

Privacy Impact Assessment Form

v 1.21

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

8a Date of Security Authorization

<p>9 Indicate the following reason(s) for updating this PIA. Choose from the following options.</p>	<table border="0"><tr><td><input type="checkbox"/> PIA Validation (PIA Refresh/Annual Review)</td><td><input type="checkbox"/> Significant System Management Change</td></tr><tr><td><input type="checkbox"/> Anonymous to Non-Anonymous</td><td><input type="checkbox"/> Alteration in Character of Data</td></tr><tr><td><input type="checkbox"/> New Public Access</td><td><input type="checkbox"/> New Interagency Uses</td></tr><tr><td><input type="checkbox"/> Internal Flow or Collection</td><td><input type="checkbox"/> Conversion</td></tr><tr><td><input type="checkbox"/> Commercial Sources</td><td></td></tr></table> <p>Documenting business contact as PII</p>	<input type="checkbox"/> PIA Validation (PIA Refresh/Annual Review)	<input type="checkbox"/> Significant System Management Change	<input type="checkbox"/> Anonymous to Non-Anonymous	<input type="checkbox"/> Alteration in Character of Data	<input type="checkbox"/> New Public Access	<input type="checkbox"/> New Interagency Uses	<input type="checkbox"/> Internal Flow or Collection	<input type="checkbox"/> Conversion	<input type="checkbox"/> Commercial Sources	
<input type="checkbox"/> PIA Validation (PIA Refresh/Annual Review)	<input type="checkbox"/> Significant System Management Change										
<input type="checkbox"/> Anonymous to Non-Anonymous	<input type="checkbox"/> Alteration in Character of Data										
<input type="checkbox"/> New Public Access	<input type="checkbox"/> New Interagency Uses										
<input type="checkbox"/> Internal Flow or Collection	<input type="checkbox"/> Conversion										
<input type="checkbox"/> Commercial Sources											
<p>10 Describe in further detail any changes to the system that have occurred since the last PIA.</p>	<p>None.</p>										
<p>11 Describe the purpose of the system.</p>	<p>The Chronic Disease Management Information System (CDMIS) is a post award grants management web-based tool that allows CDC's National Center for Chronic Disease Prevention and Health Promotion (NCCDPHP) program staff and award recipients to monitor, track, and enhance performance and transparency on strategies, activities, and outcomes across multiple years.</p> <p>The data is used to document and report on activities of the Notice of Funding Opportunity (NOFOs) recipients.</p>										

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.)

The Chronic Disease Management Information System collects and stores information so that CDC staff and awardees can conduct data analysis of strategies, activities, and outcomes across multiple years after award closeout.

The data collected are used to document and report recipient efforts through interim and annual reports by allowing states, territories and large metropolitan areas to uniformly define, collect, and report chronic disease data.

CDMIS is organized into different modules which are described below:

1. Program Information - Funded partners enter program contact information. CDC staff contacts are also stored in this module

2. Resources -Funded partners enter names, position title, email, telephone number, job descriptions, personnel status (active or inactive) and position status (filled or vacant) for human resources associated with the program

3. Planning - Funded partners document standard and non-standard data sources used to plan, evaluate, and implement actions. This module allows storage and retrieval of relevant documents over time such as state plans, evaluation plans, burden reports, and logic models.

4. Action Plan - Funded partners build Action Plans (aka work plans) using a standardized template. The template is composed of Project Period Objectives, Annual Objectives, Progress, Activities and Products. Information in the Action Plan section is used to populate annual performance reports

5. Reports - Funded partners generate annual performance reports using a step-by-step process.

6. Search Tab -The Search section allows CDC staff to search across organizations for specific information of interest. Staff only have access to the funded partners that they manage. Award recipients only have access to their own data.

13 Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

The Chronic Disease Management Information System is used by NCCDPHP and funding recipients (awardees) to document and report recipient efforts through interim and annual reports. The recipients support the development, implementation and evaluation of chronic disease programs. All recipients are required to report data to NCCDPHP using CDMIS.

The data collected are used to document and report recipient efforts through interim and annual reports by allowing states, territories and large metropolitan areas to uniformly define, collect, and report chronic disease data.

The data collected, processed, and stored by CDMIS include contact and supporting information of recipients including names, position title, email, telephone number, job descriptions, personnel status (active or inactive) and position status (filled or vacant) for human resources associated with the program. CDMIS also contains plans and reports for program implementation and evaluation.

14 Does the system collect, maintain, use or share PII?

Yes
 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 checked="" 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	<input type="text" value="Other..."/>
<input type="text" value="Other..."/>	<input type="text" value="Other..."/>
<input type="text" value="Other..."/>	<input type="text" value="Other..."/>

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

Employees
 Public Citizens
 Business Partners/Contacts (Federal, state, local agencies)
 Vendors/Suppliers/Contractors
 Patients
Other

17 How many individuals' PII is in the system?

18 For what primary purpose is the PII used?	User name and password are used to control access. Name and email address are used for CDC to communicate with recipients.
--	--

19 Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	None
--	------

20 Describe the function of the SSN.	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.	Section 301 of the Public Health Service Act [42 U.S.C. 241]
---	--

22 Are records on the system retrieved by one or more PII data elements?	<input type="radio"/> Yes <input checked="" type="radio"/> No
--	--

22a Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or identify if a SORN is being developed.	Published: <input type="text"/> Published: <input type="text"/> Published: <input type="text"/> <input type="checkbox"/> In Progress
---	---

23 Identify the sources of PII in the system.	Directly from an individual about whom the information pertains <input type="checkbox"/> In-Person <input type="checkbox"/> Hard Copy: Mail/Fax <input checked="" type="checkbox"/> Email <input checked="" type="checkbox"/> Online <input type="checkbox"/> Other Government Sources <input checked="" type="checkbox"/> Within the OPDIV <input type="checkbox"/> Other HHS OPDIV <input checked="" 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.	OMB# 0920-0739, Exp: 09/30/2019
--	---------------------------------

24 Is the PII shared with other organizations?	<input type="radio"/> Yes <input checked="" type="radio"/> No
--	--

<p>24a Identify with whom the PII is shared or disclosed and for what purpose.</p>	<p><input type="checkbox"/> Within HHS</p> <p><input type="checkbox"/> Other Federal Agency/Agencies</p> <p><input type="checkbox"/> State or Local Agency/Agencies</p> <p><input type="checkbox"/> Private Sector</p>										
<p>24b Describe any agreements in place that authorizes the information sharing or disclosure (e.g. Computer Matching Agreement, Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).</p>	<div style="border: 1px solid black; height: 60px;"></div>										
<p>24c Describe the procedures for accounting for disclosures</p>	<div style="border: 1px solid black; height: 40px;"></div>										
<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>CDC sends all award recipients a Notice of Funding Award letter that outlines the requirements of the award. Those requirements include providing CDC with contact information of staff involved in the project. This is a condition of the award.</p>										
<p>26 Is the submission of PII by individuals voluntary or mandatory?</p>	<p><input checked="" type="radio"/> Voluntary</p> <p><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>No method in place. Individuals must provide contact information as a condition of the CDC funding.</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>CDC will notify the users of upcoming changes through email. CDC also provides release notes to the users that outline changes to the system.</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>A user can notify their CDC project officer to resolve any concerns. The CDC project officer will notify the CDMIS help desk at CDMIS@cdc.gov to investigate and resolve any issues.</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 contact information and system access is reviewed annually by the CDC Project Officer for accuracy and relevancy.</p>										
<p>31 Identify who will have access to the PII in the system and the reason why they require access.</p>	<table border="0"> <tr> <td><input checked="" type="checkbox"/> Users</td> <td><div style="border: 1px solid black; padding: 2px;">State users have access to the PII of users within their state; CDC users (aka</div></td> </tr> <tr> <td><input checked="" type="checkbox"/> Administrators</td> <td><div style="border: 1px solid black; padding: 2px;">Admins (contractors) can access PII to provide technical support.</div></td> </tr> <tr> <td><input type="checkbox"/> Developers</td> <td><div style="border: 1px solid black; height: 20px;"></div></td> </tr> <tr> <td><input checked="" type="checkbox"/> Contractors</td> <td><div style="border: 1px solid black; padding: 2px;">Admins (contractors) can access PII to provide technical support.</div></td> </tr> <tr> <td><input type="checkbox"/> Others</td> <td><div style="border: 1px solid black; height: 20px;"></div></td> </tr> </table>	<input checked="" type="checkbox"/> Users	<div style="border: 1px solid black; padding: 2px;">State users have access to the PII of users within their state; CDC users (aka</div>	<input checked="" type="checkbox"/> Administrators	<div style="border: 1px solid black; padding: 2px;">Admins (contractors) can access PII to provide technical support.</div>	<input type="checkbox"/> Developers	<div style="border: 1px solid black; height: 20px;"></div>	<input checked="" type="checkbox"/> Contractors	<div style="border: 1px solid black; padding: 2px;">Admins (contractors) can access PII to provide technical support.</div>	<input type="checkbox"/> Others	<div style="border: 1px solid black; height: 20px;"></div>
<input checked="" type="checkbox"/> Users	<div style="border: 1px solid black; padding: 2px;">State users have access to the PII of users within their state; CDC users (aka</div>										
<input checked="" type="checkbox"/> Administrators	<div style="border: 1px solid black; padding: 2px;">Admins (contractors) can access PII to provide technical support.</div>										
<input type="checkbox"/> Developers	<div style="border: 1px solid black; height: 20px;"></div>										
<input checked="" type="checkbox"/> Contractors	<div style="border: 1px solid black; padding: 2px;">Admins (contractors) can access PII to provide technical support.</div>										
<input type="checkbox"/> Others	<div style="border: 1px solid black; height: 20px;"></div>										

<p>32 Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.</p>	<p>The NCCDPHP program administrator of the funding award identifies which CDC Project Officer will work with a recipient. The project officers are only given access within CDMIS to the recipients/awardees they are assigned to oversee.</p> <p>The CDC Project Officers work with the awardees in each state to determine who should have access to CDMIS within the state. The recipients only have access to information within their state.</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>Role-based access controls are in place to ensure the concept of “least privilege” is implemented. 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. Users are given access to the least amount of information necessary to complete their duties.</p> <p>Roles include: CDC user (program staff, project officer) CDC program administrator (access across a module, manage users) CDC system administrator (provides technical support to CDC and recipient users) Recipient user (limited access based on state and program activities)</p>	
<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.</p>	<p>CDC users complete annual security and privacy awareness training.</p> <p>Recipient staff do not receive training from CDC.</p>	
<p>35 Describe training system users receive (above and beyond general security and privacy awareness training).</p>	<p>None</p>	
<p>36 Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?</p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>	
<p>37 Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.</p>	<p>PII is not retained after the award activities have ended. The PII is destroyed when user accounts are removed. All PII will be destroyed when CDMIS is no longer operational.</p> <p>Federal records are retained, stored, and disposed of in accordance with CDC’s Scientific and Research Project Records Control Schedule (N1-442-09-01). PII is not retained. CDC will follow the National Archives Disposal of Records (44 USC Chapter33) guidance once retention has ended.</p>	

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

Administrative Controls:
Access to PII is role-based and limited to authorized staff only. Audits are conducted annually of PII to ensure appropriate access. A security assessment of the system is conducted annually. Administrative controls include a security plan, contingency plan, file back-up, least privilege access, and training.

Technical Controls:
All data is encrypted in transit. Access controls (user id and password) are in place to restrict access to only authorized users. Continuous monitoring is in place to detect security threats.

Physical Controls:
CDC's servers are located in a secure facility with multiple layers of restricted access. Physical controls include ID Badges, Key Cards, and Closed Circuit TV (CCTV). The system is in a data center protected by guards, gates, and surveillance at the entry point to the facility. Access to the data center is limited to authorized personnel.

REVIEWER QUESTIONS: The following section contains Reviewer Questions which are not to be filled out unless the user is an OPDIV Senior Officer for Privacy.

Reviewer Questions		Answer
1	Are the questions on the PIA answered correctly, accurately, and completely?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes <input type="text"/>		
2	Does the PIA appropriately communicate the purpose of PII in the system and is the purpose justified by appropriate legal authorities?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes <input type="text"/>		
3	Do system owners demonstrate appropriate understanding of the impact of the PII in the system and provide sufficient oversight to employees and contractors?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes <input type="text"/>		
4	Does the PIA appropriately describe the PII quality and integrity of the data?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes <input type="text"/>		
5	Is this a candidate for PII minimization?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes <input type="text"/>		
6	Does the PIA accurately identify data retention procedures and records retention schedules?	<input type="radio"/> Yes <input type="radio"/> No

Reviewer Questions		Answer
Reviewer Notes		
7	Are the individuals whose PII is in the system provided appropriate participation?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes		
8	Does the PIA raise any concerns about the security of the PII?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes		
9	Is applicability of the Privacy Act captured correctly and is a SORN published or does it need to be?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes		
10	Is the PII appropriately limited for use internally and with third parties?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes		
11	Does the PIA demonstrate compliance with all Web privacy requirements?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes		
12	Were any changes made to the system because of the completion of this PIA?	<input type="radio"/> Yes <input type="radio"/> No
Reviewer Notes		
General Comments		
OPDIV Senior Official for Privacy Signature		HHS Senior Agency Official for Privacy