Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-26384 | Form Date: 2/16/2021 10:41:01 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-5132987-098375
2a	Name:	Data Coordinating Center (DCC)
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: IT Specialist POC Name: Carman Layne POC Organization: NCHHSTP/OD POC Email: iws6@cdc.gov POC Phone: 770.488.8116
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	April 23, 2021 ☐ Not Applicable

Save

11	Describe the purpose of the system.	The Data Coordinating Center (DCC) application was developed by Division of HIV/AIDS Prevention (DHAP) to provide Local and State health departments (Grantee) with user-friendly tools to manage participant (Public Citizen) tracking information, data collection schedules, data submissions, error resolutions, and reporting. (Public Citizen) data collected by the grantees are entered into the Medical Monitoring Project (MMP) Tracking Module application then synced to DCC using Centers for Disease Control and Prevention (CDC) encrypted variables on a monthly bases. CDC uses these cumulative datasets to inform and instruct the internal data management processes.
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 types of data DCC collects and stores from National HIV Behavioral Surveillance (NHBS) and MMP area sites are; person's name, birth-date, sex at birth, year of birth, birth county, gender, race, ethnicity and MMP Participant ID (ParID). The ParID contains a list of de-identified field variables about the person's (Public Citizen) disposition which is; interview date, interview status, date of first contact and attempts, lead source, data collector IDs, user-name of person syncing and time. Data sets are then returned to the project area sites to use for their local analysis and reporting the national HIV database. Non-sensitive business contact and email address (Grantee) data is collected and stored to create their system user accounts to receive their unique user-id from the DCC administrator by email. (Grantee) user access to this application is authenticated via user-id and password. (CDC) user access is authenticated via Personal Identity Verification (PIV) and Active Directory (AD) for Single-Sign On (SSO). AD is a system with its own PIA.

Save

13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	DCC is a DHAP vendor developed application, designed to sync and receive critical MMP fielding information collected and supported by the NHBS and MMP project area sites. During each collecting period, only variables unique to the DCC identifiers will be available to CDC project staff for HIV data management and report generation. DCC primary objectives are to: 1) Receive sync data from the MMP Tracking Module collected by MMP project area sites over a secure encrypted internet connection; 2) Process received data for quality assurance and error correction; 3) Create and transfer cumulative and final data sets to CDC and to project area sites; 4) Provide ad-hoc technical assistance to National HIV Behavioral Surveillance (NHBS) and Medical Monitoring Project (MMP) area sites; 5) Provide formal training sessions for NHBS and MMP project area staff; and 6) Communicate with and report to CDC DHAP. The types of data DCC collects and stores from NHBS and MMP area sites are; person name, birth-date, sex at birth, year of birth, birth county, gender, race, ethnicity and MMP Participant ID (ParID). The ParID contains a list of de-identified field variables about the person's (Public Citizen) disposition which is; interview date, interview status, date of first contact and attempts, lead source, data collector IDs, user-name of person syncing and time. Data sets are then returned to the project area sites to use for their local analysis and reporting the national HIV database. Non-sensitive business contact and email address (Grantee) PII data is collected and stored to create their system user accounts to receive their unique user-id from the DCC administrator by email. External (Grantee) user access to this application is authenticated via user-id and password. Internal (CDC) user access is authenticated via PIV and AD for SSO. AD has its own PIA.
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 User ID and Password City, State and Zipcode sex at birth, year of birth, birth county, gender, race, and ethnicity
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: Grantees
17	How many individuals' PII is in the system?	100,000-999,999
18	For what primary purpose is the PII used?	PII (Public Citizen): data will be used for surveillance and reporting of cumulative HIV data to CDC. Business contact and Email (Grantee): will be used to create user accounts and to receive their unique user-id email from the DCC administrator for system identification and authorization.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	To control external (Grantee) access to DCC application for technical assistance, training and communication with DHAP.
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); and Sections 304, 306 and 308(d) which discuss authority to maintain data and provide assurances of confidentiality for health research and related activities (42 U.S.C. 242 b, k, and m(d)).

Save

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.	TBD
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.	The process to notify individuals is having project participants (Grantee) sign a Medical Monitoring Project Statement of Informed Consent form which notifies the individual about what type of personal information will be collected. (Public Citizen) are notified by their state and local health departments, HIV Surveillance Programs.
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.	(Grantee) participation in the DCC application is strictly voluntary. The method at the local, state level, individuals (Public Citizen) have the option to decline to answer any of the interview questions, therefore, they would not have to provide their education status.
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.	The process to notify and obtain consent in the event of major changes, the individual project area sites have contact information available to notify participants (Grantee) and obtain additional consent if the need arises. (Public Citizen) are notified by their state and local health departments, HIV Surveillance Programs.

Save

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.	The informed consent document contains information for (Grantee) contacting the appropriate individuals or organizations should they have questions/concerns about their PII. Individuals (Public Citizen) can also contact their state and local health departments, HIV Surveillance Programs for assistance.	
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.	The process is each project area (Grantee) is responsible for securing and maintaining their MMP datasets on secure drives and managing access to the data. They follow their local data destruction policies regarding any data they may have collected in addition to the final dataset in the course of their routine surveillance activities. They also follow their local policies and procedures for conducting routine reviews of the data to ensure availability, integrity, and access to the data. Accuracy is assured by CDC when they receive the dataset. CDC receives a final national dataset and maintains these annual datasets on secure CDC data drives. Annual security/ privacy reviews are conducted to control access and availability of the data to CDC users. Integrity is ensured by CDC's routine back-ups.	
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	Users need access to monitor HIV (Public Citizen) data then sync this data to DCC for CDC to analyze and document.
		☒ Administrators	To control access to the system by creating user (Grantee) accounts then emailing unique user ids to the user.
		☐ Developers	
		☒ Contractors	(Direct Contractor) To control access to the system by creating user (Grantee) accounts then emailing unique user ids to the user.
		☐ Others	
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	There are three roles in DCC, System Administrator, Analyst and Data Entry. The System Administrator role determines who has access to PII through access control list (ACL). Role-based access controls (RBAC) are configured so that each user (Grantee) could access only the data necessary for the user's role. System Administrator may access (Grantee) PII used during account creation, or if technical assistance is provided to the user. Data Analyst and Entry users (Grantee) roles only access (Public Citizen) PII which they have uploaded to the tracking module for processing.	
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.	The least-privilege model is utilized to ensure those with access to PII only have access to the minimum amount of data assigned to them by access-level (i.e., read, write, full) necessary to perform their job.	

Save

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.	(System Admin/Data Analyst/Entry): Annual CDC Security and Privacy Awareness Training (SAT). Individual MMP Sites (Grantee) are required to complete their organization specific Security Awareness training.
35	Describe training system users receive (above and beyond general security and privacy awareness training).	N/A
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.	Internal (CDC users) are required to use the CDC Records Control Schedule. The applicable section is General Records Schedule (GRS) 4.2: Information Access and Protection Records which states destruction when 3 years old, but longer retention is authorized if needed for business use. Information that would permit identification of any individual or establishment is collected with a guarantee that it will be held in confidence, will be used only for purposes stated in reporting forms, and will not be otherwise disclosed or released without the consent of the individual or the establishment in accordance with Sections 306 and 308(d) of the Public Health Service Act (42 USC 242K and 252m, {d}). Access to the data set is limited to members of the Division of HIV/AIDS performing activities or analysis supporting public health activities. Appeal is to the Director, Division of HIV/AIDS, NCHSTP, or Director, CDC. CDC doesn't access the PII, CDC data sets are encrypted when submitted to the Data Portal. No information will be disclosed to the public, parties involved in civil, criminal, or administrative litigation, or non-public-health agencies of the federal, state, or local government. The MMP project area sites are required to follow their organization specific records retention schedules for the retention and destruction of (Grantee) PII data. Retention and destruction of (Public Citizen) data process is handled by their state and local health departments, HIV Surveillance Programs.

Save

38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Administrative: The MMP project area sites are responsible for following their organization specific security procedures, which at a minimum include restricting access to the PII to only authorized (Grantee) users. CDC users are required to follow CDC, HHS, and OMB policies and procedures for protecting PII information. This includes restricting access to PII following approved access control list (ACL). Technical: Users (Grantee) can only access the application via unique user-id and password authentication. The application is set to automatically log off the when left unattended. The application utilizes role-based access controls. PII (Public Citizen) data is further protected by implementing encryption for data while in transit and at rest. Physical: DCC data centers housing the electronic data are protected with locked doors to the server rooms, in some cases, closed circuit tv may be used to monitor the facility, in other facilities, guards are posted at the front entrance to restrict access to the building to only authorized DCC individuals.

General Comments	Q10: C.2.8.9: PII Data Categorization change from Low to Moderate

OPDIV Senior Official for Privacy Signature	Jarell Oshodi -S Digitally signed by Jarell Oshodi -S Date: 2021.03.02 12:39:39 -05'00'