

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/20/2017

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

New Public Access

Internal Flow or Collection

Describe in further detail any changes to the system that have occurred since the last PIA.

Modifications and improvements were made to the FFM System:

For 2018, the Direct Enrollment (DE) Partner Program has been implemented. The Program allows DE Partners (Insurance Issuers and Web Brokers) to collect information from consumers who choose to provide their information to the DE Partners. When working with consumers, DE Partners will enter consumer information into a HealthCare.gov application for eligibility and enrollment directly from the DE Partner Website. This Program enables consumers to complete their applications, receive eligibility results, and enroll in plans when working with DE Partners and without leaving DE Partner Website(s).

An enhancement has been made to a process for receiving and handling paper eligibility and enrollment applications through digital scanning rather than manual keying consumer information. This will help streamline the eligibility and enrollment process, but does not change the data collection, retention or storage capabilities of the FFM system.

Describe the purpose of the system.

The purpose of the Federally Facilitated Marketplace is to carry out a number of functions required by the Affordable Care Act (ACA). A key provision of the ACA is the implementation of Insurance Marketplaces, to 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 shall carry out a number of functions required by the ACA, including certifying Qualified Health Plans (QHP), administering Advance Premium Tax Credits (APTC) and Cost Sharing Reductions (CSR), and providing an easy-to-use website for individuals to determine eligibility and the enrollment for health coverage. The Marketplaces will be required to interact with stakeholders, including consumers, navigators, agents, brokers, employers, Health Plan Issuers, State-based Medicaid and Children's Health insurance Program(CHIP), Federal agencies for verification checks, third-party data sources, and State Insurance Departments.

Exchange Minimum Functions: Consumer Assistance (45 CFR 155.205). Navigator Program (45 CFR 155.210). Agent Broker program (45 CFR 155.220). QHP certification (45 CFR 155.1000). Eligibility Appeals (45 CFR 155.355). Submission of Notices (45 CFR 155.230). Premium Payment (45 CFR 155.240). Exemption Determinations (45 CFR 155.605). Enrollment in QHPs (45 CFR 155.400). Eligibility Determinations (45 CFR 155.300, 155.305, 155.310). Oversight and Financial Integrity (45 CFR 155.200(c)). Establishment of Exchange network adequacy standards (45 CFR 155.1050). Quality Assessments, Disclosures & Data Reporting (45 CFR 155.200(d)). Administration of APTCs and CSRs (45 CFR 155.340). Coordination with Medicaid, Children's Health Insurance Program (CHIP), Benefit Health Plan (BHP) and Pre-existing Condition Insurance Plan (PCIP) (45 CFR 155.345)

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

The Plan Management (PM) functionality within the FFM is responsible for collecting, evaluating, and certifying Qualified Health Plans (QHP) from Issuers. The PM functionality within the FFM may collect:

- Issuer ID
- Plan and Benefits Data Administrative Data
- Accreditation Data
- Essential Community Providers (ECP)
- Data Network ID
- Service Area Prescription Drug

The Eligibility and Enrollment (E&E) functionality is used to verify an applicant's eligibility for health insurance, plan selection and enrollment through the Marketplace .E&E functionality within the FFM may collect the following types of information:

- Social Security Number
- Name
- Driver's License Number
- Mother's Maiden Name
- E-Mail Address
- Phone Numbers
- Military Status
- Taxpayer ID
- Mailing Address
- Employment Status
- Passport Number

Under the DE Proxy Program, DE Partners collect information directly from a consumer who chooses to provide their information to DE Partners. When working with consumers, DE Partners will enter consumer information into a HealthCare.gov application for eligibility and enrollment directly from the DE Partner Website. This Program enables consumers to complete their applications, receive eligibility results, and enroll in plans when working with DE Partners and without leaving DE Partner Website(s). The DE Partner Program functionality within FFM system may collect the following types of information:

- Social Security Number
- Name
- Driver's License Number
- Mother's Maiden Name
- E-Mail Address
- Phone Numbers
- Military Status
- Taxpayer ID
- Mailing Address
- Employment Status
- Passport Number

FFM collects the following information to manage authorized users access to the system:

- Name
- Business Email Address
- 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 Federally Facilitated Marketplace is made of the following functionalities:

Plan Management (PM) functions to capture and display insurer plan data for selection. The data collected supports plan certification, recertification, and the decertification processes. Data is used to monitor plan agreements, and maintain operational plan data. Data is used for rate review justification and to establish quality benchmarks and metrics for Qualified Health Plans (QHPs).

Eligibility and Enrollment (E&E) functions to determine eligibility in Medicaid, CHIP, or QHP based on Modified Adjusted Gross Income (MAGI) and other factors like disability. The data is used to determine eligibility and calculate the Advance Premium Tax Credits (APTCs) and Cost Sharing Reductions (CSR), and to determine eligibility for individual responsibility exemption. The system processes eligibility applications, and interfaces with the Data Services Hub (DSH) for validations where required. Changes in eligibility are also processed. E&E interfaces with DSH and States as required and process appeals and exemptions. Monthly and Annual Internal Revenue Service (IRS) Reporting is generated from the collected data.

Direct Enrollment (DE) functions allow DE Partners to collect E&E information from consumers and enter that information into a HealthCare.gov application. DE Partners are third party commercial entities that engage with consumers in applying for and enrolling in Qualified Health Plans by collecting E&E information and providing that information to HealthCare.gov. In accordance with the DE Proxy Partner Agreement with CMS, DE Partners are not permanently maintaining information. DE Partners may only collect the information for the purposes of facilitating consumer requests for eligibility, enrollment and for maintenance of QHP coverage. DE Partner data retention is governed by State/Federal Law, in addition to security and privacy control requirements outlined in the DE Proxy Partner Agreement with CMS.

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

Name

Driver's License Number

Mother's Maiden Name

E-Mail Address

Mailing Address

Phone Numbers

Military Status

Employment Status

Passport Number

Taxpayer ID

Other - Wage data; Tobacco use; Immigration Documents; Federal Tax Information (FTI); Pregnancy

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

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 a citizenship, immigration status, employment status, incarceration status, in support of eligibility determination in a Qualified Health Plan, Medicaid, or Children's Health Insurance Program (CHIP) program.

Exchange Minimum Functions: Consumer Assistance (45 CFR 155.205). Navigator Program (45 CFR 155.210). Agent Broker program (45 CFR 155.220). QHP certification (45 CFR 155.1000). Eligibility Appeals (45 CFR 155.355). Submission of Notices (45 CFR 155.230). Premium Payment (45 CFR 155.240). Exemption Determinations (45 CFR 155.605). Enrollment in QHPs (45 CFR 155.400). Eligibility Determinations (45 CFR 155.300, 155.305, 155.310). Oversight and Financial Integrity (45 CFR 155.200(c)). Establishment of Exchange network adequacy standards (45 CFR 155.1050). Quality Assessments, Disclosures & Data Reporting (45 CFR 155.200(d)). Administration of APTCs and CSRs (45 CFR 155.340). Coordination with Medicaid, Children's Health Insurance Program (CHIP), Benefit Health Plan (BHP) and Pre-existing Condition Insurance Plan (PCIP) (45 CFR 155.345)

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

Limited Personally Identifiable Information (PII) is also used in generation of meta-data for research, 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. 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 consumer's 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 1414; 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 an Insurance Plan.

Cite the legal authority to use the SSN.

Affordable Care Act (ACA), Section 1411
Affordable Care Act (ACA), Section 1414
42 U.S.C. Section 18081

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
42 U.S.C. Section 18081

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

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

- In-Person
- Hardcopy
- Email
- Online
- Other

Government Sources

- Within OpDiv
- State/Local/Tribal
- Other Federal Entities

Non-Governmental Sources

- Public
- Private Sector

Other

Identify the OMB information collection approval number and expiration date

OMB Control Numbers:

CMS Form Number: CMS-10400

Title: Establishment of Exchanges of Qualified Health Plans

OMB control number: 0938-1156

Expiration Date: 06/30/2019

Is the PII shared with other organizations?

Yes

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

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); DE Partners (eligibility and enrollment information).

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. 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), DE Partners agreements, 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.

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:

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

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

Health Insurance Exchange (HIX) Program, 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.

FFM does not provide a method for individuals to opt-out of the collection or use of PII because FFM requires PII to determine eligibility. The marketplace collects Personally Identifiable Information (PII) when a consumer clicks on "Apply for Coverage" at which point they will be asked to Identity Proof. Upon successful completion of Identity Proofing, the user can proceed to building their household, stating household income, and then continue onto plan compare and plan selection. 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. DE partners do not provide a method for individuals to opt-out of the collection or use of PII due to the fact that FFM requires PII to determine eligibility.

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:

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

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

Health Insurance Exchange (HIX) Program, 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, accuracy and relevancy.

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 an 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. Annually, 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 to determine eligibility or enroll in a qualified healthcare plan.

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 perform their maintenance and support activities, they may have access to PII. This access is limited to only those individual(s) that require this access to perform their job responsibilities.

Contractors:

Eligibility Support workers to help users with the eligibility and enrollment process. Direct contractors, in their role as an administrator, would have access to PII in accordance with that role.

Others:

Insurance Providers, DE Partners, Agents and Web Brokers to receive eligibility and 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 from 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.

FFM retains each collection of PI for the time period specified by the National Archive and Records Administration (NARA) approved records schedule in consultation with the records management officer to fulfill the purpose(s) identified in the notice or as required by law.

Per the current 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."

The CMS Records Schedule has been updated and includes a number of new schedules for different types of records (<https://www.cms.gov/Regulations-and-Guidance/Guidance/CMSRecordsSchedule/index.html>). You must use the schedules in those categories for the disposition of CMS's records. Please see below for a summary of the records dispositions and retention.

Leadership and Operations Records: Cutoff at the end of the calendar year. Transfer to the National Archives 15 year(s) after cutoff.

Administrative Management Records: Destroy no sooner than 7 years(s) after cutoff but longer retention is authorized. For "Routine Administrative Records", destroy no sooner than 3 years(s) after cutoff but longer retention is authorized. Financial Records: Destroy no sooner than 7 years(s) after cutoff but longer retention is authorized.

Enrollment Records: Destroy no sooner than 7 year(s) after cutoff but longer retention is authorized.

Beneficiary Records: Destroy no sooner than 10 year(s) after cutoff but longer retention is authorized.

Provider and Health Plan Record: Destroy no sooner than 7 year(s) after cutoff but longer retention is authorized.

Research and Program Analysis: Destroy 10 years(s) after cutoff or when no longer needed for agency business occurs, whichever is later.

Public Outreach and Engagement Records: Transfer to the National Archives 15 years(s) after cutoff. For "Photographs and Videos", transfer all photographs and videos, generated or accumulated pre-2013, and any related finding aids to the National Archives immediately upon approval of this schedule. Thereafter, cut off holdings in five-year block, and transfer along with any related finding aids to the National Archives when the oldest image in the block is five years old. All other Public Outreach and Engagement Record: Destroy when 1 year old, or when no longer needed for agency business, whichever is later.

Compliance and Integrity: Destroy no sooner than 7 year(s) after cutoff but longer retention is authorized.

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 Management 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 IBM Data Center in Culpepper, VA, and the DXC Technology (DXC) 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.

IBM is the service provider in the IBM Data Center and DXC is the service provider in the DXC 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 environment 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) for employees and non-consumers within FFM. FFM leverages Scalable Login System (SLS) to enable consumers to apply for and enroll in health insurance coverage. FFM users and Web services send user identity information to SLS for user authentication. Users and services are required to authenticate to establish their identity and role as an individual or connecting 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

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:

Other - Third-party tools are being used to gain visibility into when website traffic is building during busy (peak) periods. 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. Digital media is one of the cost-effective methods used to reach the uninsured consumer. Contracts are in place with companies to help connect interested consumers to Healthcare.gov, and to continuously measure and improve site performance and outreach efforts.

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?

Yes