Save

Privacy Impact Assessment Form

v 1.47.4

Status Draft | Form Number F-98249 | Form Date 5/7/2020 9:09:23 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-3384913-347360
2a	Name:	DCIPHER SaaS (DCIPHER SaaS)
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.	
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: Laboratory Information Management System (LIMS) Scientific Advisor and Coordinator POC Name: Stephen Soroka POC Organization: NCEZID/OD POC Email: znk0@cdc.gov POC Phone: 404-639-0417
7	Is this a new or existing system?	(•) New ( ) Existing
8	Does the system have Security Authorization (SA)?	( ) Yes (•) No

Save

8b	Planned Date of Security Authorization	July 8, 2020 ☐ Not Applicable
11	Describe the purpose of the system.	Data Collation and Integration for Public Health Event Responses Software as a Service (DCIPHER SaaS) is a cloud-
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.)	DCIPHER SaaS is a cloud-based data integration and management platform for use across CDC, in the Emergency Operations Center (EOC), by other federal partners, and by state, local, tribal, and territorial public health jurisdictions to:
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	DCIPHER SaaS is a cloud-based data integration and management platform for use across CDC, in the Emergency Operations Center (EOC), by other federal partners, and by
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 ☒ 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
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: potential or suspect patients, contacts of patients
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 in the response to the COVID-19 pandemic.

Save

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. 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.	
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); 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).	
22	Are records on the system retrieved by one or more PII data elements?	(•) Yes ( ) 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: 09-20-0113-Epidemic Investigation Case Records Published: 09-20-0136 Epidemiologic Studies and Surveillance of Disease Problems Published: 09-20-0106-Specimen Handling for Testing and Related Data 09-20-0171-Quarantine and Traveler Related Activities, Including Records for ☐ In Progress	

Save

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.	N/A, PII not being collected directly from the public.
24	Is the PII shared with other organizations?	◉ Yes ○ No
24a	Identify with whom the PII is shared or disclosed and for what purpose.	☒ Within HHS To support and manage public health event responses and routine public health activities at the state/local/tribal level. ☒ Other Federal Agency/Agencies To support and manage public health event responses and routine public health activities at the federal level. ☒ State or Local Agency/Agencies To support and manage public health event responses and routine public health activities at the state/local/tribal level. ☐ 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 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.
24c	Describe the procedures for accounting for disclosures	Data disclosures ("data export events") from DCIPHER SaaS are tracked by the audit/traceability functionality provided within DCIPHER SaaS .
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.	N/A. DCIPHER SaaS receives individuals PII from other systems. Therefore, it is the responsibility of the originating systems to provide notifications to individuals that their personal information is being collected.
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.	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.
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.	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 WHR 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.
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 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.

Save

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 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 .	
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.
		☒ 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.
		☒ 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.
32	Describe the 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.	
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.	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.	
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 employees, contractors and fellows are required to complete Privacy and Security Awareness Training on an annual basis.	
35	Describe training system users receive (above and beyond general security and privacy awareness training).	All DCIPHER SaaSusers receive Role-Based Training for DCIPHER SaaS .	
36	Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	◉ Yes ○ No	

Save

37	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.	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 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.
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Administrative Controls: 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; 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. Physical Controls include security guards at every facility, and physical facilities management by restricting access to the data center to authorized personnel.
General Comments		
OPDIV Senior Official for Privacy Signature	Jarell Oshodi -S Digitally signed by Jarell Oshodi -S Date: 2020.05.12 08:59:23 -04'00'	