


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 No
migrate to a Sub-
Component?:

Consolidated Parent Component

Component Name

No Records Found

General Information

PIA Name: CDC - 1CDP - QTR2 - 2024 - CDC8330238

PIA ID: 8330238

**Name of
Component:**

**Name of ATO
Boundary:** CDC OPHDST 1 CDC Data Platform

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:

VENTURA, Inocencia

Days Open:

25

Submission Status:

Submitted

Submit Date:

6/25/2024

Next Assessment Date:

07/19/2027

Expiration Date:

7/19/2027

Office:

DDPHSIS

OpDiv:

CDC

Security Categorization:

Moderate

Legacy PIA ID:

Make PIA available to Public?:

Yes

1:

Identify the Enterprise Performance Lifecycle Phase of the system

2:

Is this a FISMA-Reportable system?

3:

Does the system have or is it covered by a Security Authorization to Operate (ATO)?

4:

ATO Date or Planned ATO Date

8/19/2024

Privacy Threshold Analysis (PTA)

PTA Name

No Records Found

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.

Added Azure Active Directory (AD) as authentication in addition to Secure Access Management System (SAMS). No impact on system.

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 system collects, integrates, manages, analyzes, visualizes and shares traditional and non-traditional data sets used to support the management of all-hazards public health event responses, surveillance, research, statistical, and other public health activities. A system such as this that links and shares these data sets was identified as a critical gap in preparedness exercises and a common theme identified across response after action reports.

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.

The system collects, maintains and stores diverse types of data including epidemiological case data, laboratory test orders/results, outbreak and environmental investigations and any related supporting data, contact tracing, molecular data, population-based health information, and publicly accessible datasets.

The data contained in this platform, including PII, will be used to support and manage routine public health activities (e.g., surveillance, statistical analysis, research, etc.) and emergency event responses (e.g., outbreaks, disasters, etc.). Data will be used to describe

relationships and trends between population health and various health conditions and/or risk factors, as well as to inform public health event response decisions and management. Analysis and visualizations will be included in various reports, presentations, dashboards, and websites.

Information collected are names, phone numbers, email address, mailing address, Date of Birth, Medical Notes, Medical Record Numbers, Passport Number, and Employment Status.

The blanket answer is all of those data are collected to support program specific needs for conducting routine public health surveillance and to support outbreak response management operations.

All of those categories are not mutually exclusive either but live along a continuum. For example: Part of why programs collect epi surveillance and lab data is to assist with program or pathogen specific contract tracing for response purposes to any outbreak that may be occurring.

Yes, but the user credentials are maintained in a separate system (e.g., AD, AMS) and not collected or maintained by this system. The system providing credentials is - AD (Azure Active Directory)SAMS (Secure Access Management System)

HHS User Credentials
HHS/OpDiv PIV Card
HHS Email Address
HHS Username
Password

DCIPHER is a web-based data integration and management platform for use across CDC programs to 1-collate, 2-link, 3-manage, 4-analyze, 5-visualize, and 6-share data from multiple sources to facilitate data interpretation and to inform public health decisions. It collects, stores, and shares (as needed) epidemiological, surveillance, laboratory, environmental, personal identity, logistics, emergency response, population health, and general statistical information. It also manages a repository of historic surveillance, outbreak, emergency event response and other collected data.

The data contained in this platform, including PII, will be used to support and manage routine public health activities (e.g., surveillance, statistical analysis, research, etc.) and emergency event responses (e.g., outbreaks, disasters, etc.). Data will be used to describe relationships and trends between population health and various health conditions and/or risk factors, as well as to inform public health event response decisions and management. Analysis and visualizations will be included in various reports, presentations, dashboards, and websites.

The blanket answer is all of those data are collected to support program specific needs for conducting routine public health surveillance and to support outbreak response management operations.

All of those categories are not mutually exclusive either but live along a continuum. For example: Part of why programs collect epi surveillance and lab data is to assist with program or pathogen specific contract tracing for

- PTA - 5A:** Are user credentials used to access the system?
- 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.

response purposes to any outbreak that may be occurring.

A Memorandum of Understanding will be signed by CDC programs that want to use DCIPHER that outlines program-level responsibilities, including the use and treatment of PII, the adherence to records retention policies and procedures and Office of Management and Budget (OMB) and Paperwork Reduction Act (PRA) responsibilities.

PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	Yes
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.	The website is accessible to public health officials and the system is accessible via SAMS for login. DCIPHER SaaS is a web-based data integration and management platform for use across CDC programs to 1-collate, 2-link, 3-manage, 4-analyze, 5-visualize, and 6-share data from multiple sources to facilitate data interpretation and to inform public health decisions. It collects, stores, and shares (as needed) epidemiological, surveillance, laboratory, environmental, personal identity, logistics, emergency response, population health, and general statistical information. It also manages a repository of historic surveillance, outbreak, emergency event response and other collected data.
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 Medical Records Number Employment Status Passport Number Other - Free text Field - Medical Notes (not PHI)
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Business Partners/Contacts (Federal, state, local agencies) Employees/ HHS Direct Contractors Patients
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	501 - 2000
PIA - 4:	For what primary purpose is the PII used?	PII will be used to support and manage public health event responses and routine public health activities in the response to the COVID-19 pandemic.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	PII will also be used to support research projects as authorized/ initiated by the respective programs that own the data. Further, data will be used to describe relationships and trends between population health and various health conditions and/ or risk factors, as well as to inform public health event response decisions and management.
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); sections 304, 306, and 308(d), which discuss authority to grant assurances of confidentiality for health research and related activities (42 U.S.C. 242 b, k, and m(d)); and section 361, "Quarantine and Inspection, Control of Communicable Diseases (42 U.S.C. 264).
PIA - 8:	Are records in the system retrieved by one or more PII data elements?	Yes
PIA - 8A:	Please specify which PII data elements are used to retrieve records.	Name, Medical Record Number,
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.	09-20-0113-Epidemic Investigation Case Records, 09-20-0136 Epidemiologic Studies and Surveillance of Disease Problems, 09-20-0106-Specimen Handling for Testing and Related Data 09-20-0171-Quarantine and Traveler Related Activities, Including Records for Contact Tracing Investigation and Notification
PIA - 9:	Identify the sources of PII in the system.	Government Sources

		<p>Within the OPDIV</p> <p>Other HHS OPDIV</p> <p>State/Local/Tribal</p> <p>Other Federal Entities</p>
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	No
PIA - 10A:	Provide the information collection approval number.	
PIA - 10B:	Identify the OMB information collection approval number expiration date.	
PIA - 10C:	Explain why an OMB information collection approval number is not required.	N/A, PII not being collected directly from the public.
PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	Yes
PIA - 11A:	Identify with whom the PII is shared or disclosed.	<p>Other Federal Agency/Agencies</p> <p>State or Local Agency/Agencies</p> <p>Within HHS</p>
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	<p>Within HHS- To support and manage public health event responses and routine public health activities at the state/local/tribal level.</p> <p>Other Federal Agency/Agencies- To support and manage public health event responses and routine public health activities at the federal level.</p> <p>State or Local Agency/Agencies- To support and manage public health event responses and routine public health activities at the state/local/tribal level.</p>
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)).	DCIPHER SaaS will have an MOU in place with CDC Center for Preparedness and Response (CPR) Personnel Workforce Management System (PWMS) that allows the sharing of information from PWMS to DCIPHER SaaS. DCIPHER SaaS also has Data Use Agreements (that define system to system connections) and Program Engagement Agreements (that define the program-to-program responsibilities and relationships) with the various systems and program providing data to DCIPHER SaaS. These agreements place responsibility with the program to manage their own data, and share appropriately with states and locals based on the policies, procedures, and agreements in place within the participating program.
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.	Data disclosures ("data export events") from DCIPHER SaaS are tracked by the audit/traceability functionality provided within DCIPHER SaaS
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.	DCIPHER SaaS receives its information from other systems, and those source systems are responsible for providing methods for individuals to opt out of the collection or use of their PII.
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.	PII data are collected by State/Local/Tribal Public Health Departments and are submitted to CDC in support of public health surveillance, investigation, and response activities. In the event a major system change significantly alters the disclosure and/or use of PII maintained in the system, DCIPHER SaaS will notify the participating CDC programs and external partners, with whom we exchange data and maintain Data User Agreements and Program Engagement agreements, of

		the change so they can take appropriate action to notify their program partners, such as states, and obtain consent from the affected individuals.
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.	To report and resolve concerns, individuals can contact the POC listed in this form, who will notify the relevant program lead. The communication should reasonably identify the record and specify the information being contested, the corrective action sought, and the reasons for requesting the correction, along with supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant.
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.	DCIPHER SaaS provides participating CDC programs and external partners with an interface to review all data and PII and programs/external partners can conduct their own reviews as needed or as consistent with their existing policies. This program responsibility, including the reminder that the program is responsible for these periodic audits, is written into the DCIPHER Program Engagement Agreement, signed by the participating programs, as a responsibility delegated to the participating programs and is further codified in the Data Use Agreement that each program lead signs as part of the on-boarding process for DCIPHER SaaS.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators Developers Contractors Others HHS/OpDiv Direct Contractors
PIA - 17A:	Select the type of contractor.	
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- Program users will need access to the PII in their specific data sources in order to carry out their regular job duties. Administrators- Administrators will need to assist in mapping incoming data into the platform. Developers-Developers will need to appropriately map incoming data into the platform, perform validation checks, build ontology. Contractors-Indirect Contractors are used on this project for design, development, configuration, customization and maintenance. Other- State/local/tribal users who are owners of PII will need to access their data in order to carry out their regular job duties.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	System user access to PII is determined and managed by role-based system access, audit trail, and traceability.
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.	DCIPHER SaaS utilizes a model that allows CDC administrators to assign individual security labels and permissions to every piece of data ingested into the platform at the object, property, and relationship level. CDC administrators create unique profiles for each user and assign users to groups and subgroups and determine controls and clearance levels associated with each user and group based on the least privileged model.

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.	All CDC employees, contractors and fellows are required to complete Privacy and Security Awareness Training on an annual basis.
PIA - 22:	Describe training system users receive (above and beyond general security and privacy awareness training).	All DCIPHER SaaS users receive Role-Based Training for DCIPHER SaaS.
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).	Processes and guidelines with regard to the retention and destruction of PII varies and is dependent upon the individual systems from which the data comes. Each program using DCIPHER SaaS is responsible for applying its own existing records retention schedules to PII data, and schedules will vary across programs. This program responsibility as to following their defined records retention procedures is written into the DCIPHER White House Response (WHR) Program Engagement Agreement (PEA) that each program lead signs as part of the on-boarding process for DCIPHER SaaS which identifies the participating program as responsible (and not DCIPHER SaaS) for any and all retention related requirements with respect to their data. DCIPHER can be further configured to support automated and semi-automated deletions in accordance with program requirements as laid out in the PEA.
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.	<p>Administrative Controls:</p> <p>PII is secured in the system via FISMA compliant Management, Operational, and Technical controls documented in the systems security authorization package. Management Controls include Federal, HHS, and CDC specific Privacy, Risk Assessment, and Incident Management Policies, as well as, annual system privacy impact assessments; maintaining security & privacy incident response procedures; and mandatory annual security & privacy awareness training;</p> <p>Technical Controls include application level role-based access controls; column and row level data security; server audit and accountability measures; encryption of PII at rest and in transit; and adherence to organizationally defined minimum security controls including anti-virus and adherence to period system software security tests.</p> <p>Physical Controls include security guards at every facility, and physical facilities management by restricting access to the data center to authorized personnel.</p>

Review & Comments

Privacy Analyst Review			
OpDiv Privacy Analyst Review Status:	Approved	Privacy Analyst Review Date:	6/26/2024
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:	7/15/2024
		SOP Days Open:	20

Agency Privacy Analyst Review			
Agency Privacy Analyst Review Status:	Approved	Agency Privacy Analyst Review Date:	7/18/2024
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 7/18/2024 This PIA is ready for SAOP review and approval. Comments were for the next iteration of the PTA and one minor comment for spelling out FISMA (which I let slide but a comment has been noted) .		
		Agency Privacy Analyst Days Open:	3

SAOP Review			
SAOP Review Status:	Approved	SAOP Signature:	
SAOP Comments:	Comments were for the next iteration of the PTA and one minor comment for spelling out FISMA	SAOP Review Date:	7/19/2024
		SAOP Days Open:	1

Supporting Document(s)				
Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments				
Question Name	Submitter	Date	Comment	Attachment
PIA - 1	MOSIOS, Joshua	6/26/2024	Selected "name" and deselected "medical records (PHI)". Replaced with "medical notes (not PHI)" in the free text field.	
PIA - 1	Data Feed Service, Sync2PIAForm	7/17/2024	PTA-2A - Please add that Azure AD is also used for authentication throughout the PTA/PIA.	
PIA - 24	Data Feed Service, Sync2PIAForm	7/17/2024	Please define acronym FISMA in its first instance.	
PIA - 1	Data Feed Service, Sync2PIAForm	7/18/2024	Per previous comment, on the next iteration of the PTA: PTA-5 and PTA-9: Please make sure to include both SAMS and Azure AD as systems used for access control and authentication. PTA-5A: Select "Yes, but user credentials are maintained by another system."	