US Department of Health and Human Services

Third Party Websites and Applications Privacy Impact Assessment

Date Signed:

October 20, 2017

OPDIV:

CMS

Name:

Direct Enrollment Partner Websites

TPWA Unique Identifier:

T-6759175-019631

Is this a new TPWA?

Yes

Will the use of a third-party Website or application create a new or modify an existing HHS/OPDIV System of Records Notice (SORN) under the Privacy Act?

No

If SORN is not yet published, identify plans to put one in place.

N/A

Will the use of a third-party Website or application create an information collection subject to OMB clearance under the Paperwork Reduction Act (PRA)?

No

Indicate the OMB approval number expiration date (or describe the plans to obtain OMB clearance).

N/A

Describe the plans to obtain OMB clearance.

N/A

Does the third-party Website or application contain Federal Records?

No

Describe the specific purpose for the OPDIV use of the third-party Website or application:

In response to stakeholder input and based on the experiences of the Federally-facilitated Exchanges (FFEs), CMS is broadening the customer service channels by which consumers may submit eligibility applications to the FFEs with the assistance of licensed health insurance issuers or web-based agents or brokers (web-brokers) (collectively, Direct Enrollment Partners or DE Partners). Specifically, CMS is implementing a program under which consumers may submit application information to a DE Partner's website and receive an eligibility determination from the FFE, without the need to be redirected to HealthCare.gov.

Have the third-party privacy policies been reviewed to evaluate any risks and to determine whether the Website or application is appropriate for OPDIV use?

Yes

Describe alternative means by which the public can obtain comparable information or services if they choose not to use the third-party Website or application:

Consumers may apply and shop for coverage on HealthCare.gov, via phone with the HealthCare.gov call center, or with the assistance of Navigators, certified application counselors, or non-web-based agents or brokers.

Does the third-party Website or application have appropriate branding to distinguish the OPDIV activities from those of nongovernmental actors?

Yes

How does the public navigate to the third party Website or application from the OPIDIV?

Consumers navigate to DE Partner websites by entering the address in their browsers. Consumers do not navigate to DE Partner websites directly from HealthCare.gov or any other CMS website.

Please describe how the public navigate to the thirdparty website or application:

An external hyperlink from an HHS Website or Website operated on behalf of HHS

If the public navigate to the third-party website or application via an external hyperlink, is there an alert to notify the public that they are being directed to anongovernmental Website?

No

Has the OPDIV Privacy Policy been updated to describe the use of a third-party Website or application?

Yes

Provide a hyperlink to the OPDIV Privacy Policy:

https://www.healthcare.gov/privacy/

Is an OPDIV Privacy Notice posted on the third-part website or application?

Yes

Is PII collected by the OPDIV from the third-party Website or application?

Yes

Will the third-party Website or application make PII available to the OPDIV?

Yes

Describe the PII that will be collected by the OPDIV from the third-party Website or application and/or the PII which the public could make available to the OPDIV through the use of the third-party Website or application and the intended or expected use of the PII:

Consumers who wish to apply for coverage under a qualified health plan (QHP) through the Federally-facilitated Exchange (FFE) with the assistance of a DE Partner may submit to the DE Partner information, including PII, required to complete an FFE application for coverage. With the consumer’s specific consent, the DE Partner will collect this information through their website and transmit it to CMS in its capacity as operator of the FFE and provider of eligibility and enrollment services to State-based Exchanges that rely on the FFE’s information technology platform for their eligibility and enrollment functions (SBE-FPs).

The FFE will use PII transmitted from DE Partners to make eligibility determinations for insurance affordability programs, which include enrollment in a QHP, Medicaid, or Children's Health Insurance Program (CHIP), as well as eligibility for advance payments of the premium tax credit and cost sharing reductions. More specifically, the FFE will use this information to validate an individual's identity and for determining compliance with eligibility requirements for enrollment in a QHP. The FFE may also use the PII for program support for business operations of Plan Management, Eligibility and Enrollment (including integration with Appeals), and Financial Management.

These functions include, but are not limited to, using email addresses, mobile and residential phone numbers, and other contact information to communicate with consumer applicants regarding their application, QHP coverage, or other issues. Complete, detailed information regarding how the FFE will use consumer PII provided by DE Partners on behalf of consumers can be found in the HealthCare.gov Privacy Policy (https://www.healthcare.gov/privacy/) and Privacy Act Statement (https://www.healthcare.gov/individual-privacy-act-statement/).

Below are the PII elements which consumers may make available to CMS through DE Partner websites:

Social Security Number
Date of Birth
Photographic Identifiers
Name
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
Pregnancy status
Tobacco Use

Describe the type of PII from the third-party Website or application that will be shared, with whom the PII will be shared, and the purpose of the information sharing:

In order to verify and process the FFE applications that will be populated by DE Partners, determine eligibility, and operate the FFE, CMS will need to share selected information outside of CMS, including to:

Other federal agencies, (such as the Internal Revenue Service, Social Security Administration and Department of Homeland Security), state agencies (such as Medicaid or CHIP) or local government agencies. CMS may use the information you provide in computer matching programs with any of these groups to make eligibility determinations, to verify continued eligibility for enrollment in a qualified health plan or other insurance affordability program, or to process appeals of eligibility determinations.

Other verification sources including consumer reporting agencies

Employers identified on applications for eligibility determinations

Applicants/enrollees, and authorized representatives of applicants/enrollees

Agents, Brokers, and issuers of Qualified Health Plans, as applicable, who are certified by CMS who assist applicants/enrollees, namely DE Partners

CMS contractors engaged to perform a function for the Exchange

Anyone else as required by law or allowed under the Privacy Act System of Records Notice associated with this collection (CMS Health Insurance Exchanges System (HIX), CMS System No. 09-70-0560, as amended, 78 Federal Register, 8538, March 6, 2013, and 78 Federal Register, 32256, May 29, 2013).

If PII is shared, how are the risks of sharing PII mitigated?

CMS has in place multiple safeguards to mitigate the risk associated with PII sharing. Amongst

Will the PII from the third-party website or application be maintained by the OPDIV?

Yes

Describe how PII that is used or maintained will be secured:

CMS ensures that all information received from DE Partners is stored in the CMS Health Insurance Exchanges System (HIX), the system of record for Exchange eligibility and enrollment information. The FFE maintains compliance with CMS's Acceptable Risk Safeguards (ARS) and all relevant federal privacy requirements. CMS's ARS compliance ensures that the information in the FFE system is in compliance with all relevant FISMA, NIST and FIPS guidelines and standards.

What other privacy risks exist and how will they be mitigated?

CMS approves and registers DE Partners to collect information directly from consumers to be transmitted to the FFE for an eligibility determination. CMS's relationship with the DE Partners presents the risk that consumers may erroneously expect that their personal information will be safeguarded by DE Partners exactly as it is when in the hands of a federal agency. Because consumers will be able to obtain an eligibility determination from the FFE without ever visiting the HealthCare.gov website, there is also risk that consumers will assume that the DE Partner's site and the PII entered therein, will be maintained and controlled by a government agency and with the same level of security standards and privacy protections.

DE Partner sites will be appropriately branded to mitigate risk that consumers believe they are entering their PII directly into a government website. To mitigate the risk that consumers will expect their data to be used or disclosed exactly as it would have been by the FFE, each DE Partner site will display a CMS-approved Privacy Notice on their websites that contains (i) An explanation that the Website or application is not government-owned or government-operated; (ii) An indication of how the Federal Exchange will maintain, use, or share PII received in an Exchange application; (iii) An explanation that by using the DE Partner's website to communicate with the Federal Exchange, individuals will be providing nongovernmental third-parties with access to PII; (iv) A link to the official HealthCare.gov website; and (v) A link to the HealthCare.gov Privacy Policy.

DE Partners will have access to sensitive PII that is not traditionally required on applications for health insurance in the individual market, including but not limited to income, smoking status, pregnancy status, and a listing of members of applicant households. Also, if the DE Partner obtains informed consent, the consumer may provide additional information to the DE Partner. DE Partners also will have access to information contained in FFE-produced eligibility determination notices that will contain consumer PII and other sensitive consumer information (e.g., the fact that the information the consumer provided to the DE partner did not match with that in federal records). To mitigate risk that such information is used improperly or for purposes not authorized by federal law, each DE Partner must sign a written agreement binding itself, its employees, and other downstream entities to specific privacy and security standards designed to protect consumer PII (the DE Partner Agreement). Each DE Partner will also obtain consumers' specific consent allowing the DE Partner to submit the consumer's PII to the FFE and to have access to the consumer's FFE eligibility determination(s).

The DE Partner Agreement also requires that DE Partners appropriately secure PII and limit the use and disclosure of consumer PII submitted to and received from the FFE to only those lawful purposes outlined in the DE Partner Agreement that are necessary to assist consumers with applying for FFE coverage and other insurance affordability programs. DE Partners are also prohibited from selling or sharing consumer PII submitted to or received from the FFE. In order to mitigate risks to the security and confidentiality of consumer PII, DE Partners are required to implement and provide audit results for more than 100 security and privacy controls which are based on FISMA, NIST and FIPS. These security and privacy controls are intended to ensure that consumer PII is housed in a secure operating environment inclusive of systems, organizational policies and procedures and operational processes and internal controls. Further the referenced controls require that information only be used by authorized individuals and that access to PII is on a need to know basis only for transacting eligibility and exchange business operations. The terms of the DE Partner agreement prohibit those partners from using the subject information to further non-related commercial or other corporate interests including cross-selling, marketing or advertising of other products. DE Proxy partner agreements may be terminated any time by CMS should inappropriate or disclosure be discovered or reported to CMS.

The DE Partner Agreement, as well as federal law, authorizes CMS to immediately terminate the DE Partner's authority to collect, use, or disclose PII from Exchange applicants based on serious DE Partner misconduct in relation to PII, including any failure to adequately use or secure PII. Consumers can also contact the FFE call center to report any concerns related to their PII and DE Partners.

CMS and DE Partners take a number of steps to ensure the security and confidentiality of data as it moves between DE Partners and the FFE. This includes using the TLS 1.2 cryptographic protocol leveraging the SHA-256 cryptographic hash. This communication method ensures the security, privacy, integrity and authenticity of the communication.

DE Partners may deliver a consumer applicant's PII into the HealthCare.gov application from its website to the FFE platform (HealthCare.gov) using automation software. This automation software carries the information from a partner's website to healthcare.gov through a specialized proxy user interface that implements the same business logic, data editing and workflow as the consumer facing healthcare.gov website. Though the information will be subject to the same data verification and validation routines as normal human input, there is some residual risk that consumer PII could be mistranslated between a DE Partner's system and the FFE due to problems with a partner's automation software. Such errors could result in delayed or erroneous eligibility determinations. Erroneous eligibility determination can also result in unanticipated tax liability for consumers who are found eligible for and receive advance premium tax credits based on erroneous application information.

To mitigate these risks, CMS requires each DE Partner to engage an independent, third party auditor to conduct an operational readiness review (ORR), one of the goals of which is to ensure that information is accurately conveyed to the FFE. Consumers also may challenge erroneous eligibility determinations through the FFE's appeals process.

DE Partner websites may utilize a variety of information technology/web tools that collect and use information about a consumer's visit to the website to, among other things, improve user experience, understand a user's preference, measure the efficacy of marketing efforts, and for other business functions. These tools may collect various types of non-identifiable information, such as the date and time of a consumer's visit, as well as the consumer's IP or Mac address (an IP or internet protocol address is a number that is automatically given to a computer connected to the Web), browser, device, device screen size, operating system, geolocation (including precise locations), and language. DE Partners may not store this information at all, or they may store it indefinitely.

DE Partner websites may use tracking information to make it easier for consumers to use dynamic features of web pages. They may also use this information to collect information about consumers' perceived interests in insurance-related and non-insurance-related products or services so that the DE Partner or its partners can arrange for advertisements regarding these products or services to display on other sites consumers visit on the Internet.

Currently, DE Partners use a variety of web tools, including website analytics tools like Google Analytics, IIS Logs, Mixpanel, server logs, HTML5, Adobe Site Catalyst, JavaScript, Raygun, and Pardot. Website analytics tools collect basic site usage information such as how many visits the website receives, the pages visited by consumers, time spent on the site, the number of return visits to the site, the approximate location of the device used to access the site, types of devices used, etc. This information is then used for various purposes in connection with the website, including but not limited to monitoring site stability, measuring site traffic, optimizing site content, and improving the consumer experience.

DE partners may also use third party applications to support digital advertising and marketing activities, including, but not limited to, Adobe Marketing Cloud, Facebook Ads, Good Adwords, Google Tag Manager, and Adroll. These applications may be supported by DE Partners' installation on their websites of web tools such as cookies (session and persistent) and pixels that track user activity on DE Partner websites and across the Web. DE Partners might also match or link non-PII tracking data with other data sources to, among other things, expand and analyze its records, identify new customers, and provide products and services that may be of interest to consumers.

DE Partners may aggregate tracking data and analyze it in many combinations and across many dimensions for various purposes, including, but not limited, to optimizing web performance, improving consumer experience on its website, and generating reports on consumer activity on their websites. DE Partners also may use this information to track and reduce occurrences of bugs and site crashes, increase site performance, and optimizing user experience for the most commonly-used devices.

For example, DE Partners may use data regarding web viewing behaviors or application use gathered to predict consumer preferences or interests. This 'targeted advertising' (also known a online behavioral or interest-based advertising) uses data collected from a particular computer or device regarding a consumer's web viewing behaviors or application use to predict user preferences or interests. The DE Partner can then have ads delivered to computers or devices based on the user's preferences or interests inferred from his or her web viewing behaviors or application use.

To mitigate the risk that consumer information, including PII and non-PII tracking information, will be used in a manner undesirable to consumers, each DE Partner displays a privacy notice on their website explaining how consumer information is (or may be) used or disclosed. Moreover, information about DE Partner sites and their relationship to HealthCare.gov, as well as how HealthCare.gov will use or disclose consumer application information received from DE Partners is included in the HealthCare.gov Privacy Policy. To ensure that consumer PII used to populate an Exchange application is protected in accordance with federal law, the DE Proxy Agreement prohibits DE Partners from using web tools to collect, disclose or otherwise use PII consumers entered into DE Partner websites for purposes of submitting an Exchange application for any purpose unrelated to applying for Exchange coverage or other insurance affordability programs. Thus, these web tools generally may track consumer activities on DE Partner website pages that collect PII necessary for an Exchange application, but these tools will not capture PII entered into a DE Partner's web application.

Some DE Partners also offer website visitors the option to opt out of specific marketing programs using applications such as the TRUSTe opt-out site. Other DE Partners may not offer specific options allowing consumers to opt out of internet tracking. However, consumers may take steps to opt out of tracking, including, but not limited to, setting their browsers to reject cookies, or clearing their browser's cache and cookie history which can prevent tracking using cookies, but may disable some site functionality.

CMS will conduct periodic reviews of DE Partner's privacy policies and practices to ensure that they continue to align with agency objectives, federal law, and the DE Partner Agreement, and that DE Partners' practices do not present unreasonable or unknown risks to consumer privacy. DE Partner websites and their supporting information technology platforms will also be subject to periodic audits by CMS.