US Department of Health and Human Services

Third Party Websites and Applications Privacy Impact Assessment

Date Signed:

September 07, 2018

OPDIV:

CMS

Name:

PANDORA

TPWA Unique Identifier:

T-5319340-183694

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:

Pandora Internet Radio (also known as Pandora Radio or simply Pandora) is a music streaming and automated music recommendation service. Pandora provides a free, advertising supported version of its services. Advertising on Pandora can include audio, video, and visual advertisements. Pandora users can register for free accounts by providing their email address, year of birth, zip code, and gender to Pandora. Additional information may be solicited by Pandora through voluntary surveys. Pandora also collects behavioral information from registered users as they use Pandora (for example, whether users skip certain songs, how they rate songs, what advertisements they click on, etc.). The information collected by Pandora and associated with registered users is used to help personalize recommendations to listeners and customize other content delivered through the service, including advertising content. Pandora enables CMS to serve audio, video, and visual display advertising to Pandora users. The audio ads are heard through the music streaming service while the video and visual ads appear on the user’s device.

The user has the option of clicking on the ad for more information about the specific CMS program advertised. When the consumer clicks on the advertisement, he or she is directed to a CMS website.

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 interact with advertisements from Pandora, consumers can learn about CMS campaigns through other advertising channels such as TV, radio, CMS websites and in-person events.

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?

There is no link from CMS websites to Pandora's website or mobile services. CMS uses Pandora Advertising to place digital advertising on Pandora sites in order to educate users about CMS programs.

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

The public can visit Pandora directly by typing the address www.pandora.com into their web browsers, or downloading the Pandora mobile application.

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:

This is the privacy policy for all CMS website https://www.cms.gov/privacy/ unless one of the following is noted https://www.healthcare.gov/privacy/ and https://www.medicare.gov/privacy-policy/index.html.

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:

Not Applicable. CMS does not collect any PII through use of Pandora.

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:

Not Applicable. CMS does not collect any PII through use of Pandora.

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

Not Applicable.

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. CMS will not collect any PII through use of Pandora.

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

Persistent Cookies, Web Beacons, and Targeting based on Sensitive Information That a Consumer Voluntarily Provides to Pandora

Potential Risk:

The use of cookies, pixels, and web beacons generally presents the risk that an application could collect information about a user's activity on the Internet for purposes that users did not intend. The unintended purposes include providing users with behaviorally targeted advertising, based on information that the individual user may consider to be sensitive. In Pandora's case, the information maintained by Pandora includes PII that users voluntarily provide to Pandora and their behaviors while using the services, as well as any third party data that Pandora combines with this information.

Additional Background:

Pandora may pair with advertising partners who place cookies and web beacons on a CMS website. These advertising tools collect non-personally identifiable information from users of a CMS website. A pixel (or web beacon) is a transparent graphic image (usually 1 pixel x 1 pixel) that is placed on a web page that allows Pandora to collect information regarding the use of the web page. A cookie is a small text file stored on a website visitor's computer that allows the site to recognize the user and keep track of preferences. These technologies provide information about when a visitor clicks on or views an advertisement. Pandora uses that information to judge which advertisements are more appealing to users and which result in greater conversions, such as transactions with a CMS website.

CMS advertising displayed through Pandora's application will carry persistent cookies that enable CMS to display advertising to individuals who have previously visited the CMS website. In this instance, the Pandora persistent cookie will be stored on the user's computer for up to 24 months, unless removed by the user.

Mitigation:

CMS websites and Pandora provide users information about the use of persistent cookies, the information collected about them, and the data gathering choices they have in their website privacy policies.

When a user is routed to a CMS website by clicking on a CMS advertisement displayed on Pandora, and the Tealium iQ Privacy Manager is present on the CMS website, users are able to control which cookies they want to accept from the CMS website. Tealium iQ Privacy Manager can be accessed through information provided on the privacy policy on a CMS website. There is a large green "Modify Privacy Options" button that turns off the sharing of data for advertising purposes that can be accessed through the CMS website privacy policy.

The ability to control which cookies users want to accept is only valid when Tealium iQ Privacy Manager is installed on the website. Another alternative is for users to disable cookies through their web browser. Separately, CMS includes the Digital Advertising Alliance AdChoices icon on all targeted digital advertising. The AdChoices icon is an industry standard tool that allow users to opt out of being tracked for advertising purposes, like the Tealium iQ Privacy Manager.

Users may also opt-out via the methods listed below:

An opt-out link on http://www.pandora.com/advertising/preferences/; and
Click on the “Ad Choices” logo in the corner of an ad served by Pandora, or by clicking on the link provided in AdChoices link in the Pandora privacy policy, which provides consumers with the ability to opt-out of data collection for behavioral advertising by all companies who participate in the Digital Advertising Alliance.

Targeted advertising Based on Sensitive Information Acquired by Pandora

Potential Risk:

Pandora works with advertising partners that collect and maintain information on consumers, including information about their use of various websites over time. These partners may provide Pandora with certain information about those customers for the purposes of serving advertisements and or/marketing offers to their customers on the Pandora site. Pandora also works with marketing companies and data providers that create, maintain, and distribute marketing lists or segments, or maintain and distribute other marketing, or similar data. These advertisements and marketing offers may be served based, in whole or in part, on data that an individual consumer considers sensitive.

Mitigation:

As a mitigation to this risk, CMS and Pandora will enter a written agreement under which Pandora will agree not to create marketing lists or share data that can be used to identify a user based solely on an interaction with a CMS ad to benefit Pandora or any of its other advertisers. This agreement will be provided in writing between CMS and Pandora before any advertising is placed.