US Department of Health and Human Services

Third Party Websites and Applications Privacy Impact Assessment

Date Signed:

May 13, 2022

OPDIV:

CMS

Name:

Qualtrics 2022

TPWA Unique Identifier:

T-7749648-608534

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).

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

Describe the plans to obtain OMB clearance.

Explanation: 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:

The Centers for Medicare & Medicaid Services (CMS) uses Qualtrics, an Experience Management platform, to gather feedback from visitors to 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), to gauge overall satisfaction with the website and to find out how to improve the customer experience. These TLDs are hereafter referred to as "CMS' websites." Feedback collected is general consumer feedback information via multiple-choice and open-ended questions such as, "What is your feedback about?" "How can we improve this page?" and "Did you find the information helpful?" Consumers provide feedback through online surveys facilitated by the Qualtrics tool. The Qualtrics platform gathers feedback from CMS website visitors to gauge overall satisfaction with the website to build an omni-channel voice of the customer (VoC) program in an effort to improve the consumer experience.

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 a member of the public chooses not to provide feedback, there will be no impact to their experience on the site. The technology is used to improve the customer experience.
Survey questions are used to improve the customer experience and are not applicable to alternative application channels.

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?

Incorporated or embedded on HHS Website

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

The public does not navigate to Qualtrics as the application is embedded into CMS website pages.

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?

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:

The personally identifiable information (PII) is collected to provide for an enriched and personalized user experience. A primary consideration of this technology is the ability to identify the same user across multiple devices and across multiple sessions. To achieve this, a Tealium ID must be captured.Behavioral data from one session/device is leveraged to provide an improved and consistent user experience in future sessions/devices. Users may voluntarily include PII in open-ended questions similar to “How can we improve this page?”

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:

The personally identifiable information (PII) collected is a Tealium ID. Qualtrics is used in concert

with Tealium as the only third-party vendors designated to store Tier-3 level personally identifiable information. Data within Qualtrics is not accessible by personnel from Tealium and vice versa. Only designated federal staff and contractors who need this information to perform their duties have access to this data. No other third party organization will have access to the information collected.

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

Access to the platform is managed by role-based permissioning to ensure visibility is limited to

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:

Qualtrics is FedRamp Authorized. FedRAMP is the gold standard of U.S. government security compliance, with over 300 controls based on the highly-regarded NIST 800-53 that requires constant monitoring and periodic independent assessments. For more information on the Qualtrics FedRamp Authorization, see: https://marketplace.fedramp.gov/#!/product/qualtrics-xm-platform?sort=productName

All response data resides in Amazon Web Services (AWS) GovCloud (environment is specific only for Federal customers), and data is protected by disk level encryption and database encryption. AWS GovCloud has an existing ATO (Authority to Operate) under FedRAMP, which gives Government agencies the ability to leverage AWS GovCloud for sensitive workloads.

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

CMS will use Qualtrics 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 Qualtrics' 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. Qualtrics is employed solely for the purposes of improving CMS' services and activities online related to operating CMS websites such as CMS.gov, Medicare.gov, MyMedicare.gov, HealthCare.gov, CuidadoDeSalud.gov, Medicaid.gov, InsureKidsNow.gov, and various subdomains of the above top level domains.

Information collected by Qualtrics is created and maintained by Qualtrics.

Potential Risk:
Persistent cookies are used with third-party tools on CMS' websites and can be stored on a user's local browser. Qualtrics cookies are stored for one year.

Mitigation:
Qualtrics' privacy policies, notices from CMS' websites, information published by Qualtrics about its privacy policies, and the requirement for users to opt-in to receive an enriched and personalized user experience before Tier 3 data collection occurs, or the ability for consumers to opt-out of providing their information to Qualtrics maximizes consumers' ability to protect their information and mitigate risks to their privacy.

Additionally, Qualtrics' surveys are voluntary and consumers can choose not to participate in surveys. CMS has configured its use of Qualtrics to mask IP addresses before being stored to add additional safeguards to ensure that this data cannot be connected with other data in order to identify a consumer who completes a survey supported by Qualtrics. In some cases, consumers may inappropriately add PII informationin the free text field of surveys. A query is implemented in the system to redact the inappropriate PII when included in the response of a free text field.

CMS will not deploy the Qualtrics tool if the website is not using Tealium iQ.

Potential Risk :

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

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