

Privacy Impact Assessment Form

v 1.47.4

Status

Form Number

Form Date

Question

Answer

1 OPDIV:

2 PIA Unique Identifier:

2a Name:

3 The subject of this PIA is which of the following?

- General Support System (GSS)
 Major Application
 Minor Application (stand-alone)
 Minor Application (child)
 Electronic Information Collection
 Unknown

3a Identify the Enterprise Performance Lifecycle Phase of the system.

3b Is this a FISMA-Reportable system?

- Yes
 No

4 Does the system include a Website or online application available to and for the use of the general public?

- Yes
 No

5 Identify the operator.

- Agency
 Contractor

6 Point of Contact (POC):

POC Title

POC Name

POC Organization

POC Email

POC Phone

7 Is this a new or existing system?

- New
 Existing

8 Does the system have Security Authorization (SA)?

- Yes
 No

8b Planned Date of Security Authorization

 Not Applicable

11 Describe the purpose of the system.	The purpose of this system is to create a Technical Assistance (TA) Hub that delivers comprehensive technical assistance and
12 Describe the type of information the system will collect, maintain (store), or share. (Subsequent questions will identify if this information is PII and ask about the specific data elements.)	TAH collect organizational email addresses to send notifications and collaborate with other users, password for authentication, and security role to specify privileges of the users in the system. TAH also collects user names to identify a
13 Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	TAH collect basic program information on OD2A; OD2A program participants request for technical assistance; the administration and execution of the technical assistance;
14 Does the system collect, maintain, use or share PII?	<input checked="" type="radio"/> Yes <input type="radio"/> No
15 Indicate the type of PII that the system will collect or maintain.	<input type="checkbox"/> Social Security Number <input type="checkbox"/> Date of Birth <input checked="" type="checkbox"/> Name <input type="checkbox"/> Photographic Identifiers <input type="checkbox"/> Driver's License Number <input type="checkbox"/> Biometric Identifiers <input type="checkbox"/> Mother's Maiden Name <input type="checkbox"/> Vehicle Identifiers <input checked="" type="checkbox"/> E-Mail Address <input type="checkbox"/> Mailing Address <input type="checkbox"/> Phone Numbers <input type="checkbox"/> Medical Records Number <input type="checkbox"/> Medical Notes <input type="checkbox"/> Financial Account Info <input type="checkbox"/> Certificates <input type="checkbox"/> Legal Documents <input type="checkbox"/> Education Records <input type="checkbox"/> Device Identifiers <input type="checkbox"/> Military Status <input checked="" type="checkbox"/> Employment Status <input type="checkbox"/> Foreign Activities <input type="checkbox"/> Passport Number <input type="checkbox"/> Taxpayer ID UserID & Password
16 Indicate the categories of individuals about whom PII is collected, maintained or shared.	<input checked="" type="checkbox"/> Employees <input type="checkbox"/> Public Citizens <input checked="" type="checkbox"/> Business Partners/Contacts (Federal, state, local agencies) <input checked="" type="checkbox"/> Vendors/Suppliers/Contractors <input type="checkbox"/> Patients Other <input type="text"/>
17 How many individuals' PII is in the system?	<input type="text" value="100-499"/>
18 For what primary purpose is the PII used?	The PII Information is used for user registration, login and contact and follow-up.
19 Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	<input type="text" value="N/A"/>
20 Describe the function of the SSN.	<input type="text" value="N/A"/>

20a Cite the **legal authority** to use the SSN. N/A

21 Identify **legal authorities** governing information use and disclosure specific to the system and program. Public Health Service Act, Section 301, "Research and Investigation" (42 U.S.C. 241)

22 Are records on the system retrieved by one or more PII data elements? Yes
 No

23 Identify the sources of PII in the system.

	Directly from an individual about whom the information pertains	
<input checked="" type="checkbox"/>		In-Person
<input type="checkbox"/>		Hard Copy: Mail/Fax
<input checked="" type="checkbox"/>		Email
<input type="checkbox"/>		Online
<input type="checkbox"/>		Other
	Government Sources	
<input checked="" type="checkbox"/>		Within the OPDIV
<input type="checkbox"/>		Other HHS OPDIV
<input type="checkbox"/>		State/Local/Tribal
<input type="checkbox"/>		Foreign
<input type="checkbox"/>		Other Federal Entities
<input type="checkbox"/>		Other
	Non-Government Sources	
<input type="checkbox"/>		Members of the Public
<input type="checkbox"/>		Commercial Data Broker
<input type="checkbox"/>		Public Media/Internet
<input type="checkbox"/>		Private Sector
<input type="checkbox"/>		Other

23a Identify the OMB information collection approval number and expiration date. TBD

24 Is the PII shared with other organizations? Yes
 No

<p>25 Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.</p>	<p>The participants are informed that personal information is required for registration and identify proofing. The contractor communicates to the site users in three ways:</p> <p>1) Site registration form- The online form that people use to request access (membership) to the OD2A-TAC website includes the following notice before the entry fields: "NOTE: Personally identifiable information (e.g., name, email address) is collected solely for the purposes of providing password-protected access to the OD2A-TAC website, facilitating internal communication among OD2A-TAC website users, and sending system notifications."</p> <p>2) Site My Account Edit screen – The Site My Account screen which allows the site users to view and edit their Personal information has the following disclaimer: "NOTE: Personally identifiable information (e.g., name, email address) is collected solely for the purposes of providing password-protected access to the OD2A-TAC website, facilitating internal communication among OD2A-TAC website users, and sending system notifications."</p> <p>3) Site Login screen – The login screen contains a disclaimer stating unauthorized or improper use of this system is prohibited and may result in disciplinary action and/or civil and criminal penalties. At any time, and for any lawful government purpose, the government may monitor, record, and audit your system usage and/or intercept, search and seize any communication or data transiting or stored on this system. Therefore, you have no reasonable expectation of privacy. Any communication or data transiting or stored on this system may be disclosed or used for any lawful Government purpose."</p>	
<p>26 Is the submission of PII by individuals voluntary or mandatory?</p>	<p><input checked="" type="radio"/> Voluntary <input type="radio"/> Mandatory</p>	
<p>27 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.</p>	<p>There is no method to opt out of the collection of the PII for this systems since the PII collected is name, email address, and employment status is required in order to communicate with the site users. We could not communicate or authenticate the users without the PII requested.</p>	
<p>28 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.</p>	<p>The participants are contacted via email to notify and obtain consent when major changes occur.</p>	

<p>29 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.</p>	<p>User PII is limited to name, email, jurisdiction, and role – all of which are intended to be shared within the system with other users, via a member directory. Internal sharing of this information facilitates connections and communication among OD2A recipients, who are eager to learn from and support one another. The notice on the member directory records reminds users “Personally identifiable information (e.g., name, email address) is provided solely for the purposes of internal communication among OD2A Technical Assistance Center (TAC) website users and for system notifications.”. Users also have access to their own account profile, which they can update or correct at any time, to fix any inaccurate PII. Users can contact overdosedata2action@cdc.gov with concerns about the use of their personal information.</p>											
<p>30 Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. If no processes are in place, explain why not.</p>	<p>The system automatically prompts users (via email) every 60 days to update their password and review their profile information. This encourages self-maintenance of PII. New requests for system access are reviewed to ensure that only agency email addresses are used and to check for correct role selection. They are also reviewed and approved by DOP before being added to the system. This process takes place on a rolling basis to ensure new users are added to the system in a timely manner. Contractor Administrators and Developers may also access user profiles when needed – for example to delete them if DOP leadership requests this (for a recipient who had retired or resigned, for example).</p>											
<p>31 Identify who will have access to the PII in the system and the reason why they require access.</p>	<table border="1"> <tr> <td data-bbox="716 961 954 1056"> <input checked="" type="checkbox"/> Users </td> <td data-bbox="954 961 1422 1056"> The users have access to PII for collaboration and or editing. </td> </tr> <tr> <td data-bbox="716 1056 954 1171"> <input checked="" type="checkbox"/> Administrators </td> <td data-bbox="954 1056 1422 1171"> Indirect contractors add, edit, remove; PII to ensure integrity, accuracy and relevancy of information. </td> </tr> <tr> <td data-bbox="716 1171 954 1266"> <input checked="" type="checkbox"/> Developers </td> <td data-bbox="954 1171 1422 1266"> Indirect contractors debugging data-related issues. </td> </tr> <tr> <td data-bbox="716 1266 954 1381"> <input checked="" type="checkbox"/> Contractors </td> <td data-bbox="954 1266 1422 1381"> Indirect contractors add, edit, remove; PII to ensure integrity, accuracy and relevancy of information. </td> </tr> <tr> <td data-bbox="716 1381 954 1465"> <input type="checkbox"/> Others </td> <td data-bbox="954 1381 1422 1465"></td> </tr> </table>	<input checked="" type="checkbox"/> Users	The users have access to PII for collaboration and or editing.	<input checked="" type="checkbox"/> Administrators	Indirect contractors add, edit, remove; PII to ensure integrity, accuracy and relevancy of information.	<input checked="" type="checkbox"/> Developers	Indirect contractors debugging data-related issues.	<input checked="" type="checkbox"/> Contractors	Indirect contractors add, edit, remove; PII to ensure integrity, accuracy and relevancy of information.	<input type="checkbox"/> Others		
<input checked="" type="checkbox"/> Users	The users have access to PII for collaboration and or editing.											
<input checked="" type="checkbox"/> Administrators	Indirect contractors add, edit, remove; PII to ensure integrity, accuracy and relevancy of information.											
<input checked="" type="checkbox"/> Developers	Indirect contractors debugging data-related issues.											
<input checked="" type="checkbox"/> Contractors	Indirect contractors add, edit, remove; PII to ensure integrity, accuracy and relevancy of information.											
<input type="checkbox"/> Others												
<p>32 Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.</p>	<p>Users' roles are approved by the program management team and they do not have access to PII. The program management team must approve all user role classifications before they are</p>											
<p>33 Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.</p>	<p>The site will only collect the bare minimum PII in order to register the user on the site and ensure that the user is who they say they are. Furthermore, role-based access control are in place to ensure the concept of "least privilege" is implemented. Job function determines the level of access and users are assigned only those rights necessary to fulfill responsibilities for approved roles and system-level audit controls to safeguard and audit use.</p>											

34 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.	All staff are required to take annual training in cybersecurity, security awareness, and privacy training. This training has been reviewed and is in accordance with the CDC requirements.	
35 Describe training system users receive (above and beyond general security and privacy awareness training).	Training for administrators and developers is tailored to the TAH information system and their roles.	
36 Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	<input checked="" type="radio"/> Yes <input type="radio"/> No	
37 Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.	Records are retained and disposed of in accordance with the CDC Records Control Schedule (N1-442-09-1) and in accordance with contractual agreement. Record copy of study reports are maintained in the agency from two to three years in accordance with retention schedules. Source documents for computers are disposed of when they are no longer needed by program officials. Personal identifiers may be deleted from records when no longer needed in the study as determined by the system manager, and as provided in the signed consent form, as appropriate. Disposal methods include erasing computer tapes, burning or shredding paper materials or transferring records to the Federal Records Center when no longer needed for evaluation and analysis. Records are retained for 20 years; for longer periods if further study is needed.	
38 Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	The administrative security controls employed include adhering to department, policies and procedures around security and privacy; and annual awareness training for all users holding accounts for the system. The technical controls are shared between the system and the Amazon Web Service (AWS) platform. The system provides controls such as multi- factor authentication for all users to include Personal Identity Verification (PIV) login capability and role-based system access to control the amount of PII available to a user; 2 rounds of two-factor authentication for each individual accessing a data center floor. AWS provides infrastructure controls such as secure network access points. The physical controls will all be inherited by the AWS platform and include the following: Restricting physical access to the data center both at the perimeter and at building ingress points through the help of video surveillance, intrusion detection systems, and Visitors and contractors are required to have ID, sign-in with building security, and be escorted by an authorized staff at all times; Fire detection and suppression systems; Uninterruptible Power Supply (UPS); Climate and Temperature control; and Preventative maintenance.	

General Comments

OPDIV Senior Official
for Privacy Signature