

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 the system is to facilitate a Landscape Assessment Survey to increase enrollment in CDC's National
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.)	<p>PII Maintained: Business contact information, including name, email address and mailing address of CDC-recognized organizations offering lifestyle change programs.</p> <p>Non-PII Maintained: Lifestyle change program characteristics (community-level, program-level, and introductory-session level); Perceived barriers and facilitators to enrolling in the National DPP lifestyle change program; First-session attendance as well as registration in the lifestyle change program among introductory session participants; and Indicators of intervention fidelity among sites.</p> <p>External users receive a uniquely assigned weblink to access the survey and credential are permanently store until the end of the project. For survey respondents that did not complete an online survey, they are to complete a paper-based and submitted/uploaded the surveys via Secure File Transfer Protocol (SFTP) using User ID and Password.</p> <p>Internal user is utilizing Active Directory (user id/password) to authenticate; credentials are permanently stored until the project ends. Active Directory is a separate system with its own PIA.</p>
13 Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The system will be used to conduct a Landscape Assessment survey of CDC-recognized organizations providing National Diabetes Prevention Program's Lifestyle Change Programs
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 checked="" 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 type="checkbox"/> Employment Status
<input type="checkbox"/> Foreign Activities	<input type="checkbox"/> Passport Number
<input type="checkbox"/> Taxpayer ID	

User Id and password

16 Indicate the categories of individuals about whom PII is collected, maintained or shared.

<input type="checkbox"/> Employees
<input type="checkbox"/> Public Citizens
<input checked="" type="checkbox"/> Business Partners/Contacts (Federal, state, local agencies)
<input type="checkbox"/> Vendors/Suppliers/Contractors
<input type="checkbox"/> Patients
Other <input type="text"/>

17 How many individuals' PII is in the system?

18 For what primary purpose is the PII used?

19 Describe the secondary uses for which the PII will be used (e.g. testing, training or research)

20 Describe the function of the SSN.

20a Cite the **legal authority** to use the SSN.

21 Identify **legal authorities** governing information use and disclosure specific to the system and program.

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

- In-Person
- Hard Copy: Mail/Fax
- Email
- Online
- Other

Government Sources

- Within the OPDIV
- Other HHS OPDIV
- State/Local/Tribal
- Foreign
- Other Federal Entities
- Other

Non-Government Sources

- Members of the Public
- Commercial Data Broker
- Public Media/Internet
- Private Sector
- Other

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

24 Is the PII shared with other organizations? Yes No

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.

26 Is the submission of PII by individuals voluntary or mandatory? Voluntary Mandatory

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.

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.

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.	There is no 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, because the PII is being obtained from the CDC-recognized organization to which the individual is associated or is employed.										
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.	Periodic reviews are not necessary as this is a one point in time assessment.										
31 Identify who will have access to the PII in the system and the reason why they require access.	<table border="1"> <tr> <td><input checked="" type="checkbox"/> Users</td> <td>data entry</td> </tr> <tr> <td><input type="checkbox"/> Administrators</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Developers</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/> Contractors</td> <td>Indirect contractor: Statistical analysis and reporting.</td> </tr> <tr> <td><input type="checkbox"/> Others</td> <td></td> </tr> </table>	<input checked="" type="checkbox"/> Users	data entry	<input type="checkbox"/> Administrators		<input type="checkbox"/> Developers		<input checked="" type="checkbox"/> Contractors	Indirect contractor: Statistical analysis and reporting.	<input type="checkbox"/> Others	
<input checked="" type="checkbox"/> Users	data entry										
<input type="checkbox"/> Administrators											
<input type="checkbox"/> Developers											
<input checked="" type="checkbox"/> Contractors	Indirect contractor: Statistical analysis and reporting.										
<input type="checkbox"/> Others											
32 Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The National DPP Introductory Session Project leader (at CDC) is responsible for ensuring that personnel have controlled access only to what is relevant to their specific work on the										
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>Role-based access controls are in place to ensure the concept of "least privilege" is implemented. Based on the technical director and project director's assessment of each team member, the network administrator creates and implements network access groups. The access groups include managers, system staff, data analyst, web developer, database administrator, statisticians working on data validation, processing, visualization etc. Each individual assigned to work on the project is assigned to a group associated with their role. Access rights are then derived from that role.</p> <p>The project network directory structure is organized such that access to each sub folder is restricted to one or more network access groups, effectively ensuring that an individual's access to data containing PII is restricted only to network areas pertaining to tasks the individual is required to perform.</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.	The indirect contractors that process these data files are trained in standards and procedures to maintain the security and confidentiality of PII. Audits are conducted throughout the year to ensure adherence to these standards.										
35 Describe training system users receive (above and beyond general security and privacy awareness training).	None										
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, stored, and disposed of in accordance with CDC's Records Control Schedule for Scientific and Research Project Records (N1-442-09-01). PII will be removed before records are archived. Contractors will destroy all records no later than five years after the end of the project.

38 Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Administrative Controls: Administrative controls include a security plan, contingency plan, file back-up, least privilege, and training. Access reports are reviewed on a monthly basis.

Technical Controls: PII data is encrypted and stored in a secure database. Technical controls are in place to manage user identity, identity proofing, authentication and authorization.

Physical Controls: Physical controls include ID Badges and Key Cards. The system is in a location protected by security guards, gates, and surveillance at the entry point to each facility. Access to the buildings is limited to authorized personnel.

General Comments

OPDIV Senior Official for Privacy Signature