Privacy Impact Assessment (PIA): OS - 405(d) Public Website - QTR2 - 2021 - OS1078367

Date Signed: 5/11/2021

Acronyms

ATO - Authorization to Operate
CAC - Common Access Card
FISMA - Federal Information Security Management Act
ISA - Information Sharing Agreement
HHS - Department of Health and Human Services
MOU - Memorandum of Understanding
NARA - National Archives and Record Administration
OMB - Office of Management and Budget
PIA - Privacy Impact Assessment
PII - Personally Identifiable Information
POC - Point of Contact
PTA - Privacy Threshold Assessment
SORN - System of Records Notice
SSN - Social Security Number
URL - Uniform Resource Locator

General Information

Status:	Approved	**PIA ID:**	1324620
PIA Name:	OS - 405(d) Public Website - QTR2 - 2021 - OS1078367	**Title:**	OS - HHS 405(d) Aligning Health Care Industry Security Approaches Public Website
OpDiv:	OS		

PTA

PTA - 1A:	Identify the Enterprise Performance Lifecycle Phase of the system	Initiation
PTA - 1B:	Is this a FISMA-Reportable system?	Yes
PTA - 2:	Does the system include a website or online application?	Yes

URL Details

Type of URL	List Of URL
Internet (publicly available)	www.405d.hhs.gov

PTA - 3A:	Is the data contained in the system owned by the agency or contractor?	Agency
PTA - 5:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?	No
PTA - 5B:	If no, Planned Date of ATO	5/31/2021
PTA - 6:	Indicate the following reason(s) for this PTA. Choose from the following options.	New Public Access
PTA - 7:	Describe in further detail any changes to the system that have occurred since the last PIA	new application
PTA - 8:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions?	Public Facing website supporting the 405(d) initiative providing access to the initiative's products and documents and hosts the 405(d) Collaboration Portal, which provides a platform for task group members to collaborate and create new products.
PTA - 9:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.	The 405(d) Website will be the main online resource for all of the 405(d) awareness products and engagement materials. The majority of content housed on the website are downloadable

		documents such as pdfs, word documents, excel files, and PowerPoints designed to educate and bring awareness to the sector. All of the content is written and created for public use and awareness. In addition to these documents our website also has a subscribe form that is linked to a third party software, MailChimp, that collects users information such as name, email, and organization. The website itself doesn't not store this information. It is all stored on to Mailchimp. However, the website also collects Personally identifiable information (PII) from potential task group members from our Get Involved page, which is a form designed on the website through Amazon Web Service (AWS) which asks for name, organization, title, area of expertise, and email and this information is collected by the website on to AWS and kept for 6 months. Also, the public website hosts the log-in button for the 405(d) Collaboration Portal, which requires a username and password, which no one but the task group members know. Additionally, The 405(d) Website hosts the 405(d) Collaboration Portal which will be the main platform for all of the Task group's working documents and products. It acts as a SharePoint site that allows for version control, meeting scheduling and collaboration between members. The portal will house updates to the Health Industry Cybersecurity Practices (HICP) document, revisions to the Quick Start Guides and a new product the Task Group is currently working on. The nature of the information on the portal is for public use once it's complete but is considered sensitive while being created and revised. The Collaboration Portal is only accessible for Task group members, who are eligible to create a username and password for the site.
PTA -9A:	Are user credentials used to access the system?	Yes
PTA - 9B:	Please identify the type of user credentials used to access the system.	Non-HHS User Credentials Password Username
PTA - 10:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual	The website also Personally identifiable information (PII) from potential task group members from our Get Involved page, which is a

		form designed on the website through Amazon Web Service (AWS) which asks for name, organization, title, area of expertise, and email and this information is collected by the website on to AWS and kept for 6 months. This information is not used for anything other than to maintain a communications distribution list. The application does not retrieve this information at all Also, the public website hosts the log-in button for the 405(d) Collaboration Portal, which requires a username and password, which no one but the task group members know. The Collaboration Portal is only accessible for Task group members, who are eligible to create a username and password for the site. No information is shared with another system. Information that is entered into the system by any individual remains within the application. The subscribe form that is linked to a third party software, MailChimp, that collects users information such as name, email, and organization is a standalone form that does not across or share any information outside of its Mailchimp. This information is not used for anything other than to maintain a communications distribution list. The application does not retrieve this information at all.
PTA - 10A:	Are records in the system retrieved by one or more PII data elements?	No
PTA - 11:	Does the system collect, maintain, use or share PII?	Yes
	PIA	
PIA - 1:	Indicate the type of PII that the system will collect or maintain	Name E-Mail Address Others - organization, title, area of expertise,
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared	Public Citizens
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system	501 - 2000
PIA - 4:	For what primary purpose is the PII used?	Communications and outreach.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research)	None
PIA - 7:	Identify legal authorities, governing information use and disclosure specific to the system and program	5 USC 301, Departmental regulations: This authority states that the head of an Executive department may prescribe regulations for the government of his department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property. In other words, each agency has some authority to create and maintain records in order to carry out the work of that agency.
PIA - 8:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	09-90-1901 HHS Correspondence, Customer Service, and Contact List Records

		SORN history: 84 FR
PIA - 9:	Identify the sources of PII in the system	Directly from an individual about whom the information pertains Online Non-Government Sources Members of the Public
PIA - 9A:	Identify the OMB information collection approval number or explain why it is not applicable.	Per the Office of the Secretary Report Clearance Officer, and the OMB Desk Officer, the activities we are using the 405(d) website for, specifically communications and engagement, do not fall under the paperwork reduction act (PRA) and do not require our website to obtain an OMB control number.
PIA - 10:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11:	Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason	Individuals are providing their information via the web form on the website. There is a written statement above for each form detailing what the purpose of the form is and why we need the information.
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 13:	Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason	All Personally Identifiable Information (PII) is voluntarily given by the individual. If they don't want to subscribe or get involved they simply to do not need to fill out the forms.
PIA - 14:	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained	No system changes impact the use of their PII.
PIA - 15:	Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not	End users can request to unsubscribe from our communications list by clicking the unsubscribe button at the bottom of all of our MailChimp communications. They will be asked to enter the relevant email and will receive a notification on that page as to the successful removal of the email from our subscribers list or they can email us at the CISA405d@hhs.gov inbox to ask to stop receiving communications or to air concerns about the usage of their information. The 405(d) support team checks the inbox and MailChimp every day, therefore, end users can unsubscribe or email the inbox at any time to ask questions and unsubscribe from our distribution list. The 405(d) Support Team will email the concerned individual within 48 hours of their message with a response. If individual is requesting to be removed from our distribution lists, their information will be removed from our Mailchimp list as well as the excel document we keep with subscribers information.
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. If no processes are in place, explain why not	Invalid email addresses will result in the removal of that individual's PII from our distribution list. All bounced back emails are assessed and removed based on the frequency at which we receive

		bounce back notifications for that email based on our distributed communications. Since we use MailChimp to collect our subscribers information we have the information backed up on MailChimp as well as an excel spreadsheet. Users receive an annual email requesting that they review their information and ensure that it is accurate and up to date. To ensure relevancy, system administrators send an annual Microsoft form to request users to update their information. If updates are provided, system administrators can change the individuals' information accordingly. Data integrity is maintained through user recertification and encryption through MailChimp and our website security.
PIA - 17:	Identify who will have access to the PII in the system and the reason why they require access	Administrators Developers Contractors
PIA - 17A:	Provide the reason of access for each of the groups identified in PIA-17 Administrators will need to be able to see the PII in order to complete their task of engagement, direct communications, and to ensure they are added to our outreach distribution lists. Contractors will be administrators of this application and thus will see the data. Developers will also be able to see the data if they are in the application making changes or providing services.	
PIA - 17B:	Select the type of contractor	HHS/OpDiv Direct Contractor
PIA - 18:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII	Program administrators and the program support team who manage the website and collaboration portal and send communications will have access to the PII. Any member of the program support team has gone through multiple rounds of interviews, and been approved to work on the project by the project team's manager. They have been trained on Mailchimp by more experience program support staff and understand the procedures in place for acquiring 405(d) program subscribers and vetting potential 405(d) task group members. Some of the PII is collected by third party system, MailChimp, and by our website's get involved form and the get involved information is stored on the back-end of our website. The above categories of individuals have access based on their role of the 405(d) support team. The program administrators and program support contractors are directly involved in the 405(d) communications due to product releases and updates being sent out they have been vetted by HHS staff and approved to work on 405(d) and use the PII to generate interest in the program. The project developer maintains and updates the website with content and he has access to the PII because he updates and maintains the website's AWS code and system controls.
PIA - 19:	Describe the technical methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job	The information will only be accessed when sending communications. Privileges to the information are only assigned based on position and necessary access.

PIA - 20:	Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained	During the on-boarding process, training and awareness is provided to personnel that accessing or leveraging the PII can only be used when delivering official program communications. As well as Annual HHS Information Systems Security Awareness Training. In addition Standard Operating Process (SOP) has been developed that provide all users direct guidance on how to use the system, what data is in the system, what their role is, and what they should or should not be doing in terms of their access to the data/application
PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific NARA records retention schedule(s) and include the retention period(s)	Per the Standard National Archives and Records Administration (NARA) guidelines these are the records retention guidelines relevant to the information on our website and the PII we are collecting and housing. GRS. 3.1 Item 20 • Information technology operations and maintenance records. GRS 5.2 Item 10 Transitory records GRS 5.1 Item 020 – Non-recordkeeping copies of electronic records
PIA - 24:	Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response	The PII data (email addresses and user submitted passwords) will be stored in Amazon Web Services' Cognito, a managed user access

		control service. Cognito is Federal Risk and Authorization Management Program (FedRAMP) approved (Moderate East/West) and so maintains the highest security standards in terms of data protection. Furthermore, role-based access control will enabled tiered read/write access, e.g., only administrators can issue password resets and delete/add users. PII data is physically stored within a FedRAMP Moderate security boundary, which meets all physical controls for a Federal Information Security Management Act (FISMA) Moderate system. Access to the systems that hold the data is protected by several layers of security controls, firewalls, Intrusion Detection/Prevention Systems, and Access Control Lists. To protect against interception of communications over the network all data is transmitted using Federal Information Processing Standard (FIPS) 140-2 encryption. To ensure protection of data at rest, the systems that maintain the data as well as backups are encrypted using Advanced Encryption Standard (AES) 256-bit encryption. Operating system logs are kept and reviewed for anomalies on an as-needed basis. Administratively, these systems and data stored on the systems are only accessible by HHS cleared personnel that have been through Security Awareness Training, Role Based Training, and signed a Rules of Behavior, all of which includes handling of PII data. In order to access the data, a user must be approved by HHS to work on the systems that hold the data and access the system using two-factor authentication and are assigned a role-based group depending on the level of access needed.
PIA - 25:	Describe the purpose of the web site, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response	Public Facing website supporting the 405(d) program providing access to the program's products and documents and hosting the 405(d) Collaboration Portal on the back-end, which provides a platform for task group members to collaborate and create new products. The general public will be able to access the website via a public URL. This URL has been secured via Office of the Assistant Secretary for Public Affairs (ASPA). The collaboration Portal will be for 405(d) Task Group members only. These task group members have been vetted and approved. They will have individual access based on a user name and password that they choose. No one else will have access to their password.
PIA - 26:	Does the website have a posted privacy notice?	Yes
PIA - 27:	Does the website use web measurement and customization technology?	Yes
PIA - 27A:	Select the type of website measurement and customization technologies is in use and if it is used to collect PII	Session Cookies - Does Not Collect PII

PIA - 28:	Does the website have any information or pages directed at children under the age of thirteen?	No
PIA - 28B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	No
PIA - 29:	Does the website contain links to non-federal government websites external to HHS?	Yes
PIA - 29A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	Yes
PIA - 29B:	Is a TPWA needed for this system?	No