

US Department of Health and Human Services

Third Party Websites and Applications Privacy Impact Assessment

Date Signed:

September 24, 2015

OPDIV:

CMS

Name:

Optimizely

TPWA Unique Identifier:

T-8824339-672155

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

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

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:

Optimizely is a technology platform that supports customer experience optimization. Optimizely provides the ability to conduct A/B or split screen testing, multipage and multivariate testing and is used for making data-driven decisions. The CMS staff analyze and report using the collected data from Optimizely. The reports are available only to CMS managers, teams who implement Federally Facilitated Marketplaces programs represented on HealthCare.gov, members of the CMS communications and web teams, and other designated federal staff and contractors who need this information to perform their duties.

CMS uses this information to determine what types of changes need to be made to HealthCare.gov to improve the user experience for visitors by delivering different user interfaces to consumers and observing which allows consumers to perform a task easier.

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 consumers do not want Optimizely to collect information related to their visits to HealthCare.gov, consumers can use the paper application, use the call center, or visit an agent or broker to enroll in coverage. In addition to these options, a consumer can use the Tealium iQ Privacy Manager on HealthCare.gov's privacy page and "opt out" of having data collected about them by Optimizely. Alternatively, a consumer can disable their cookies, and/or block this functionality in the browsers Flash player settings manager, Global Privacy Settings panel, if they do not want their information to be collected.

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

No

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

The public does not navigate to Optimizely. Optimizely works in the background .

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

The public does not navigate to Optimizely. Optimizely. works in the background.

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?

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:

CMS does not collect any PII through the use of Optimizely.

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:

PII is not stored or shared.

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

No PII is shared with CMS.

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 Optimizely in a manner that protects the privacy of consumers who visit HealthCare.gov and respects the intent of HealthCare.gov users. CMS will conduct periodic reviews of Optimizely'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 consumer privacy. Optimizely is employed solely for the purposes of improving CMS' services and activities online related to operating HealthCare.gov. Information collected by Optimizely is created and maintained by Optimizely .

Risk #1:
Optimizely's tools use persistent cookies on HealthCare.gov and can be stored on a user's local system. The maximum length of time that Optimizely cookies exist on a user's local system is two years. This timeframe helps CMS to evaluate year to year and target tests to audiences based on actions taken in a prior year's open enrollment period.

Mitigation:
Users can opt-out of Optimizely by using the Tealium iQ Privacy Manager on HealthCare.gov's privacy page. Alternatively, a consumer can disable their cookies, if they do not want their information to be collected. Optimizely's privacy policies, notices from HealthCare.gov and Optimizely informing consumers of its privacy policies, and the ability of consumers to opt out of providing their information to Optimizely, mitigate risks to consumer privacy.

For consumers that do not opt out, CMS has configured its use of Optimizely to mask IP addresses before being stored to add additional safeguards to ensure that this data cannot be connected with other data.

Risk #2:
In addition to using persistent cookies, Optimizely uses local object storage such as HTML5.

Mitigation:
Local object storage, can store data within the user's browser. Local object storage is more secure, and large amounts of data can be stored locally, without affecting website performance. Unlike cookies, the storage limit is far larger and information is never transferred to the server. Users can opt-out of Optimizely by using the Tealium iQ Privacy Manager on HealthCare.gov's privacy page. Alternatively, users have the ability to block this functionality in the browsers Flash player settings manager, Global Privacy Settings panel.

Risk #3:
CMS also recognizes that if Optimizely is not implemented correctly in relation to HealthCare.gov, personal information could be collected about HealthCare.gov visitors.

Mitigation:
To mitigate this risk, CMS only allows a limited number of trained and credentialed staff or contractors to implement Optimizely.