US Department of Health and Human Services

Third Party Websites and Applications Privacy Impact Assessment

Date Signed:

December 23, 2020

OPDIV:

CMS

Name:

Tealium

TPWA Unique Identifier:

T-4740171-610022

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: N/A

Does the third-party Website or application contain Federal Records?

Yes

Describe the specific purpose for the OPDIV use of the third-party Website or application:

Many of the third-party tools used in connection with the Centers for Medicare & Medicaid Services' (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), rely on cookies or web beacons to perform their functions.

These TLDs are hereafter referred to as "CMS' websites." Tealium is used as a solution for CMS staff to manage these cookies and web beacons from a single interface. Specifically, Tealium allows CMS to control, which cookies or web beacons are enabled/disabled, and thus which third-party tools are enabled/disabled. Tealium adds, removes and modifies code across CMS' websites. Many of the tools CMS uses to gather data on visitors' onsite behavior, interactions, and the performance of CMS Websites are deployed using Tealium. Tealium gives CMS and its staff and contractors an easy way to manage all of these tools.

Tealium also includes the iQ Privacy Manager which offers opt-in or opt-out choices to site visitors and gives site visitors control over which tags or cookies you want to accept while you visit the site.

The Tealium Customer Data Hub also allows CMS to define custom attributes and audiences for the purpose of audience discovery, and to syndicate enriched data or trigger action directives via 3rd party applications.

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 to use CMS' websites due to the site's use of Tealium, 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 disable their cookies if they do not want their device 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?

Other...

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

Not Applicable. The public cannot navigate directly to Tealium since the application 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?

No

Provide a hyperlink to the OPDIV Privacy Policy:

https://www.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?

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:

When a user has expressly opted-in to an enriched and personalized user experience, the Tealium Customer Data Hub may collect personally identifiable information (PII).

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 common user identifier must be captured. An example of a user identifier is a numeric user identifier or an email address. Behavioral data from one session/device, such as web page visited, is leveraged to provide an improved and consistent user experience in future sessions/devices.

Medical and beneficiary personal health information will not be collected and stored in the Tealium Customer Data Hub.

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:

When a user has expressly opted-in to an enriched and personalized user experience, an email address or numeric user identifier may be collected by the Tealium Customer Data Hub. This information may be shared with approved technologies within CMS to achieve the objective of providing an enriched and personalized user experience. These approved technologies already contain the email address or user identifier, so no new personally identifiable information would be directly shared outside of the Tealium Customer Data Hub.

The data within the Tealium Customer Data Hub are available only to CMS managers, teams who implement CMS programs, members of the CMS communications and web teams, and other designated federal staff and contractors who need this information to perform their duties.

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

Access to the platform is managed by role-based permissions to ensure visibility is limited to appropriate CMS staff and contractors. Multi-factor authentication is required to log in to the system. The roles within the system are Publisher, Editor and Reader.

Publishers can make changes and publish them.
Editors can make changes and save them, but not publish. Readers have only 'read-only' access.

Tealium’s Customer Data Hub is hosted in Tealium Private Cloud which has achieved 3rd party security and privacy certifications such as HIPAA & HITECH, ISO 27001 and 27018, Privacy Shield and SSAE18 SOC 2 Type I & II. Administrative controls include items such as, but not limited to user training, system documentation that advises on proper use, implementation of need to know and minimum necessary principles when awarding access, and others. Technical controls include items such as, but not limited to, firewalls, network monitoring and intrusion detection. Physical controls include that all system servers are protected by guards, locked facility doors, and climate controls. Other appropriate controls have been selected from the National Institute of Standards and Technology (NIST) guidance.

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:

All data transmitted from the user’s browser, is encrypted over Hypertext Transfer Protocol Secure (HTTPS) Secure Sockets Layer (SSL). The https:// on website addresses ensures that you are connecting to the official website and that any information you provide is encrypted and transmitted securely. The information will be stored on Tealium’s Private Cloud solution, which is a single-tenant environment that provides data isolation and security compliance. This means data is isolated and secured separately away from other data sources. All data is encrypted at rest in Tealium’s Private Cloud solution. Tealium’s Private Cloud has achieved a pedigree of 3rd party security and privacy certifications: HIPAA, ISO 27001 and 27018 and SSAE18 SOC 2 Type II.

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

CMS will use Tealium 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 Tealium’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. Tealium is employed solely for the purposes of improving CMS' services and activities online related to operating CMS’ websites. Information collected by Tealium is created and maintained by Tealium.

Potential Risk:
Persistent cookies are used by third party Tealium’s tools on CMS’ websites to collect user’s information such as IP address, host name, operating system, browser, screen resolution, timestamp, etc. These cookies are stored on a user’s local browser. Persistent cookies remain in your browser after you close your browser or turn off your computer. With the exception of the Tealium "Privacy Manager" cookie discussed below, Tealium cookies remain on users’ browsers for one year.

The Tealium "Privacy Manager" feature creates a cookie that and has a lifespan of 3 years. This cookie only stores information about consumer's privacy settings to ensure their preferences are saved. Because the Privacy Manager works using a cookie that is installed on a site visitor's browser, the opt-in and opt-out choices made through the Privacy Manager will only be effective on the device through which a user makes opt-in or opt-out choices using the Privacy Manager, and a user's choices will expire after 3 years when the Privacy Manager cookie expires. Thereafter, users must revisit the Privacy Manager to renew their opt-in and opt-out choices.

Mitigation:
Tealium’s privacy policies, notices from CMS’ websites, information published by Tealium about its privacy policies, and the ability for consumers to disable cookies and opt out of providing their information to Tealium maximizes consumers ability to protect their information and mitigates risks to their privacy.

Potential Risk:
CMS also recognizes that if Tealium is not implemented correctly in relation to CMS’ websites, personal information could be collected about visitors without expressed consent.

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