Centers for Medicare & Medicaid Services
Information Security and Privacy Group

CMS Third Party Website and Application (TPWA) Privacy Impact Assessment (PIA) DataDog for Government

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.	DataDog for Government		
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: N/A 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: http://www.whitehouse.gov/sites/default/files/omb/assets/inforeg/SocialMediaGuidance_04072010.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 www.whitehouse.gov/omb/inforeg_infocoll If the system uses an official, OMB-approved form(s) to collect information from the public it may display an OMB approval number and expiration date that you can use to answer this question. You can also search OMB's Government-Wide Inventory of Currently Approved Information Collections and the CMS PRA page. 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**	OMB Approval Number: Expiration Date: Explanation:

collections from agencies, instrumentalities, or employees of the United States in their official capacities.	
7 – Does the Third Party Website or Application contain Federal Records? **CMS Guidance:** Each TPWA should be assessed to determine if it maintains federal records. If the TPWA maintains federal records, Your Records Officer can help you determine applicable records requirements. The e-mail contact for the records office is below: Records_Retention@cms.hhs.gov	☐ **Yes** ☒ **No**

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:	Information System Security Officer (ISSO)		
POC Name:	Information System Security Officer (ISSO)	**POC Organization:**	Centers for Medicare & Medicaid Services (CMS)

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.	Datadog is an analytics tool used by CMS, Center for Clinical Standards and Quality (CCSQ), Quality Payment Program (QPP) to collect, report, and analyze visitor interactions on CMS' websites top-level domains (TLDs). These TLDs are hereafter referred to as "CMS' websites." CMS uses this information to help find performance issues with the website as well any application errors that might happen during a consumer's browsing session. The CMS staff analyze and report using the collected data from these tools. The reports are available only to CMS managers, teams who implement the CMS programs 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.
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	☒ **Yes** ☐ **No**

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.	
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.	The QPP Website offers Privacy Settings which gives control over what tracking and data collection takes place during the visit. Third-party tools are enabled by default to provide a quality consumer experience. The Privacy Settings provide the choice to opt-in or to opt-out of the different categories of third-party tools used by the QPP Website analytic tools. The Privacy Settings prevents third-party tools from loading regardless of your cookie settings, which provides consumers with an additional layer of privacy that prevents the tool from loading at all. Because the Privacy Settings creates a cookie in the browser, the opt-in and opt-out choices made through the Privacy Settings will only be effective on the device and browser used to make choices, and choices will expire when the cookie expires. Once the cookie is created, the Privacy Settings will retain settings for 3 years from the date of the most recent visit. Thereafter, the Privacy Settings maybe revisited to renew opt-in and opt-out choices. Please note that by opting out of cookies, it will disable cookies from all sources, not just from CMS websites. If disabling cookies in browser, Privacy Settings will not be able to store preferences and will not function properly. If you do not wish to use QPP's Privacy Settings to opt-out of the tools used by the QPP Website, the tools can be opt-out individually. Alternatively, consumers can opt-out of the tool if they do not want their information to be collected by following instructions published at https://www.datadoghq.com/legal/privacy/

12 – Does the third-party Website or application have appropriate branding to	☐ **Yes** ☒ **No**

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.	

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 Incorporated or embedded on HHS Website

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 DataDog Browser. DataDog monitoring tool works in the background.

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** **N/A**

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 https://qpp.cms.gov/privacy
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:	☐ **Yes**

(Skip to Q16 if Q15 is "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	☐ **No**

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	☐ **Yes** ☒ **No**

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 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.	CMS does not collect any Personally Identifiable Information (PII) through the user of DataDog browser.
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.	PII is not stored with CMS.

19a – If PII is shared, how are the risks of sharing PII mitigated? **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.	N/A

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** N/A
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	Not Applicable

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 will use of DataDog Browser 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 DataDog'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. DataDog Browser is employed solely for the purposes of improving CMS' services and activities online related to operating CMS' websites.

Information collected by DataDog Browser is created and maintained by DataDog Browser.

Potential Risk:

The DataDog Browser tools use persistent cookies on CMS' websites and can be stored on a user's local system.

Users approximate geographic location is collected by DataDog Browser based on the IP address of the user's local system. Other information collected consists of Page Views, JavaScript Errors, Browser, Session Traces and other information specific to the health and performance of CMS' websites.

Mitigation:

DataDog Browser uses session cookies that expire at the end of a user's browsing session.

DataDog Browser's privacy policies, notices from CMS' websites, information published by DataDog Browser about its privacy policies, and the ability for consumers to opt-out of providing their information to DataDog Browser maximizes consumers' abilities to protect their information and mitigate risks to their privacy.

Consumers can also use QPP's Privacy Settings on each CMS website's privacy page and "opt out" of having data collected by third-party tools.

Potential Risk:

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

Mitigation:

Therefore, to mitigate this risk, CMS only allows a limited number of trained and credentialed staff or contractors to implement DataDog Browser. Staff will receive privacy and security training to help avoid incidents and errors.