medicaid/CHIP Agencies)

Describe the procedures for accounting for disclosures.
The Privacy Policy contains information about privacy and use of information. This policy also contains a link to the Privacy Act Statement and other information related to disclosures.

Per language in the Computer Matching Agreements (CMAs) and Interconnection Security Agreements (ISAs), parties are required to report privacy breaches or suspected breaches to CMS within one (1) hour of detection.

Disclosure of privacy information between systems is managed under routine use notices. In addition system logs maintain transaction information only (not the PII itself) as a record or accounting of each time it discloses information as part of routine use.

CMS has data use agreements (DUAs) for tracking of disclosure of data with Office of Personnel Management and Peace Corp. as titled "Data Use Agreement Between U.S. Office of Personnel Management" and "The Department of Health and Human Services, Centers for Medicare & Medicaid Services".

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 Privacy Policy section of the Individual Application contains information about the privacy and use of information. This also contains a link to the Privacy Act Statement and other information related to disclosures.
The following SORNs have been posted on the HHS website to inform the public:
SORN 09-70-0560, 02/06/2013
SORN 09-70-0560, 05/27/2013
SORN 09-70-0560, 10/23/2013

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.
When a consumer creates an account, they have the option to Opt In or Out to marketplace "Announcements and Updates." The Marketplace does not collect Personally Identifiable Information (PII) until a consumer clicks on "Apply for Coverage" at which point they will be asked to complete the Identity Proofing process. Upon successful completion of Identity Proofing, they can proceed to submit the PII necessary to provide information on the composition of their household, state their household income, and then may proceed to compare QHPs and select a plan. During the Identity Proofing process and subsequent screens, the Marketplace will ask for PII that is used to establish their identity, determine their Eligibility for financial assistance and determine the available plans and premiums for that consumer. Create an Account is not part of this system function, however, this function is discussed in a separate PIA for Enterprise Identity Management (EIDM).

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. In addition the System of Record Notice will be updated and posted on the HHS website to inform the public:

SORN 09-70-0560, 02/06/2013
SORN 09-70-0560, 05/27/2013
SORN 09-70-0560, 10/23/2013

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.
An individual can contact the Health Insurance Marketplace call center at 1-800-318-2596 to report concerns, unlock user accounts, and to reset passwords.
An individual record subject who wishes to know if this system contains records about him or her should write to the system manager who will require the system name, and for verification purposes, the subject individual's name (woman's maiden name, if applicable), and social security number (SSN) (furnishing the SSN is voluntary, but it may make searching for a record easier and prevent delay).

An individual seeking access to records about him or her in this system should write to the system manager and reasonably specify the record contents being sought. (These procedures are in accordance with Department regulation 45 CFR 5b.5(a)(2).)

To contest a record, the subject individual should contact the system manager, and reasonably identify the record and specify the information being contested. The individual should state the corrective action sought and the reasons for the
correction with supporting justification. (These procedures are in accordance with Department regulation 45 CFR 5b.7.)

System Manager:
Director, Consumer Information and Insurance Systems Group, Center for Consumer Information and Insurance Oversight, Centers for Medicare & Medicaid Services
7501 Wisconsin Ave, 9th Floor
Bethesda, MD 20814

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 Centers for Medicare and Medicaid Services (CMS) has a continuous monitoring program based on the National Institutes of Science and Technology (NIST) recommendations to ensure system integrity, availability. The individual enrollment application is designed with logic checks to ensure data accuracy and integrity. Centers for Medicare and Medicaid Services (CMS)/Center for Consumer Information and Insurance Oversight (CCIIO) is establishing and Enrollment Resolution and Reconciliation program to provide services necessary to resolve errors and reconcile discrepancies in enrollment data between the Health Insurance Exchange, State Based Marketplaces, issuer community, and CMS. Yearly, CCIIO is required to review and update the enrollment process to ensure data collected is relevant to the health insurance enrollment process.

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

Users:
To review the information that was submitted by them or their authorized designee

Administrators:
To ensure data Confidentiality, Integrity and Availability.

Contractors:
Eligibility Support workers to help users with the eligibility and enrollment process, and contractor personnel for the purpose of verifying individual identity.

Others:
Insurance issuers to receive enrollment information

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.
The Federally Facilitated Marketplace (FFM) has both public and protected content. Guest/anonymous users will be permitted to access only public content. The Centers for Medicare and Medicaid Services (CMS) uses role-based access controls to ensure administrators and contractors are granted access on a "need-to-know" and "need-to-access" commensurate with their assigned duties.

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 Personally Identifiable Information (PII) to only those elements needed to perform specific tasks. Second, is to limit the transmission of PII to validate information rather than copy or pull information form another authoritative source. Third, is to implement role based access controls and auditing to 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 Federal and Contractor staffs who access or operate a Centers for Medicare and Medicaid Services (CMS) system 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. Furthermore, CMS also complies with requirements to complete Internal Revenue Service (IRS) security awareness training for safeguarding Federal Tax Information.
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).
The Federally Facilitated Marketplace (FFM) is a public system and users are provided links to Privacy and Security policies. CMS employees and contractors with privileged access are required to complete role-based training and meet continuing education requirements commensurate with their role.

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.
A record retention schedule for the Health Insurance Exchange (HIX) is under development with the National Archive and and Records Administration (NARA). Please check the NARA website for posting and updates to the Disposition Authority (DAA).

Per the System of Record Notice (SORN) 09-70-0560, "These records will be maintained until they become inactive, at which time they will be retired or destroyed in accordance with published records schedules of the Centers for Medicare & Medicaid Services as approved by the National Archives and Records Administration."

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.
The Federally Facilitated Marketplace (FFM) system is located in a Tier-1 network data center which provides premier physical control protections. The FFM system and application is built using industry best practices and independently reviewed against Federal Information Security Managment Act (FISMA) and National Institute of Science and Technology (NIST) Security and Privacy controls to ensure technical, operational, and management controls are properly applied.
Personally Identifiable Information (PII) on The Federally Facilitated Marketplace (FFM) system is secured administratively by ensuring that the system goes through the Assessment and Authorization (A&A) process, and all documentation is submitted to the Office of Information Security (OIS) that supports the system and to comply with Federal Information Security Management Act (FISMA) regulations. The system is currently stored at the Terremark Federal Group in Culpepper, VA, and the HP Enterprise Services (HPES) Cherokee Data Center in Tulsa, OK. The system is accessed via Internet only, which is protected by firewalls which secure the information from intruders. The physical controls that are in place such as security guards ensure that access to the buildings is granted to authorized individuals. Identification of personnel is checked at each facility. URS is the service provider in the Terremark data center and HP is the service provider in the HPES data center. Both service providers monitor and support the operating system and underlying infrastructure hardware and network. The eXchange Operations Center (XOC) is responsible for monitoring the FFM application. The FFM cloud contains continuous monitoring tools for end-to-end alerting, reporting, and trending.
The user identity data is stored in the centralized Lightweight Directory Access Protocol (LDAP) store managed by Enterprise Identity Management (EIDM). FFM users and web services send user Identity information to EIDM for user authentication and are required to authenticate to establish their identity and role as an individual or system interacting with the target system.
If Agent/Brokers or Call Center Representatives forget the password but remember the security question/password that was set during their initial registration, they can use the 'Forgot Password' link via the CMS Enterprise Portal to reset their passwords. The new password can be used to log into the system. If users forget the security questions/answers and contact the CMS Help Desk for support, the password is reset and an email is sent to users with the reset link to reset the password. Consumers can use the 'Forgot Password' link via the Marketplace to reset their password.

Identify the publicly-available URL:
www.healthcare.gov

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:

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 access the Internet
• IP address (an IP or internet protocol address is a number that is automatically given to a computer connected to the Web)
• Operating system on the consumers' computer and information about the browser used when visiting the site
• Date and time of visit
• Pages visited
• Address of the website that connected to HealthCare.gov (such as google.com or bing.com)
However, third-party tools do not have access through Healthcare.gov to the name, address, Social Security Number, or email address of the consumer, or any other information that consumers enter on the single streamlined application.
Digital advertising and outreach tools are cost –effective methods used by the Federally Facilitated Marketplace to reach and assist consumers in obtaining health coverage. Contracts are in place with companies to help consumers through the application process including to assist in the delivery withof notices and helpful information, to continuously measure and improve site performance and outreach efforts, and to increase outreach and assess the effectiveness of outreach tools.

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