

US Department of Health and Human Services

Third Party Websites and Applications Privacy Impact Assessment

Date Signed:

April 04, 2024

OPDIV:

CMS

Name:

LaunchDarkly

TPWA Unique Identifier:

T-6045138-311777

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.

null

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: null

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:

The Centers for Medicare & Medicaid Services (CMS) uses LaunchDarkly Feature Management and Experimentation to support CMS' websites, including CMS.gov, Medicare.gov, HealthCare.gov, CuidadoDeSalud.gov, Medicaid.gov, InsureKidsNow.gov, and various subdomains of the above top-level domains (TLDs). These TLDs are hereafter referred to as "CMS' websites." LaunchDarkly is a technology platform that supports feature management to improve customer experience. CMS uses LaunchDarkly feature management to improve user's website experiences and reduce risk with new functionality releases. Developers configure a LaunchDarkly Software Development Kit (SDK) to collect and transmit data about end-users to LaunchDarkly for the purpose of feature targeting. LaunchDarkly enables CMS to deploy persistent experiences, which can be delivered to users with specific behavioral profiles. The CMS staff analyzes and reports on the aggregated user-interaction data collected by LaunchDarkly. The reports are available only to CMS managers, teams who

implement CMS represented on CMS' websites, 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 CMS' websites 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 LaunchDarkly to collect information related to their visits to CMS' websites, consumers can use other means of interaction, including but not limited to paper applications, call centers, or in-person assisters. In addition to these options, a consumer can use the Tealium IQ Privacy Manager on CMS' websites privacy page(s) and "opt out" of having data collected about them by Launch Darkly. Alternatively, a consumer can disable their browser cookies if they do not want their information to be collected. Consumers can follow instructions published at <https://launchdarkly.com/policies/privacy/>.

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?

Other...

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

Not applicable. The public does not navigate to LaunchDarkly. LaunchDarkly is only accessible by CMS/HHS software developers and admins that have completed the necessary access and identity management steps.

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?

null

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.cms.gov/privacy-policy/>

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:

LaunchDarkly does not collect any PII from the public directly, and CMS does not gather any PII from LaunchDarkly.

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:

N/A

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

N/A

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 uses LaunchDarkly in a manner that protects the privacy of consumers who visit CMS' websites and respects the intent of visitors. CMS conducts periodic reviews of LaunchDarkly'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. LaunchDarkly is employed solely for the purposes of improving CMS' services and activities online related to operating CMS' websites.

Potential Risk: In using LaunchDarkly to manage features, CMS applications send information to LaunchDarkly about the current request context in order to determine which features to enable or disable. Which information is provided about the current request context is at the discretion of CMS application developers and is kept to only the required minimum for a specific use case.

Mitigation: Policies and procedures are created and communicated to clarify information that will not identify a person is only acceptable to send to LaunchDarkly for feature evaluation and experimentation. If consumers do not want Launch Darkly to collect information related to their visits to CMS' websites, consumers can use other means of interaction, including but not limited to paper applications, call centers, or in-person assisters. In addition to these options, a consumer can use the Tealium IQ Privacy Manager on CMS' websites privacy page(s) and "opt out" of having data collected about them by Launch Darkly. Alternatively, a consumer can disable their browser cookies if they do not want their information to be collected. Consumers can follow instructions published at <https://launchdarkly.com/policies/privacy/>.

Another way this privacy risk is mitigated is through the strong protections of the privacy program of LaunchDarkly, which is audited against both ISO 27001 and NIST 800-53 privacy controls annually. These protections include data confidentiality and integrity controls, data retention and deletion controls, and privacy by design principles embedded in the software development process.

Potential Risk: LaunchDarkly transfers browser information (cookies, user agent, and local storage) when CMS uses the LaunchDarkly JavaScript or React client-side Software Development Kit (SDK) which contacts LaunchDarkly directly.

Mitigation: Users can opt-out of LaunchDarkly by using the Tealium IQ Privacy Manager on CMS' websites privacy pages. Alternatively, a consumer can disable their cookies, if