

US Department of Health and Human Services

Third Party Websites and Applications Privacy Impact Assessment

Date Signed:

September 07, 2018

OPDIV:

CMS

Name:

YAHOO

TPWA Unique Identifier:

T-6911468-818651

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.

Not Applicable.

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).

Expiration Date: 1/1/01 12:00 AM

Describe the plans to obtain OMB clearance.

Explanation: Not Applicable.

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:

CMS uses Yahoo Gemini to place digital advertisements on Yahoo in order to reach new users and provide information to previous visitors to a CMS website. A common example are the ads a person sees when they are searching for information on Yahoo. Conversion tracking will be in place to enable Yahoo Gemini to measure the activity of consumers on a CMS website who were driven to the website as a result of clicking on a CMS website's digital ad that was delivered by Yahoo Gemini.

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:

If users do not want to interact with Yahoo Gemini or the CMS website ads Yahoo Gemini may deliver, but still want to obtain health insurance or information through a CMS website, they can obtain comparable information by visiting the CMS website directly. The public can also call into the call center to obtain information about comparable information generally offered through the CMS website or CMS website advertisements served by Yahoo Gemini.

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?

The public does not navigate to Yahoo's website search page from a CMS website. Rather, the public may independently navigate to Yahoo to perform web searches.

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

The public may independently navigate to Yahoo to perform web searches.

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:

This is the privacy policy for all CMS website <https://www.cms.gov/privacy/> unless one of the following is noted <https://www.healthcare.gov/privacy/> and <https://www.medicare.gov/privacy-policy/index.html>.

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

No

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

No

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

No

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:

Not applicable. CMS does not collect any PII through the use of Yahoo Gemini.

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:

Not applicable. No PII is shared by Yahoo Gemini.

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

Not applicable.

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

No

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

Not applicable.

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

CMS will use Yahoo Gemini in a manner that will support CMS' mission to inform users of CMS services, while respecting the privacy of users. CMS will conduct periodic reviews of Yahoo's privacy practices to ensure its policies continue to align with agency objectives and privacy policies and do not present unreasonable or unmitigated risks to user privacy. CMS employs Yahoo Gemini solely for the purposes of improving CMS' services and activities online related to CMS websites.

Potential Risk:

As described in our Privacy Policy, we use persistent cookies on CMS websites to support our digital advertising outreach, and these cookies may be stored on a user's local browser for a limited time. Yahoo Gemini advertising cookies used to provide CMS with the Yahoo Gemini advertising services are set to expire within two years. The use of persistent cookies presents the risk that a user's activity on the internet may be tracked across multiple sites and over time, compromising user privacy. The use of persistent cookies for an extended period of time presents the risk that more information will be collected about users than is necessary to fulfill the purpose of the collection, further compromising user privacy.

Mitigation:

The CMS business need for advertising cookie retention longer than one year is to accurately target users over multiple open enrollment periods.

CMS websites and Yahoo offer users notice in their website privacy policies about the use of persistent cookies, the information collected about users, and the data gathering choices users have.

CMS uses a Tealium iQ Privacy Manager to give users control over which tags or cookies they want to accept from a CMS website.

Yahoo offers users the ability to opt-out of having Yahoo target them using cookies by opting out through an opt-out button on http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/details.html; and opt-out options on websites of industry self-regulation programs respected by Yahoo, including the Digital Advertising Alliance and the Network Advertising Initiative.

Potential Risk:

The ability of Yahoo to record, analyze, track, and profile the activities of internet users with data that is both personally identifiable and data that is not personally identifiable presents risk that data about CMS website users could be used to personally identify CMS website users or could otherwise be misused. In addition, Yahoo displays targeted advertisements based on personal information.

Mitigation:

CMS does not receive any personally identifiable information from Yahoo, and aggregated reporting data received from Yahoo is available only to CMS managers, and other designated federal staff and contractors who need this information to perform their duties.

Potential Risk:

CMS uses Yahoo Gemini advertising services for conversion tracking. These advertising techniques use cookies to track users across multiple sites and over time, and the resulting combined information could be used to compromise user privacy by revealing patterns in behavior that the user may not want to disclose to CMS or to Yahoo Gemini for provision of advertising services to other Yahoo Gemini customers who may wish to target the health care sector.

Conversion tracking allows advertisers to measure the impact of their advertisements by tracking whether users who view or interact with an ad later visit a particular site or perform desired actions on such site, such as enrolling in health care coverage on a CMS website.

Conversion tracking enables CMS to improve the performance of ads by delivering them to relevant audiences and measuring their effect.

Mitigation:

To mitigate this risk, CMS uses a Tealium iQ Privacy Manager to give users control over which tags or cookies they want to accept from a CMS website, including whether they want to accept advertising cookies.

CMS observes the “Do Not Track” browser setting for digital advertising that uses retargeting. If “Do Not Track” is set before a device visits a CMS website, third party retargeting tools will not load on the site. If you did not have “Do Not Track” on before visiting a CMS website, there are other mitigation strategies, such as the Tealium iQ Privacy Manager mentioned above. For more information on Do Not Track or information on how to set the “Do Not Track” setting in a browser, go to the “Do Not Track” website at <http://donottrack.us/>.