Save

Privacy Impact Assessment Form

v 1.47.4

Status Draft Form Number F-26297 Form Date 4/8/2020 5:00:39 PM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-4516785-462169
2a	Name:	Million Hearts Recognition Programs (MHRP)
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.	Development
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: ISSO POC Name: Cindy Allen POC Organization: NCCDPHP POC Email: CDL1@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
8b	Planned Date of Security Authorization	June 19, 2020 □ Not Applicable

Save

11	Describe the purpose of the system.	The Million Hearts Hospitals and Health Systems Recognition Program (MHHHS) system is an electronic application 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 MHHHS system collects data and maintains the program application webform used to award and acknowledge hospitals and health system institutions for the outstanding achievement in keeping people healthy, optimizing care,
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	Million Hearts Hospitals and Health System (MHHHS) is a web-based system designed for collecting applications in an award recognition program to help evaluate whether a given
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.	□ Social Security Number ☒ Name □ Driver's License Number □ Mother's Maiden Name ☒ E-Mail Address ☒ Phone Numbers □ Medical Notes □ Certificates □ Education Records □ Military Status □ Foreign Activities □ Taxpayer ID □ Date of Birth □ Photographic Identifiers □ Biometric Identifiers □ Vehicle Identifiers ☒ Mailing Address □ Medical Records Number □ Financial Account Info □ Legal Documents □ Device Identifiers □ Employment Status □ Passport Number Username and Password
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?	100-499
18	For what primary purpose is the PII used?	System User's Authentication--the emails will be used to establish an access account in order to allow users to securely access the system for administration, application submissions, software development, and maintenance purposes.

Save

19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	PII is used for communication. If provided, specific contact details considered PII (name, email address, phone number) will be used to contact the associated individual. If no PII is provided, the generic contact information provided will be used to contact the associated representative of the hospital or health system to be recognized.
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.	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 □ 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 Control Number 0920-1274 | Expiration Date 11/30/2022
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.	There are no process in place to notify individuals their PII will be collected. The PII provided is a requirement to be considered for recognition program. Therefore, there is no need for these individuals to receive a forewarning that the information they provide will be collected. The data collected is in accordance to the aforementioned approved OMB control number stated.

Save

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.	Administrator cannot opt-out of having their user credentials and emails used because it is required for their role. This information is necessary to establish an account in supporting the program and accessing the system. Generic email addresses may be used by applicants so they do not have to disclose any PII or references to PII.	
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.	CDC publishes Million Hearts Hospitals and Health Systems Recognition Program reporting requirements and announces major changes in Federal Register Notices. The information collected does not provide identifying information that would allow for notification of individuals if there were changes to disclosure or data; however, the assurance of confidentiality in place prohibits data that are collected from disclosure.	
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 defined process as this situation is very unlikely to happen, as an individual would provide their contact information to allow CDC to contact them.	
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.	PII is an organizational contact info and is reviewed only as the CDC further engages participating organizations providing PII. PII is reviewed on a regular basis and conducted by OpDiv personnel. On a weekly basis, data is exported from the system to track progress and conduct compliance checks; data is then verified by OpDiv personnel by contacting the individuals.	
31	Identify who will have access to the PII in the system and the reason why they require access.	☐ Users	
		☒ Administrators	Administrators are given access to the PII in the system in order to support supporting the engagement with system users and reviewing PII for
		☒ Developers	Developers are given access to the PII in order to access structures and hardware in supporting the information system. business contact
		☒ Contractors	Non Direct contractors include both developers and administrators and therefore must access the PII in the system for either of the reasons
		☐ Others	
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access to data is based on the roles of users as authorized by program administrators and National Association of Chronic Disease Directors (NACDD) personnel.	

Save

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. Based on the technical director's and project director's assessments of each team member, the network administrator creates and implements network access groups. There is a network role of Users who have limited access to view any data, only the PII info they have submitted with their username and credentials. The Administrators are limited to the project directors and technical directors logins. They will have access to view the users PII through a backend WordPress panel for the purpose of technical support and data for the project.
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 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. . Developers/contractors may be required to complete the Information Security Awareness Training (SAT) annually which covers all aspects of systems and data security and confidentiality, upon CDC request. Systems and network staff with higher roles and responsibilities are similarly encouraged to complete additional training on contingency plans and disaster recovery training on an annual basis. Additionally, security training is conducted periodically upon the introduction of new staff/personnel and any significant system updates and/or requirements . The training includes a review of the security requirements and procedures for the project, including relevant portions of the security plan.
35	Describe training system users receive (above and beyond general security and privacy awareness training).	Internal organization system administrator with high professional experience are trained and conducts training in procedurals of data security and management in order to maintains highest security standards inside the organization responsible for maintaining the system. Example: Systems and network infrastructure staff receive specific security training based on the technology they support on an ongoing basis and receive additional security training as necessary to meet contract requirements.
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.	The contractor shall adhere to Common Record Schedule and regulations for appropriately retaining and destroying PII. Records are retained, stored, and disposed of in accordance with CDC's records control schedule for Employee Health and Safety Record, GRS 2.7. PII will be detroyed before records are annually archived and purged from the system. Contractors will transfer relevant records periodically and upon request.

Save

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 an admin access evaluation to limit number of individuals with access to PII, security plan, contingency plan, data back-ups, least privilege controls, training for developers and administrators, and retention and destruction of data plan Technical Controls: PII data is encrypted and stored in a secure database that is not accessible from other parties than CDC, NACDD administrators and Ensemble developers. Technical controls are in place to manage user identity, identity proofing, authentication and authorization. Physical Controls: Before destruction, PII is stored in a server in an data center with access only to approved employees. All employees who need data center access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access, and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions. (Source: https://aws.amazon.com/compliance/data-center/controls/)
39	Identify the publicly-available URL:	https://hospitals.millionhearts.hhs.gov
40	Does the website have a posted privacy notice?	● Yes ○ No
40a	Is the privacy policy available in a machine-readable format?	○ Yes ● No
41	Does the website use web measurement and customization technology?	● Yes ○ No
41a	Select the type of website measurement and customization technologies is in use and if it is used to collect PII. (Select all that apply)	Technologies — Collects PII? ☐ Web beacons — ○ Yes ○ No ☐ Web bugs — ○ Yes ○ No ☒ Session Cookies — ○ Yes ● No ☐ Persistent Cookies — ○ Yes ○ No Other... — ○ Yes ○ No
42	Does the website have any information or pages directed at children under the age of thirteen?	○ Yes ● No

Save

43	Does the website contain links to non- federal government websites external to HHS?	● Yes ○ No
43a	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	● Yes ○ No
General Comments		
OPDIV Senior Official for Privacy Signature	Jarell Oshodi -S	Digitally signed by Jarell Oshodi -S Date: 2020.04.15 13:10:58 -04'00'