Centers for Medicare & Medicaid Services
Information Security and Privacy Group

CMS Third Party Website and Application (TPWA) Privacy Impact Assessment (PIA) Template

I. INTRODUCTION

The Office of Management and Budget Memorandum 10-23, Guidance for Agency Use of Third-Party Websites and Applications[1], requires that federal agencies assess their uses of third-party Websites (e.g., LinkedIn, Twitter, Flickr, Facebook, Instagram, blog/microblogging tools, YouTube, etc.) and applications to ensure that the uses protect privacy. The mechanism by which agencies perform this assessment is a TPWA privacy impact assessment (PIA). In accordance with HHS policy, operating divisions (OPDIVs) are responsible for completing and maintaining PIAs on all third-party websites and applications in use. Upon completion of each assessment, agencies are required to make the PIAs publicly available.

Tips for Writing an Effective TPWA PIA:

- State the specific purpose of the CMS' use of the third-party website or application.
- Answer briefly; text fields have a limited capacity when translated to the final documentation.
- Write in a way that is easily understood by the general public; avoid using overly technical language, clearly define technical terms and references if needed to describe system.
- Define each acronym the first time it is used; use the acronym alone in all subsequent references.
- Do not include sensitive/confidential information or information that could allow a potential threat source to gain unauthorized access into the system.
- Explain what information will be made available to CMS from the use of the TPWA. Also clearly explain what information the public can provide directly to CMS using the TPWA.
- Answer whether the agency's activities will create or modify a system of records (SOR) under the Privacy Act.

[1] Memorandum 10-23, Guidance for Agency Use of Third- Party Websites and Applications

II. TPWA PIA FORM

1 – OPDIV: **CMS Guidance:** By default, this should always show CMS.	**CMS**
2 – TPWA Unique Identifier: **CMS Guidance:** This should display an auto-generated number.	*Leave blank*
3 – TPWA Name: **CMS Guidance:** Enter name of system or project.	LaunchDarkly
4 – Is this a new TPWA? **CMS Guidance:** Indicate whether the TPWA is new or an existing TPWA. If the TPWA is an existing system, subsequent questions within the PIA will ask the reason for reviewing and updating the PIA.	☒ **Yes** ☐ **No**
4a – Please provide the reason for revision. **(Skip to Q5 if Q4 is "Yes")** **CMS Guidance:** If the TPWA PIA is being revised, indicate the reason why, common may examples include: revising the PIA as part of the review process or revising the PIA to reflect changes in CMS's use of the TPWA.	
Click or tap here to enter text.	
5 – Will the use of a Third-Party Website or application create a new or modify an existing HHS/CMS System of Records Notice (SORN) under the Privacy Act? **CMS Guidance:** Each use of a TPWA should be assessed to determine the impact from the Privacy Act of 1974. The CMS Privacy Act Officer can assist to determine if a System of Records Notice (SORN) is required and supply the number if needed. Not all uses of TPWAs create a requirement for a SORN.	
☐ **Yes** ☒ **No**	
5a – Indicate the SORN number (or identify plans to put one in place). **CMS Guidance:** Provide the number of the applicable SORN or describe the plans to put a SORN in place. Most SORNs can be found at HHS and Operating Divisions (OPDIV) SORNs	

SORN Number: **If not published:**	
6 - Will the use of a third-party Website or application create an information collection subject to OMB clearance under the Paperwork Reduction Act (PRA)? **CMS Guidance: Each use of a TPWA should be assessed to determine the impact of the PRA. The CMS PRA team can provide more information on determining the applicability of the PRA. Not all uses of TPWAs create a requirement for OMB clearance under the PRA. Complete information on PRA requirements for social media can be found at:** https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/inforeg/inforeg/memos/2014/web-based-interactive-technologies-data-search-tools-calculators-paperwork-reduction-act.pdf **For expert guidance contact the CMS PRA Team via their page:** https://www.cms.gov/Regulations-and-Guidance/Legislation/PaperworkReductionActof1995/PRA-Listing.html	☐ **Yes** ☒ **No**
6a - Indicate the OMB approval number and approval number expiration date (or describe the plans to obtain OMB clearance.) CMS Guidance: The PRA focuses on increasing the efficiency of the federal government's information collection practices. It requires agencies to receive an OMB information collection approval number (also known as an "OMB control number") for an information system, prior to using that system to collect information from 10 or more respondents. For more information on federal collection of information please see the Federal Collection of Information on the OMB website at https://www.whitehouse.gov/omb/information-regulatory-affairs/federal-collection-information/ If the system uses an official, OMB-approved form(s) to collect information from the public it may display an OMB approval number and	OMB Approval Number: Expiration Date: Explanation:

expiration date that you can use to answer this question. You can also search OMB's Government-Wide Inventory of Currently Approved Information Collections at https://www.reginfo.gov/public/do/PRAMain and the CMS PRA page at https://www.cms.gov/medicare/regulations-guidance/legislation/paperwork-reduction-act-1995/pra-listing. One system may contain information from multiple OMB approved collections. The approval number and expiration for each/all should by entered for each collection. **Note: The PRA applies to standardized information collections from more than 10 respondents. It does not apply to data collections from agencies, instrumentalities, or employees of the United States in their official capacities.**	

8 - Point of Contact (POC)	**CMS Guidance:** This is generally the system/business owner or ISSO contact information. It is possible individuals in other roles may manage the use of the TPWA on behalf of CMS as well.
POC Title:	Director
POC Name:	Jon Booth
POC Organization:	CMS/OC/WETG
POC Email:	Jon.booth@cms.hhs.gov
POC Phone:	410-786-6577

9 – Describe the specific purpose for the OpDiv use of the third-party Website or application: **CMS Guidance:** CMS may use the TPWA to maximize opportunities to engage and communicate with the public. While the PIA's primary purpose is to convey the impact to privacy through use of the TPWA in question, this question provides the opportunity to explain the reasoning behind why a TPWA is being used and its importance.	The Centers for Medicare & Medicaid Services (CMS) uses LaunchDarkly Feature Management and Experimentation to support CMS' websites, including CMS.gov, Medicare.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." LaunchDarkly is a technology platform that supports feature management to improve customer experience. CMS uses LaunchDarkly feature management to improve user's website experiences and reduce risk with new functionality releases. Developers configure a LaunchDarkly Software Development Kit (SDK) to collect and transmit data about end-users to LaunchDarkly for the purpose of feature targeting. LaunchDarkly enables CMS to deploy persistent experiences, which can be delivered to users with specific behavioral profiles. The CMS staff analyzes and reports on the aggregated user-interaction data collected by LaunchDarkly. The reports are available only to CMS managers, teams who implement CMS 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.

	CMS uses this information to determine what types of changes need to be made to CMS' websites to improve the user experience for visitors by delivering different user interfaces to consumers and observing which allows consumers to perform a task easier.
10 – 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? **CMS Guidance:** Prior to utilizing a TPWA, CMS should evaluate the privacy policies of the third party to determine if there are any risks to a user that would preclude utilizing the tool to engage the public. Examples of a potential risk could include if the third-party releases account or other personal information for commercial purposes, if the third-party does not notify users of changes to the third-party's privacy policies, or if the third-party does not have any posted privacy policies.	☒ **Yes** ☐ **No**
11 – 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: **CMS Guidance:** Members of the public should not be required to use a TPWA to obtain information or services. The public must be provided with an alternative means to get the same information or services being offered by the TPWA.	If consumers do not want LaunchDarkly 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, a consumer can use the Tealium IQ Privacy Manager on CMS' websites privacy page(s) and "opt out" of having data collected about them by Launch Darkly. Alternatively, a consumer can disable their browser cookies if they do not want their information to be collected. Consumers can follow instructions published at https://launchdarkly.com/policies/privacy/.

12 – Does the third-party Website or application have appropriate branding to distinguish the OPDIV activities from those of nongovernmental actors? **CMS Guidance:** Departmental use of TPWAs and the content therein must clearly identify ownership or sponsorship through the use of Departmental or OpDiv branding. Branding is not required to be an official agency seal or logo; however, the image must clearly indicate a government presence. CMS or HHS logo policies also apply to TPWA use.	☐ **Yes** ☒ **No**

13 – How does the public navigate to the third-party Website or application from the OpDiv?

CMS Guidance: This question tries to identify how the public navigates to the TPWA from CMS. Select whether CMS: (i) provides an external hyperlink to the TPWA from the CMS website or a website operated on behalf of the CMS; (ii) incorporates or embeds the TPWA on the CMS website; or (iii) utilizes another approach. If this is a revision of an existing PIA, please provide a reason for revision.

Select from the drop down
Other...

13a – Please describe how the public navigates to the third-party Website or application:

CMS Guidance: According to OMB M-03-22 and Title II and III of the E-Government Act, each website must post clear privacy policies on top-level/principal websites, including major on-line public resource websites and any other known major public entry points, as well as any webpage that collects or posts personal information. Privacy policy links must be clearly labeled and easy to access by all visitors to a website. If the privacy statement is combined with other mandated or recommended website statements or information, the link should be labeled accordingly, (e.g., Privacy Act notification statement).

Not applicable. The public does not navigate to LaunchDarkly. LaunchDarkly is only accessible by CMS/HHS software developers and admins that have completed the necessary access and identity management steps.

13b - If the public navigates 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 a nongovernmental Website?

CMS Guidance: According to OMB M-03-22 and Title II and III of the E-Government Act, each website must post clear privacy policies on top-level/principal websites, including major on-line public resource websites and any other known major public entry points, as well as any webpage that collects or posts personal information. Privacy policy links must be clearly labeled and easy to access by all visitors to a website. If the privacy statement is combined with other mandated or recommended website statements or information, the link should be labeled accordingly, (e.g., Privacy Act notification statement).

☐ **Yes**
☐ **No**

14 – Has the OpDiv Privacy Policy been updated to describe the use of a third-party Website or application?

CMS Guidance: The term "Privacy Policy" refers to a single, centrally located statement that is accessible from an agency's general privacy related practices that pertains to its official website and other online activities. The privacy policy should be consolidated explanations of CMS's general privacy-related practices that pertain to its website and other online activities. The privacy policy should be a consolidated explanation of the CMS's general privacy-related practices that pertain to its official

website and its other online activities. The CMS privacy policy must be updated to include required information about the use of a TPWA. See Implementation of OMB M-10-22 and OMB M-10-23 at: http://www.hhs.gov/ocio/policy/implementation_of_omb_m-10-22_and_m-10-23.html for more information about required content for all HHS OpDiv Privacy Policies.
☒ **Yes** ☐ **No**

14a – Provide a hyperlink to the OpDiv Privacy Policy: **CMS Guidance:** Provide the hyperlink for the Privacy Policy that informs the public of the CMS's use of the TPWA.	https://www.cms.gov/privacy-policy/ https://www.healthcare.gov/privacy/ https://www.medicare.gov/privacy-policy https://www.medicaid.gov/privacy-policy/index.html https://www.insurekidsnow.gov/privacy-policy/index.html
15 – Is an OpDiv privacy notice posted on the third-party Website or application? **CMS Guidance:** A privacy notice is a brief description that describes the application of the agency's privacy policy to specific situations. The privacy notice should notify individuals before they engage an agency and should be provided on the specific website or application where individuals can make PII available to the agency; and, the privacy notice must be prominently displayed on the TPWA used by the CMS. The privacy notice clarifies how the CMS privacy policies will apply in context of using/visiting the TPWA. See Implementation of OMB M-10-22 and M-10-23 at: http://www.hhs.gov/ocio/policy/implementation_of_omb_m-10-22_and_m-10-23.html for more information about the required content and placement of the privacy notice. **Note: The use of some third-party websites or applications may make it difficult to post a privacy notice due to technical limitations. CMS should make their best efforts to ensure that a privacy notice is posted when it is feasible.**	☐ **Yes** ☒ **No**

15a – Confirm that the privacy notice contains all of the following elements: **(Skip to Q16 if Q15 is "No")**	☐ **Yes** ☐ **No**

(i) An explanation that the Website or application is not government-owned or government-operated; **(ii) An indication of whether and how the OpDiv will maintain, use, or share PII that becomes available;** **(iii) An explanation that by using the third-party Website or application to communicate with the OpDiv, individuals may be providing nongovernmental third parties with access to PII;** **(iv) A link to the official OpDiv Website; and** **(v) A link to the OpDiv Privacy Policy.** **CMS Guidance:** Provide a confirmation that the privacy notice includes the required content. HHS guidance for implementing OMB M-10-22 and OMB M-10-23, which describe the development and implementation of a TPWA privacy notice, can be found in the HHS Implementation of OMB M-10-22 and M-10-23 at: http://www.hhs.gov/ocio/policy/implementation_of_omb_m-10-22_and_m-10-23.html	

15b – Is the OpDiv's privacy notice prominently displayed at all locations on the third-party Website or application where the public might make PII available? **(Skip to Q16 if Q15 is "No")** **CMS Guidance:** Provide confirmation that the privacy notice is prominently placed at all locations on the TPWA where the public might make PII available. Please note that the requirement refers to situations in which the public might make PII available according to OMB M-10-23.	☐ **Yes** ☐ **No**
16 – Is PII collected by the OpDiv from the third-party Website or application? **CMS Guidance:** Although not defined by OMB, "collecting PII" is defined for the purposes of these procedures as any act, whether by humans or a technology, to collect or obtain any PII that is requested or made available through the TPWA with or without the consent of the user for any period. For example, if you are copying and pasting comments and	☐ **Yes** ☒ **No**

the affiliated PII around the comments into a file for other uses, that is considered a collection. Please note this question refers to the activities of CMS, not the activities of the TPWA.	
17 – Will the third-party Website or application make PII available to the OpDiv? **CMS Guidance:** Please note that the OMB definition of "make PII available" is very broad; therefore, it is likely that any use of a TPWA by CMS is making PII available to CMS. TPWAs that use features such as an option to become a follower to comment or to allow users to post and/or display names of the visitors, is considered to be making PII available to CMS. Please note that this question refers to the activities of the CMS, not the activities of the TPWA.	☐ **Yes** ☒ **No**
18 – Describe the PII that will be collected by the OpDiv from the third-party Website or application and/or the PII that 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 Guidance:** The purpose of this question is to clearly outline to the public the type of PII that is collected or that will likely be made available to CMS through the public's use of the TPWA and to identify how CMS will use that information. As a best practice, the PIA author can categorize the PII under the appropriate heading and indicate what the CMS intends to do with each type of PII. It is also recommended that the PIA Author ensure that the answer considers the situation in which a visitor to the TPWA could submit his or her own PII using comments or similar features of the TPWA and how this information may be used. A common example would be if a member of the public used the TPWA to provide information about him or herself to the CMS.	LaunchDarkly does not collect any PII from the public directly, and CMS does not gather any PII from LaunchDarkly.
19 – 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: **CMS Guidance:** The purpose of this question is to outline the type of PII collected (e.g., name, e-mail address) or made available to the CMS through the use of a TPWA, who the PII will be shared will be shared with (whether the sharing is internal to HHS or is available to parties outside of HHS), and the business purpose for sharing the PII.	N/A
19a – If PII is shared, how are the risks of sharing PII mitigated?	N/A

CMS Guidance: Provide a description for how any risks associated with sharing the PII are mitigated. Within the answer, describe any applicable administrative, technical, or operational controls that help minimize the risks associated with the information sharing.	

20 - Will the PII from the third-party Website or application be maintained by the OpDiv? **CMS Guidance:** Although not defined by OMB, for the purpose of this document, the term "maintained" implies that the PII (in any format) is actively maintained for a specific period of time. For example, the creation of back-up tapes for the purposes of business continuity and business resumption, information contained within e-mails, or any other process that creates a temporary record should be included within the definition of CMS maintaining the PII from the TPWA. For example, if comments posted to the TPWA are being saved in a file, the comments are being exported, and/or screen shots are being saved, that is considered maintaining PII.	☐ **Yes** ☒ **No**
20a – If PII will be maintained, indicate how long the PII will be maintained: **(Skip to Q21 if Q20 is "No")** **CMS Guidance:** Describe how long CMS plans to maintain the PII. A complete response will indicate the timeframe records will be maintained per record schedule guidance. For more information about the appropriate timeframes for maintaining records, please reach out to your Records Officer. The e-mail contact for the records office is below: Records_Retention@cms.hhs.gov	**Click or tap here to enter text.**

21 - Describe how PII that is used or maintained will be secured: **CMS Guidance:** Provide a description of the applicable physical, technical, or management controls that will be used to secure the PII being used or maintained by CMS.	Not Applicable

22 - What other privacy risks exist and how will they be mitigated? **CMS Guidance:** CMS should assess additional privacy risks and make plans to mitigate these risks. Any use of a TPWA does introduce some new privacy risks. For example, a TPWA that allows individuals to provide comments introduce the privacy risk that members of the public could provide their own PII. A means for managing this risk could be the development of policies and

procedures to monitor and moderate comments. Other examples of common privacy risks include changes in technology or modifications to the TPWA's privacy policies.
CMS uses LaunchDarkly in a manner that protects the privacy of consumers who visit CMS' websites and respects the intent of visitors. CMS conducts periodic reviews of LaunchDarkly'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. LaunchDarkly is employed solely for the purposes of improving CMS' services and activities online related to operating CMS' websites. Potential Risk: In using LaunchDarkly to manage features, CMS applications send information to LaunchDarkly about the current request context in order to determine which features to enable or disable. Which information is provided about the current request context is at the discretion of CMS application developers and is kept to only the required minimum for a specific use case. Mitigation: Policies and procedures are created and communicated to clarify information that will not identify a person is only acceptable to send to LaunchDarkly for feature evaluation and experimentation. If consumers do not want Launch Darkly 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, a consumer can use the Tealium IQ Privacy Manager on CMS' websites privacy page(s) and "opt out" of having data collected about them by Launch Darkly. Alternatively, a consumer can disable their browser cookies if they do not want their information to be collected. Consumers can follow instructions published at https://launchdarkly.com/policies/privacy/. Another way this privacy risk is mitigated is through the strong protections of the privacy program of LaunchDarkly, which is audited against both ISO 27001 and NIST 800-53 privacy controls annually. These protections include data confidentiality and integrity controls, data retention and deletion controls, and privacy by design principles embedded in the software development process. Potential Risk: LaunchDarkly transfers browser information (cookies, user agent, and local storage) when CMS uses the LaunchDarkly JavaScript or React client-side Software Development Kit (SDK) which contacts LaunchDarkly directly. Mitigation: Users can opt-out of LaunchDarkly by using the Tealium IQ Privacy Manager on CMS' websites privacy pages. Alternatively, a consumer can disable their cookies, if they do not want their information to be collected. LaunchDarkly's privacy policies, notices from CMS websites and LaunchDarkly informing consumers of its privacy policies, and the ability of consumers to opt out of providing their information to LaunchDarkly, mitigate risks to consumer privacy. CMS will not deploy the LaunchDarkly tool if the website is not using Tealium iQ.