Save

Privacy Impact Assessment Form

v 1.21

Status | Form Number | Form Date 02/13/19

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	TBD
2a	Name:	WISEWOMAN Reporting System
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.	Operations and Maintenance
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: Information Systems Security Off POC Name: Cindy Allen POC Organization: CDC POC Email: clallen@cdc.gov POC Phone: 770-488-5388
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	Mar 21, 2019

Save

9	Indicate the following reason(s) for updating this PIA. Choose from the following options.	☒ PIA Validation (PIA Refresh/Annual Review) ☒ Anonymous to Non-Anonymous ☐ New Public Access ☐ Internal Flow or Collection ☐ Commercial Sources ☐ Significant System Management Change ☐ Alteration in Character of Data ☐ New Interagency Uses ☐ Conversion Other...
10	Describe in further detail any changes to the system that have occurred since the last PIA.	The system will now be used to document user credentials. Otherwise, there have been no changes to the system or the data collected.
11	Describe the purpose of the system.	The WISEWOMAN Reporting System is used by CDC funded WISEWOMAN programs in States and tribal organizations to submit Minimum Data Elements (MDEs) and other program related data.
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 system will maintain the email address of the awardee staff member uploading data. MDEs include items relating to screening and assessment, health coaching, and lifestyle programs.
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The email address is used for authentication to the system. User credentials (emaill address and password) are maintained temporarily until system access is no longer needed. MDEs are a set of standardized data variables maintained and shared to ensure cardiovascular disease risk factor information is collected for each participant. CDC does not require awardees to collect direct participant-level identifying information to be reported. MDEs serve the purposes of describing, monitoring, and assessing individual and program progress. MDEs are collected at the clinical provider level in States and tribal organizations, among low-income, uninsured and underinsured women ages 40 to 64. MDEs include information about the screening site, client demographics, risk factors and clinical assessment, and participation in health coaching and lifestyle programs. Health outcome measures assessed include, but are not limited to, systolic and diastolic blood pressure readings, total cholesterol, weight, smoking status, nutrition, and physical activity variables. The written progress report, submitted annually, is primarily a narrative description of the program's activities and accomplishments and is a requirement for awardees as outlined in the Funding Opportunity Announcement.
14	Does the system collect, maintain, use or share **PII**?	◉ Yes ○ No

Save

15	Indicate the type of PII that the system will collect or maintain.	☐ Social Security Number ☐ Date of Birth ☐ Name ☐ Photographic Identifiers ☐ Driver's License Number ☐ Biometric Identifiers ☐ Mother's Maiden Name ☐ Vehicle Identifiers ☒ E-Mail Address ☐ Mailing Address ☐ Phone Numbers ☐ Medical Records Number ☐ Medical Notes ☐ Financial Account Info ☐ Certificates ☐ Legal Documents ☐ Education Records ☐ Device Identifiers ☐ Military Status ☐ Employment Status ☐ Foreign Activities ☐ Passport Number ☐ Taxpayer ID Other... password Other... Other... 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?	<100
18	For what primary purpose is the PII used?	The primary purpose of using PII is to document user authentication to the system.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	Not applicable.
20	Describe the function of the SSN.	Not applicable.
20a	Cite the **legal authority** to use the SSN.	Not applicable.
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?	○ Yes ◉ 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: Published: Published: ☐ In Progress

Save

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.	OMB No. 0920-0612, Expired 12/31/2018
24	Is the PII shared with other organizations?	◯ Yes ◉ No
24a	Identify with whom the PII is shared or disclosed and for what purpose.	☐ Within HHS ☐ Other Federal Agency/Agencies ☐ State or Local Agency/Agencies ☐ Private Sector
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)).	n/a
24c	Describe the procedures for accounting for disclosures	n/a
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.	Awardees designate a data manager as a condition of the cooperative agreement funding. The awardee data manager is granted access to the WISEWOMAN Reporting System which requires email address for authentication.
26	Is the submission of PII by individuals voluntary or mandatory?	◉ Voluntary ◯ Mandatory

Save

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.	Awardee data managers may not opt-out of the collection of their email address, since awardees must designate a data manager as a condition of the cooperative agreement funding.	
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.	Awardees will be notified by email of any major changes to the system.	
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.	Users can contact the Centers for Disease Control and Prevention (CDC) Information Systems Security Officer with any concerns.	
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.	Reviews are conducted quarterly of all collected email addresses. Those no longer involved with this information collection are removed.	
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users ☐ Administrators ☐ Developers ☒ Contractors ☐ Others	Only specific CDC authorized personnel have access to the email CDC contractors have access to email addresses for user and system support.
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access is role based; users and contractors are granted access based on their roles and responsibilities with the program.	
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.	Role based access controls are in place to ensure the concept of "least privilege" is implemented.	
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.	CDC staff and contractors complete annual Security Awareness and Privacy training.	
35	Describe training system users receive (above and beyond general security and privacy awareness training).	Not applicable.	
36	Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	◉ Yes ○ No	
37	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.	CDC's Records Control Schedule for Scientific and Research Project Records, Significant and or Secondary Research Records; authorized disposition is to maintain the data at least eleven years, but no longer than twenty years, after the retirement of the system.	

Save

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 quarterly of PII to ensure appropriate access. A security assessment of the system is conducted annually. Technical Controls: All data is encrypted in transit. Access controls (emaill address and password) are in place to restrict access to 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.

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?	◯ Yes ◯ No
Reviewer Notes		
2	Does the PIA appropriately communicate the purpose of PII in the system and is the purpose justified by appropriate legal authorities?	◯ Yes ◯ No
Reviewer Notes		
3	Do system owners demonstrate appropriate understanding of the impact of the PII in the system and provide sufficient oversight to employees and contractors?	◯ Yes ◯ No
Reviewer Notes		
4	Does the PIA appropriately describe the PII quality and integrity of the data?	◯ Yes ◯ No
Reviewer Notes		
5	Is this a candidate for PII minimization?	◯ Yes ◯ No
Reviewer Notes		
6	Does the PIA accurately identify data retention procedures and records retention schedules?	◯ Yes ◯ No
Reviewer Notes		
7	Are the individuals whose PII is in the system provided appropriate participation?	◯ Yes ◯ No
Reviewer Notes		

Save

	Reviewer Questions	Answer
8	Does the PIA raise any concerns about the security of the PII?	◯ Yes ◯ No
Reviewer Notes		
9	Is applicability of the Privacy Act captured correctly and is a SORN published or does it need to be?	◯ Yes ◯ No
Reviewer Notes		
10	Is the PII appropriately limited for use internally and with third parties?	◯ Yes ◯ No
Reviewer Notes		
11	Does the PIA demonstrate compliance with all Web privacy requirements?	◯ Yes ◯ No
Reviewer Notes		
12	Were any changes made to the system because of the completion of this PIA?	◯ Yes ◯ No
Reviewer Notes		

General Comments	

OPDIV Senior Official for Privacy Signature	Jarell Oshodi -S Digitally signed by Jarell Oshodi -S Date: 2019.03.26 08:57:22 -04'00'	HHS Senior Agency Official for Privacy	