




Copy PIA (Privacy Impact Assessment)

Do you want to copy this PIA ?

Please select the user, who would be submitting the copied PIA.

Instructions

Review the following steps to complete this questionnaire:

- 1) Answer questions.** Select the appropriate answer to each question. Question specific help text may be available via the  icon. If your answer dictates an explanation, a required text box will become available for you to add further information.
- 2) Add Comments.** You may add question specific comments or attach supporting evidence for your answers by clicking on the  icon next to each question. Once you have saved the comment, the icon will change to the  icon to show that a comment has been added.
- 3) Change the Status.** You may keep the questionnaire in the "In Process" status until you are ready to submit it for review. When you have completed the assessment, change the Submission Status to "Submitted". This will route the assessment to the proper reviewer. Please note that all values list questions must be answered before submitting the questionnaire.
- 4) Save/Exit the Questionnaire.** You may use any of the four buttons at the top and bottom of the screen to save or exit the questionnaire. The button allows you to complete the questionnaire. The button allows you to save your work and close the questionnaire. The button allows you to save your work and remain in the questionnaire. The button closes the questionnaire without saving your work.

Acronyms

- ATO - Authorization to Operate
- CAC - Common Access Card
- FISMA - Federal Information Security Management Act
- ISA - Information Sharing Agreement
- HHS - Department of Health and Human Services
- MOU - Memorandum of Understanding
- NARA - National Archives and Record Administration
- OMB - Office of Management and Budget
- PIA - Privacy Impact Assessment
- PII - Personally Identifiable Information
- POC - Point of Contact
- PTA - Privacy Threshold Assessment
- SORN - System of Records Notice
- SSN - Social Security Number
- URL - Uniform Resource Locator

Does this need to migrate to a Sub-Component?:

Consolidated Parent Component

Component Name

No Records Found

General Information

PIA Name:	CDC - DCC - QTR1 - 2024 - CDC7960055	PIA ID:	7960055
Name of Component:	Data Coordinating Center	Name of ATO Boundary:	Data Coordinating Center

Migrated Sub-Component PIA

PIA Name

No Records Found

Sub-Component


Software Name

No Records Found

Original Related PIA ID

PIA Name

No Records Found

Overall Status:		PIA Queue:	
Submitter:	LAYNE, Carman	# Days Open:	202
Submission Status:	Re-Submitted	Submit Date:	7/25/2024
Next Assessment Date:	09/19/2027	Expiration Date:	9/19/2027
Office:	DDID	OpDiv:	CDC
Security Categorization:	Moderate		
Legacy PIA ID:		Make PIA available to Public?:	Yes
1:	Identify the Enterprise Performance Lifecycle Phase of the system		Operations and Maintenance
2:	Is this a FISMA-Reportable system?		Yes
3:	Does the system have or is it covered by a Security Authorization to Operate (ATO)?		No
4:	ATO Date or Planned ATO Date		7/1/2024

Privacy Threshold Analysis (PTA)

PTA Name

CDC - DCC - QTR1 - 2024 - CDC7950423

History Log: [View History Log](#)

PTA

PTA		
PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	System's single factor authentication (username and password) has been upgraded to SAMS two-factor authentication.
PTA - 3:	Is the data contained in the system owned by the agency or contractor?	Agency

PTA - 4:	Please give a brief overview and purpose of the system by describing what the functions of the system are and how the system carries out those functions.	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 basis. CDC uses these cumulative datasets to inform and instruct the internal data management processes.
PTA - 5:	List and/or describe all the types of information that are collected (into), maintained, and/or shared in the system regardless of whether that information is PII and how long that information is stored.	<p>The types of data DCC collects and stores from National HIV Behavioral Surveillance (NHBS) and MMP area sites are person's name, birthdate, 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, username 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.</p> <p>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 via Secure Access Management System (SAMS) authentication. Internal (CDC) user access is authenticated via Personal Identify Verification (PIV) and Active Directory (AD) for Single Sign On (SSO). AD and SAMS has its own PIA.</p>
PTA - 5A:	Are user credentials used to access the system?	Yes, but the user credentials are maintained in a sep
PTA - 5B:	Please identify the type of user credentials used to access the system.	

PTA - 6:	Describe why all types of information is collected (into), maintained, and/or shared with another system. This description should specify what information is collected about each category of individual.	<p>BUSINESS CONTACT DATA:</p> <p>Non-sensitive business contact and email address (Grantee) PII data is collected and stored to create their system user accounts and to receive their unique user-id from the DCC administrator by email.</p> <p>Name - to create their system user accounts. Email - to receive their unique user-id. Phone - user's phone number. Mailing address - user's mailing address User ID and Password - to access the application for surveillance data-set collection.</p> <p>De-identified field variables about the person's (Public Citizen) disposition, which includes interview date, interview status, date of first contact and attempts, lead source, data collector IDs, username of person syncing and time, are used for their local analysis and reporting the national HIV database.</p>
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	No
PTA - 8:	Does the system include a website or online application?	Yes
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?	No
PTA - 9:	Describe the purpose of the website, who has access to it, and how users access the web site (via public URL, log in, etc.). Please address each element in your response.	To train project areas interviewers to use a standardized, anonymous questionnaire to collect information on HIV-related risk behaviors, HIV testing, and the use of HIV prevention services. Interviewers are provided a URL to log into the training site.
PTA - 10:	Does the website have a posted privacy notice?	Yes
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?	No
PTA - 11A:	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?	
PTA - 12:	Does the website use web measurement and customization technology?	No
PTA - 12A:	Select the type(s) of website measurement and customization technologies in use and if it is used to collect PII.	
PTA - 13:	Does the website have any information or pages directed at children under the age of thirteen?	No
PTA - 13A:	Does the website collect PII from children under the age thirteen?	
PTA - 13B:	Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 14:	Does the system have a mobile application?	No
PTA - 14A:	Is the mobile application HHS developed and managed or a third-party application?	
PTA - 15:	Describe the purpose of the mobile application, who has access to it, and how users access it. Please address each element in your response.	
PTA - 16:	Does the mobile application/ have a privacy notice?	

PTA - 17:	Does the mobile application contain links to non-federal government website external to HHS?	
PTA - 17A:	Is a disclaimer notice provided to users that follow external links to resources not owned or operated by HHS?	
PTA - 18:	Does the mobile application use measurement and customization technology?	
PTA - 18A:	Describe the type(s) of measurement and customization technologies or techniques in use and what information is collected.	
PTA - 19:	Does the mobile application have any information or pages directed at children under the age of thirteen?	
PTA - 19A:	Does the mobile application collect PII from children under the age thirteen?	
PTA - 19B:	Is there a unique privacy policy for the mobile application and does the unique privacy policy address the process for obtaining parental consent if any information is collected?	
PTA - 20:	Is there a third-party website or application (TPWA) associated with the system?	No
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?	No

PIA		
PIA		
PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Name Email Address Phone numbers Date of Birth Mailing Address User Credentials Other - Free text Field - sex at birth, year of birth, bir
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Business Partners/Contacts (Federal, state, local agencies) Grantees Members of the public
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	Above 2000
PIA - 4:	For what primary purpose is the PII used?	(Public Citizen): PII data will be used for surveillance and reporting of cumulative human immunodeficiency virus (HIV) data to Centers for Disease Control and Prevention (CDC). (Grantee): Business contact and email will be used to create user accounts and to receive their unique user-id email from the Data Coordination Center (DCC) administrator for system identification and authorization.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	For technical assistance, training and program communication.
PIA - 6:	Describe the function of the SSN and/or Taxpayer ID.	N/A

PIA - 6A:	Cite the legal authority to use the SSN.	N/A
PIA - 7:	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)).
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	No
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	
PIA - 8B:	Provide the number, title, and URL of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or indicate whether a new or revised SORN is in development.	
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Email Government Sources State/Local/Tribal Non-Government Sources Members of the Public
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA - 10A:	Provide the information collection approval number.	OMB No: 0920-0740
PIA - 10B:	Identify the OMB information collection approval number expiration date.	5/31/2027
PIA - 10C:	Explain why an OMB information collection approval number is not required.	Provided
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11A:	Identify with whom the PII is shared or disclosed.	
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
PIA - 11C:	List any agreements in place that authorize the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	
PIA - 11D:	Describe process and procedures for logging/tracking/accounting for the sharing and/or disclosing of PII. If no process or procedures are in place, please explain why not.	
PIA - 12:	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
PIA - 12A:	If PII submission is mandatory, provide the specific legal requirement that requires individuals to provide information or face potential civil or criminal penalties.	
PIA - 13:	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, (Public Citizen) have the option to decline to answer any of the interview questions, therefore, they would not have to provide their education status.

PIA - 14:	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 and obtain consent by their state and local health departments, HIV Surveillance Programs.
PIA - 15:	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 process to resolve an individual's concerns is contained within the Medical Monitoring Project (MMP) Statement of Informed Consent form which provides information for contacting the appropriate individuals or organizations should they have questions about their PII. (Public Citizen) concerns are resolved by their state and local health departments, HIV Surveillance Programs.
PIA - 16:	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. Please address each element in your response. 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.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Contractors
PIA - 17A:	Select the type of contractor.	HHS/OpDiv Direct Contractors
PIA - 17B:	Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices?	Yes
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Users: 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. Direct Contractors: To control access to the system by creating user (Grantee) accounts then emailing unique user ids to the user.

PIA - 19:	Describe the administrative 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.
PIA - 20:	Describe the technical 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.
PIA - 21:	Identify the general security and privacy awareness training provided to system users (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.
PIA - 22:	Describe training system users receive (above and beyond general security and privacy awareness training).	N/A
PIA - 23:	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific National Archives and Records Administration (NARA) records retention schedule(s) and include the retention period(s).	<p>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.</p> <p>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.</p>

PIA - 24:

Describe how the PII will be secured in the system using administrative, technical, and physical controls. Please address each element in your response.

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.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	Privacy Analyst Review Date:	7/25/2024
Privacy Analyst Comments:	OpDiv Analyst: Joshua Mosios (Contractor)	Privacy Analyst Days Open:	

SOP Review

SOP Review Status:	Approved	SOP Signature:	JWO Signature.docx
SOP Comments:	Approved on behalf of Beverly Walker	SOP Review Date:	8/7/2024
		SOP Days Open:	13

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	Agency Privacy Analyst Review Date:	9/17/2024
Agency Privacy Analyst Review Comments:	This PIA is ready for SAOP review and approval.	Agency Privacy Analyst Days Open:	41

SAOP Review

SAOP Review Status:	Approved	SAOP Signature:	
SAOP Comments:		SAOP Review Date:	9/19/2024
		SAOP Days Open:	2

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
DCC HHS PIA_2212024.pdf	576794	.pdf	7/24/2024 11:34 AM	2

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 15	MOSIOS, Joshua	7/25/2024	What is described he is a notice process, not a resolution process. Please revise.	