Save

# Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-44232 | Form Date: 11/19/2020 8:51:04 AM

| | Question | Answer |
|---|---|---|
| 1 | OPDIV: | CDC |
| 2 | PIA Unique Identifier: | P-4137049-320366 |
| 2a | Name: | Data Collation and Integration for Public Health Event Responses (DCIPHER) |
| 3 | The subject of this PIA is which of the following? | ○ General Support System (GSS)<br>○ Major Application<br>○ Minor Application (stand-alone)<br>◉ Minor Application (child)<br>○ Electronic Information Collection<br>○ Unknown |
| 3a | Identify the Enterprise Performance Lifecycle Phase of the system. | Operations and Maintenance |
| 3b | Is this a FISMA-Reportable system? | ○ Yes<br>◉ No |
| 4 | Does the system include a Website or online application available to and for the use of the general public? | ○ Yes<br>◉ No |
| 5 | Identify the operator. | ◉ Agency<br>○ Contractor |
| 6 | Point of Contact (POC): | POC Title: Laboratory Information Management System (LIMS) Scientific Advisor and Coordinator<br>POC Name: Stephen Soroka<br>POC Organization: NCEZID/OD<br>POC Email: znk0@cdc.gov<br>POC Phone: 404-639-0417 |
| 7 | Is this a new or existing system? | ◉ New<br>○ Existing |
| 8 | Does the system have Security Authorization (SA)? | ○ Yes<br>◉ No |

Save

| | | |
|---|---|---|
| 8b | Planned Date of Security Authorization | January 29, 2021<br>☐ Not Applicable |
| 11 | Describe the purpose of the system. | Data Collation and Integration for Public Health Event Responses (DCIPHER) will collect, integrate, manage, analyze, visualize and share 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. The ability to electronically integrate and link data from multiple sources is repeatedly identified as a critical gap in preparedness exercises and a common theme identified across Response After Action Reports. DCIPHER addresses this gap. |
| 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 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.<br><br>Specific information collected consists of name, email, mailing address, telephone number, medical notes, date of birth, medical records number, employment status, HHS User ID, passport number, statistical analysis, and research information of public health events.<br><br>All users authenticate via CDC's Digital Support Office - Secure Access Management System (SAMS). SAMS is a separate 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. | 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.<br><br>DCIPHER 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. Specifically, the system maintains patient demographic information with name, email, mailing address, telephone number, medical notes, date of birth, medical records number, employment status, and passport number. Currently, information is primarily used in support of COVID19 pandemic activity along with other emergency and routine surveillance, statistical analysis, and research information for public health events.<br><br>Data maintained in this platform is 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 further 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. HHS User ID is used to identify the CDC employee accessing the data collections.<br><br>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 OMB/Paperwork Reduction responsibilities.<br><br>All users authenticate via CDC's Digital Support Office - Secure Access Management System (SAMS). SAMS is a separate system with its own PIA. |
| 14 | Does the system collect, maintain, use or share **PII**? | (•) Yes<br>( ) No |

Save

| | | |
|---|---|---|
| 15 | Indicate the type of PII that the system will collect or maintain. | ☐ Social Security Number<br>☒ Date of Birth<br>☒ Name<br>☐ Photographic Identifiers<br>☐ Driver's License Number<br>☐ Biometric Identifiers<br>☐ Mother's Maiden Name<br>☐ Vehicle Identifiers<br>☒ E-Mail Address<br>☒ Mailing Address<br>☒ Phone Numbers<br>☒ Medical Records Number<br>☒ Medical Notes<br>☐ Financial Account Info<br>☐ Certificates<br>☐ Legal Documents<br>☐ Education Records<br>☐ Device Identifiers<br>☐ Military Status<br>☒ Employment Status<br>☐ Foreign Activities<br>☒ Passport Number<br>☐ Taxpayer ID<br>User ID |
| 16 | Indicate the categories of individuals about whom PII is collected, maintained or shared. | ☒ Employees<br>☒ Public Citizens<br>☐ Business Partners/Contacts (Federal, state, local agencies)<br>☐ Vendors/Suppliers/Contractors<br>☒ Patients<br>Other |
| 17 | How many individuals' PII is in the system? | 1,000,000 or more |
| 18 | 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. |
| 19 | Describe the 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.<br><br>HHS User Credential: To identify the CDC employee accessing collection of data.<br><br>Physicians enrolled in the program use PII for quality assurance, research and to support determinations related to drug administration. |
| 20 | Describe the function of the SSN. | Not Applicable. SSNs are not collected. |
| 20a | Cite the **legal authority** to use the SSN. | N/A |

Save

| | | |
|---|---|---|
| 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); sections 304, 306, and 308(d), 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). |
| 22 | Are records on the system retrieved by one or more PII data elements? | (•) Yes<br>( ) 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: 09-90-2001 Records Used for Surveillance and Study of Epidemics, Preventable Diseases and Problems<br>Published: 09-20-0136 Epidemiologic Studies and Surveillance of Disease Problems<br>Published: 09-20-0106- Specimen Handling for Testing and Related Data;<br>09-20-0171: Quarantine and Traveler Related<br>☐ In Progress |
| 23 | Identify the sources of PII in the system. | Directly from an individual about whom the information pertains<br>☐ In-Person<br>☐ Hard Copy: Mail/Fax<br>☐ Email<br>☐ Online<br>☐ Other<br>Government Sources<br>☒ Within the OPDIV<br>☒ Other HHS OPDIV<br>☒ State/Local/Tribal<br>☐ Foreign<br>☐ Other Federal Entities<br>☐ Other<br>Non-Government Sources<br>☐ Members of the Public<br>☐ Commercial Data Broker<br>☐ Public Media/Internet<br>☐ Private Sector<br>☐ Other |

Save

| | | |
|---|---|---|
| 23a | Identify the OMB information collection approval number and expiration date. | As it relates to COVID-19 information collections, the following applies: Pursuant to section 319 of the Public Health Service (PHS) Act, 42 U.S.C. 247d, Secretary Alex M. Azar, II determined that, as the result of the confirmed cases of 2019 Novel Coronavirus (2019-nCoV), now known as Coronavirus Disease 2019 (COVID-19), a public health emergency (PHE) has existed nationwide since January 27, 2020. As a result of the PHE, the Secretary also determined pursuant to section 319(f) of the PHS Act that circumstances of the PHE necessitate a waiver from the requirements of the Paperwork Reduction Act, 44 U.S.C. § 3501 et seq., effective as of the date of this notice. The waiver is justified to collect information to support the Department of Health and Human Services' investigation of and response to the COVID-19 pandemic. This waiver applies to information to be collected by the Centers for Disease Control and Prevention from individuals, healthcare providers, states, and other partners in order to a facilitate rapid response to the PHE.<br><br>Overall and for information collections other than those related to COVID-19, each participating program signs a Program Engagement Agreement with DCIPHER that delegates responsibility to the participating program for designing its own data collection tools and obtaining OMB approval, if required. For example, the Division of STD Prevention has their own OMB compliance procedures and obtained collection approvals on their own for the Enhanced STD Surveillance Network (SSuN), (OMB Control No. 0920-1072 Exp. 09/30/2021)—Revision—National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention (NCHHSTP), Centers for Disease Control and Prevention (CDC), and Gonococcal Isolate Surveillance Project (GISP) (OMB control 0920-0307 exp 08/31/2021) data collection tools. |
| 24 | Is the PII shared with other organizations? | ◉ Yes<br>○ No |
| 24a | Identify with whom the PII is shared or disclosed and for what purpose. | ☐ Within HHS<br>☐ Other Federal Agency/Agencies<br>☒ State or Local Agency/Agencies<br>To support and manage public health event responses and routine public health activities at the state/local/tribal level. CDC programs have the ability to both receive and share PII data from/with their state/local/territorial/tribal counterparts and it is up to each CDC program to decide when receiving and/or sharing PII is needed.<br>☐ Private Sector |

Save

| | | |
|---|---|---|
| 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)). | DCIPHER has Data Use Agreements (DUA) in place for all direct system to system connections. The DUA defines how the data will be accessed, the direction(s) of the data flow, whether PII will be shared, and the process for new users to access the data in DCIPHER, which are all defined by the participating program (for example, some programs want the new user approving point of contact to be listed in the DUA; others do not). These agreements collectively 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. |
| 24c | Describe the procedures for accounting for disclosures | The DCIPHER Business Steward defers to the participating program to confirm and process information disclosure requests. DCIPHER accepts approved requests as provided by the program and releases the data through the participating program for appropriate distribution. DCIPHER will only release information as directed by the participating program. |
| 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 processes in place will vary by program and use and it is up to each program to utilize its own existing processes to notify individuals that their personal information will be collected or not. This program responsibility is written into the DCIPHER Program Engagement Agreement that each program lead signs as part of the on-boarding process for DCIPHER which identifies the participating program as responsible (and not DCIPHER) for any and all privacy related requirements with respect to their data. Based on the method of data collection, this responsibility will lie with either the CDC program or with the states contributing data to the CDC program, but this determination of responsibility is made outside the scope of DCIPHER. |
| 26 | Is the submission of PII by individuals voluntary or mandatory? | (•) Voluntary<br>( ) 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. | The methods will vary by program and use and it is up to each program to provide an opt-out method (or not) for the collection or use of their PII. This program responsibility is written into the DCIPHER Program Engagement Agreement that each program lead signs as part of the on-boarding process for DCIPHER which identifies the participating program as responsible (and not DCIPHER) for any and all privacy related requirements with respect to their data. Based on the method of data collection, this responsibility will lie with either the CDC program or with the states contributing data to the CDC program, but this determination of responsibility is made outside the scope of DCIPHER. |

Save

| | | |
|---|---|---|
| 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. | If a CDC program is initiating a data collection that includes PII then the consent responsibility rests with that CDC program. Similarly, if PII data are collected by State/Local/Territorial/ Tribal Public Health Departments and are submitted to CDC in support of public health surveillance, investigation, and response activities, then responsibility for obtaining consent (or determining that consent is unneeded) rests with the State/ Local/Territorial/Tribal jurisdiction In the event a major system change significantly alters the disclosure and/or use of PII maintained in the system, DCIPHER will provide written notice to the participating CDC programs and external partners, with whom we exchange data and maintain PEAs and/or DUAs, of the change so they can take appropriate action to notify their program partners, such as states, and obtain consent from the affected individuals. |
| 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. | To report and resolve concerns, individuals can contact the POC listed in this form, who will notify the relevant program lead. The correspondence 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. |
| 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. | DCIPHER 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. |
| 31 | Identify who will have access to the PII in the system and the reason why they require access. | ☒ Users: Program users will need access to the PII in their specific data sources in order to carry out their regular job duties.<br>☒ Administrators: Administrators will need to assist in mapping incoming data into the platform.<br>☒ Developers: Developers will need to appropriately map incoming data into the platform, perform validation checks, build ontology.<br>☒ Contractors: Direct Contractors are used on this project for design, development, configuration, customization and maintenance.<br>☒ Others: State/local/tribal users who are owners of PII will need to access their data in order to carry out their regular job duties. |

Save

| | | |
|---|---|---|
| 32 | Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII. | The Business Steward is limiting access to the smallest possible number of people necessary to access PII data for conducting official responsibilities through specific Role-based requirements. If the individual's manager determines that access to the system is required for the individual to perform their regular duties, they will make a request to the system administrator who will establish an account for the user to access the system. Access to PII is strictly enforce by setting up user profile on the Principle of Least Privilege and a Need To Know standard. Individuals can only see selected functions and information that are necessary for its valid purpose based on their user profile.<br><br>System Administrators in coordination with the Business Steward will assign designated personnel for read/write to data fields and Subject Matter Experts to analyze transactional user's access, monitor process and protocols used, control asset inventory.<br><br>The HHS credentialed employee PII data is identified as non-Sensitive Internal Business information (Identified by name and CDC issued UserID) and limited to authorized Administrators and Subject Matter Experts. |
| 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. | Least privilege, Role Based Access methods are used to allow those with access to PII to only access the minimum amount of information necessary to perform their job. The system administrator is responsible for setting up the user access to the system based on the CDC user ID and the permissions assigned to it. |
| 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. | All CDC personnel are required to complete annual Security and Privacy Awareness Training. |
| 35 | Describe training system users receive (above and beyond general security and privacy awareness training). | All CDC employees who have significant security responsibilities are required to complete HHS/CDC Role based training. |
| 36 | Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices? | (●) Yes<br>( ) No |
| 37 | Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules. | Each program using DCIPHER is responsible for applying its own existing records retention schedules to PII data, and schedules will vary across programs.<br><br>Specific to DCIPHER, the records are maintained in accordance with General Records Schedule (GRS) and comply with CDC Records Control Schedule (RCS). Input/output records are disposed of when no longer needed: GRS 20.2d and 20.6. Disposal methods include erasing computer tapes, burning or shredding paper materials or transferring records to the Federal Records Center when no longer needed for evaluation and analysis. |

Save

| | | |
|---|---|---|
| 38 | Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls. | Administrative controls: Completion of training requirements; risk analyses performed annually; branch management reviewing access requests and granting minimal amount of access.<br><br>Technical controls: Users are authenticated and data secured using operating system and server security, administered by the local system administrator. DCIPHER's user access and authentication is controlled by CDC's Secure Access Management System. PII data is encrypted at rest and in transits with access restricted to specific authorized users as required by HHS and CDC policy.<br><br>Physical: The server is housed on CDC property with gate guards at the entrances to the property, individual user access credentials are required for each non-public building, floor, and office. Closed Circuit TV is also used by the internal security guards to check for and grant access to authorized individuals. All components of the DCIPHER system reside in CDC managed data center. |
| General Comments | | Q10: Data Collation and Integration for Public Health Event Responses DCIPHER) and System for Enteric Disease Response, Investigation, and Coordination (SEDRIC) (ESC 1771) merged into one system. SEDRIC utilized coded data (No PII) by joining epidemiologic and laboratory data in real time; and enhanced electronic information sharing of surveillance, outbreak, recall, and other data among local, state, and federal partners during multi-state foodborne disease outbreak investigations. SEDRIC is a retired system effective 19 February 2019.<br><br>DCIPHER has started the process of migrating to a cloud environment by migrating all COVID related data and processes to HHS Protect system. DCIPHER is currently in the midst of planning for a full cloud migration for all DCIPHER programs and data to either the HHS-managed, HHS Protect or a CDC managed DCIPHER Cloud. |
| OPDIV Senior Official for Privacy Signature | | Beverly E. Walker -S<br>Digitally signed by Beverly E. Walker -S<br>Date: 2021.01.12 16:45:13 -05'00' |