US Department of Health and Human Services

Third Party Websites and Applications Privacy Impact Assessment

Date Signed:

February 07, 2022

OPDIV:

CMS

Name:

Hotjar

TPWA Unique Identifier:

T-5339607-964609

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)?

Yes

Indicate the OMB approval number and approval number expiration date (or describe the plans to obtain OMB clearance).

OMB Approval 938-1397

Indicate the OMB approval number expiration date (or describe the plans to obtain OMB clearance).

Expiration Date: 7/31/24, 12:00 AM

Describe the plans to obtain OMB clearance.

Explanation: The Quality Payment Program (QPP) website is visited by thousands of users each day with various objectives including, but not limited to, checking clinician eligibility status, choosing and downloading measure specification forms, learning about reporting requirements, submitting data, and reviewing feedback. These site visitors may include, but are not limited to, clinicians, office administrators, hospital administrators, third-party intermediaries, and professional association staff. These visitors rely on the content on the website to be clear, accessible, and up to date to meet or support clients in meeting CMS regulatory standards and participate in the Quality Payment Program.

The QPP Site Intercept Survey is designed to collect feedback in real time from site visitors regarding their satisfaction with the website and their goals when visiting the website. The survey will be available on the QPP website to provide visitors the opportunity to share their experience throughout the year. This information will allow the QPP Human-Centered Design (HCD) Team to assess visitor needs and satisfaction to plan enhancements to the digital experience. Information will be collected through a combination of questions with pre-set responses and open text fields.

Demographic data will be collected to better understand the type of user and segment findings, but no Personally Identifiable Information will be included in the Site Intercept Survey. Estimated time to complete survey is less than 5 minutes.

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 purpose for this tool is to:

visually represent where users click, hover, and scroll on our site (Heatmaps); create and use targeted surveys to get a better understanding of our users (Surveys).

Heatmap: Utilizing Hotjar's Heatmap functionality will allow the Quality Payment Program's (QPP) Human-Centered Design team to visualize user behavior by viewing "hot spots" on screenshots of our site content. In summary, configuration and implementation of Hotjar's Heatmap functionality on QPP will provide the following benefits:

Discover what attracts attention - See the elements of a page that capture attention so we can deliver the right information to our users at the right time;
See where user attention drops - Remove the guesswork and learn where users drop off our page. Discover practical ways design and copy can keep users' attention; and
Compare engagement on different devices - Spot problems on mobile, like unclickable elements or broken forms, by switching between desktop, tablet, and mobile views.

Surveys: Utilizing Hotjar's Survey functionality will allow QPP's Human-Centered Design team to bring the voice of the customer to our decision making via an onsite survey. In summary, configuration and implementation of Hotjar's Survey functionality on QPP directly supports the overarching CCSQ Customer Satisfaction (CSAT) initiative being led by the HCD Centers of Excellence. Specifically, the HCD Team has developed a customer satisfaction survey that will prompt users of the unauthenticated Frontend to answer a few questions about their experience, once per quarter.

The survey has been submitted for PRA approval.

A TPWA is being completed to ensure that the configuration, implementation and usage of Hotjar protects the privacy of our end users.

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:

Through the use of Privacy Manager the public will have the option to block Hotjar, thus preventing the government from having the ability to collect the corresponding information, while still allowing the QPP site to function as originally intended.

As referenced below in Response number 13, Hotjar is embedded into the QPP Website and is imperceptible by end users.

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?

Incorporated or embedded on HHS Website

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

N/A. As referenced above in Response number 13, Hotjar is embedded into the QPP Website and is imperceptible by end users.

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?

Yes

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://qpp.cms.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:

N/A. Neither the OpDiv or the application will be collecting PII.

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. Neither the OpDiv or the application will be collecting PII.

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

N/A. Neither the OpDiv or the application will be collecting PII.

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:

N/A. Neither the OpDiv or the application will be collecting PII.

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

CMS will use Hotjar in a manner that protects the privacy of consumers who visit qpp.cms.gov and respects the intent of qpp.cms.gov users. CMS will conduct periodic reviews of Hotjar'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.

Hotjar is employed solely for the purposes of improving CMS services and on-line activities related to operating qpp.cms.gov.

Risk number 1:
Persistent cookies are used by Hotjar on qpp.cms.gov and can be stored on a user’s local browser.

For heatmapping and session recording, the main cookie stores the universally unique identifier (UUID) for 365 days. All other cookies expire after 30 minutes or the end of the session and are mostly used to monitor that a user is still active. A full list of cookies is provided here: https://help.hotjar.com/hc/en-us/articles/115011789248-Hotjar-Cookie-Information

Mitigation:
Hotjar's privacy policies, notices from qpp.cms.gov, information published by Hotjar about its privacy policies, and the ability for consumers to opt-out of having their information collected by Hotjar maximizes consumers' ability to protect their information and mitigate risks to their privacy.

Additionally, the Hotjar surveys on qpp.cms.gov are voluntary and consumers can choose not to participate in surveys. CMS has configured its use of Hotjar to mask IP addresses before being stored to ensure that this data cannot be connected with other data in order to identify a consumer who completes a survey. In some cases, consumers may volunteer PII information in the free text field of surveys. If CMS staff see this occur, they will delete this information from the system.

Finally, consumers can also use the Tealium iQ Privacy Manager on qpp.cms.gov privacy page and "opt out" of having data collected about them by Hotjar.