US Department of Health and Human Services

Third Party Websites and Applications Privacy Impact Assessment

Date Signed:

September 07, 2018

OPDIV:

CMS

Name:

New Relic

TPWA Unique Identifier:

T-3914791-979549

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:

The Health Insurance Marketplace uses New Relic Browser to collect, report, and analyze visitor interactions on CMS' websites, including CMS.gov, Medicare.gov, MyMedicare.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." CMS uses this information to help find performance issues with the website as well any application errors that might fire during a consumer's browsing session.

The CMS staff analyze and report using the collected data from these tools. The reports are available only to CMS managers, teams who implement the CMS programs 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.

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 New Relic Browser 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, consumers can use the Tealium IQ Privacy Manager on each CMS website's privacy page and opt out of having data collected about them by New Relic Browser.

Alternatively, a consumer can disable their cookies 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 OPIDIV?

Not applicable - the public does not navigate to New Relic Browser. New Relic Browser works in the background.

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

Not applicable - the public does not navigate to New Relic Browser. New Relic Browser 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.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:

CMS does not collect any PII through the use of New Relic Browser.

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

Information collected by New Relic Browser is created and maintained by New Relic Browser.

Potential Risk:

The New Relic Browser tools use persistent cookies on CMS' websites and can be stored on a user's local system. Users approximate geographic location is collected by New Relic Browser based on the IP address of the user's local system. Other information collected consists of Page Views, JavaScript Errors, Browser, Session Traces and other information specific to the health and performance of CMS' websites.

Mitigation:

New Relic Browser uses session cookies that expire at the end of a user's browsing session. New Relic Browser's privacy policies, notices from CMS' websites, information published by New Relic Browser about its privacy policies, and the ability for consumers to opt-out of providing their information to New Relic Browser maximizes consumers' abilities to protect their information and mitigate risks to their privacy.

CMS will not deploy the New Relic Browser tool if the website is not using Tealium iQ.

Potential Risk:

CMS also recognizes that if New Relic Browser is not implemented correctly in relation to CMS' websites, personal information could be collected about visitors.

Mitigation:

Therefore, to mitigate this risk, CMS only allows a limited number of trained and credentialed staff or contractors to implement New Relic Browser.