Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-14959 | Form Date: 9/18/2019 10:24:15 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-1607737-379253
2a	Name:	Emerging Infections Program Clostridium Difficile Infection Incident Case Management System (EIP CDI ICMS)
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: ELC PROGRAM COORDINATOR POC Name: Alvin Shultz POC Organization: NCEZID POC Email: fcu9@cdc.gov POC Phone: 404-639-7028
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	December 12, 2019 ☐ Not Applicable

Save

11	Describe the purpose of the system.	The CDC's Division of Preparedness and Emerging Infections (DPEI) - Scientific and Program Services Branch is responsible for and maintaining the Emerging Infection Program (EIP) Clostridium difficile Infection (CDI) Incident Case Management System (ICMS) or EIP_CDI_ICMS. System is also called/known as ICMS. ICMS is a web based application that supports the surveillance activities of EIP CDI program, tracking cases and associated data of patients (mainly unidentified) with CDI infections including the integration of epidemiological and laboratory information.
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.)	Data collection is performed by trained surveillance epidemiologists at each participating external EIP sites (State/ Local/Tribal activities) and manually imported into the system. External user access is through CDC's Secure Access Management Services (SAMS) and information is restricted to their data. EIP_CDI_ICMS collects and maintains patient demographic (system assigned patient id, date of birth, gender, ethnicity, race, and state) and clinical information (laboratory test results for the infection). The collected demographic information is used to determine case eligibility, conduct sampling and analyze risk factors among different patient groups. This information is used by the CDC CDI program to analyze and develop preventative measure for reducing the spread of the infections. User names and email addresses are collected for the external EIP users. External user access is through CDC's SAMS and information is restricted to their data. No user credentials are stored in the system. Internal users access is via Application Hosting Branch's Active Directory/Personal Identity Verification (Smart Card) system. Active Directory and SAMS are separate systems with separate PIAs.

Save

13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	Surveillance officers from participating external EIP sites (State/ Local/Tribal activities) manually import incident cases, completed Case Report Forms (CRF) and health interviews, as well as access incident case information from the ICMS web application. EIP_CDI_ICMS collects and maintains patient demographic (system assigned patient id, date of birth, gender, ethnicity, race, and state) and clinical information (laboratory test results for the infection). The collected demographic information is used to determine case eligibility, conduct sampling and analyze risk factors among different patient groups. This information is used by the CDC CDI program to analyze and develop preventative measure for reducing the spread of the infections. User names and email addresses are collected for the external EIP users. CDC lab staff upload reference test results into the ICMS web application. The main ICMS functions are: 1) import incident case information from external EIP sites, 2) provide incident case information to external EIP sites, 3) perform incident case classification, 4) allow CDC labs to enter and view test results, 5) provide interfaces to generate datasets for CDC epidemiology group, CDC lab, and EIP sites, 6) and facilitate specimen tracking. ICMS also provides a function to search for an incident case by; State identifier (ID), Patient ID (system assigned), Incident Specimen Collection Date range or Case Last Updated Date range, Case Classification Status, and Case Processing Status. The search function using State identifier and Patient ID are for the states only. Patient ID and State ID are de-identified information coming from states, and CDC has no insight. External user access is through CDC's SAMS and information is restricted to their data. No user credentials are stored in the system. Internal users access is via Application Hosting Branch's Active Directory/Personal Identity Verification (Smart Card) system. Active Directory and SAMS are separate systems with separate PIAs.
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 Gender Ethnicity PatientID, State ID Race State User name
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
17	How many individuals' PII is in the system?	10,000-49,999
18	For what primary purpose is the PII used?	Determine the population-based incidence of community- and healthcare-associated CDI among participating external EIP sites (State/Local/Tribal activities); Characterize C. difficile strains that are responsible for CDI in the population under surveillance with a focus on strains from community-associated cases; describe the epidemiology of community- and healthcare-associated CDI and generate hypotheses for future research activities using the EIP CDI surveillance infrastructure. User IDs and email addresses of eternal users are used to contact those users.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	None
20	Describe the function of the SSN.	N/A
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); 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)).
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.	N/A
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 ☐ Other Federal Agency/Agencies ☒ State or Local Agency/Agencies Surveillance officers from external EIP sites (State/Local/ Tribal) provide Clostridium difficile Infection (CDI) case file information to EIP_CDI_ICMS. CDC does not share specific external data with other EIP sites. EIP sites are restricted to their data and CDC generated reports. ☐ 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)).	None
24c	Describe the procedures for accounting for disclosures	In the event of disclosure, CDC staff will follow the CDC Notification Process for breach of PII and report incidents with a potential breach of PII within one hour of discovery in accordance with CDC's Privacy Officer guidance. EIP_CDI_ICMS PII data collection is from external EIP sites (State/Local/Tribal) and limited to date of birth, gender, race, and state.
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.	Since the data is collected by and received from EIP sites, CDC relies upon the responsible State or Local Agency to put processes in place to notify individuals that their personal information will be 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.	The project is a public health surveillance activity, and the collected demographic information is used to determine case eligibility, conduct sampling and analyze risk factors among different patient groups. Since the data is collected by and received from participating external EIP sites (State/Local/ Tribal activities), CDC relies upon the responsible State or Local Agency to implement 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.	Since the data is collected by and received from EIP sites(states), CDC relies upon the responsible State or Local Agency to put processes in place to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system. Most states obtain consent for collection of information through making CDI a state reportable condition via law. CDC does not access to patients directly.
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.	Patients may notify CDC or state/local health department if their PII is incorrect or inappropriately used. However, since the data is collected by and received from participating external EIP sites (State/Local/Tribal activities), CDC relies upon the responsible State or Local Agency to put processes 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. The limited PII that the CDC has would make it difficult for a patient or CDC to know if the information actually pertained to an individual with a concern. The data is used to aggregate and analyze to determine if the condition is spreading or controlled.

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.	CDI Program in conjunction with the participating external EIP sites (State/Local/Tribal activities) do self-assessments of the data, both monthly and annually. The review of the data occurs when closing each month's surveillance data and then again annually. Each case is reviewed by the state that entered it to ensure accuracy. The states are responsible for the accuracy, since they have all information and only provide CDC with minimal PII.	
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	Local EIP sites, which have access to their data only, lab users, epidemiology group for study.
		☒ Administrators	Manage the database and trouble shoot the application .
		☐ Developers	
		☐ Contractors	
		☐ Others	
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Program officials review and approve all requests for system access. Authorized accounts are assigned access according to role-based user types designed to limit PII access according to	
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 ICMS program officials will grant least privilege, Role Based Access methods to limit the access to PII for the minimum amount of information and functions 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 by the Business Steward.	
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 access to PII/sensitive information 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 ○ No	

Save

37	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.	The records are maintained in accordance with General Records Schedule (GRS) and comply with CDC Records Control Schedule (RCS). Final reports are created to document programmatic decisions, policies, and other related issues and are maintained permanently (CDC RCS, B-321, 4-1d). Input Data-Data entered by user via web form: Dispose when no longer needed - GRS 20.2d. Input Data-Electronic feed(s) from other electronic systems: Dispose when no longer needed - GRS 20.2c. Output Data-Routine Reporting Material: Five Year GRS 20.6. System Data Precedent setting, received remarkable interest from the public health community and garner extreme interest by the public, media, and health researchers; these records have long-term evidentiary and informational value. Personal identifiers may be deleted from records when no longer needed in the study as determined by the system manager, and as provided in the signed consent form, as appropriate. 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. Records are retained for 20 years; for longer periods if further study is needed.
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. Technical controls: Users are authenticated and data secured using operating system and server security, administered by the local system administrator. PII data is encrypted at rest and in transit with access restricted to specific authorized users as required by HHS and CDC policy. Physical: The server is housed on CDC property with security 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.
General Comments		
OPDIV Senior Official for Privacy Signature	Jarell Oshodi -S Digitally signed by Jarell Oshodi -S Date: 2019.09.24 11:54:10 -04'00'	