Privacy Impact Assessment (PIA): CDC - OCIO Azure GSS - EIP C.diff Infection Incident Case Management System-Cloud - QTR1 - 2025 - CDC8644968
Created Date: 3/17/2025 7:20 AM Last Updated: 4/8/2025 1:42 PM

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?:	No

Consolidated Parent Component

Component Name
No Records Found

General Information

PIA Name:	CDC - OCIO Azure GSS - EIP C.diff Infection Incident Case Management System-Cloud - QTR1 - 2025 - CDC8644968	**PIA ID:**	8644968
Name of Component:	OCIO Azure GSS	**Name of ATO Boundary:**	OCIO Azure GSS

Migrated Sub-Component PIA

PIA Name
No Records Found

Sub-Component

Software Name
EIP C.diff Infection Incident Case Management System-Cloud

Original Related PIA ID

PIA Name
No Records Found

Overall Status:		**PIA Queue:**	
Submitter:	BROWN, Lashell SIZEMORE, Curtis	**# Days Open:**	21
Submission Status:	Submitted	**Submit Date:**	3/17/2025
Next Assessment Date:	04/06/2028	**Expiration Date:**	4/6/2028
Office:	OD	**OpDiv:**	CDC
Security Categorization:	High		
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)?	Yes
4:	ATO Date or Planned ATO Date	

Privacy Threshold Analysis (PTA)

PTA Name
CDC - OCIO Azure GSS - EIP C.diff Infection Incident Case Management System-Cloud - QTR1 - 2025 - CDC8644872

History Log: View History Log

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	New
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	
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 Emerging Infection Program (EIP) Clostridium difficile Infection (CDI) Incident Case Management System (ICMS) is a web-based application that supports the operational activities of EIP CDI project incident case's data and information management including the integration of epidemiologic and laboratory information from CDI incident cases.
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.	Surveillance officers from external EIP sites (State/Local/Tribal) manually import incident cases, complete Case Report Forms (CRF) and health interviews, as well as access incident case information from the ICMS web application through CDC's Secure Access Management Services (SAMS). CDC lab staffs upload reference test results into the ICMS web application. There are no automated system processes that facilitate data transfer between other systems and EIP CDI ICMS. Incident case information file imported into ICMS is generated at the EIP sites. The ICMS System has an import function that involves importing of records that are contained in an excel file from the EIP sites onto the systems database. This step is invoked by the user and is not a system process. System checks for formatting and validity of the data by ICMS before data is imported. System also collects and maintains patient demographic (system assigned patient id, date of birth, sex, 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.
PTA - 5A:	Are user credentials used to access the system?	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 - Internal and Privileged Internal Users are identified and authenticated via Active Directory. Active Directory is a separate system with its own PIA. External Users are identified and authenticated via Secure Access Management System (SAMS). SAMS is a separate system with its own PIA.
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.	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 external EIP sites, 6) and facilitate specimen tracking. ICMS also provides a function to search for an incident case by State ID, Patient ID, Incident Specimen Collection Date range or Case Last Updated Date range, Case Classification Status, and Case Processing Status. System also collects and maintains patient demographic (system assigned patient id, date of birth, sex, 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. The data collected in the ICMS database will be imported into Power BI to perform visual analysis of data by CDC program staff.
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)?	Yes
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 Emerging Infection Program (EIP) Clostridium difficile Infection (CDI) Incident Case Management System (ICMS) is a web-based application that supports the operational activities of EIP CDI project incident case's data and information management including the

		integration of epidemiologic and laboratory information from CDI incident cases. Non-organizational user access is limited to only cases belonging to their site. They have full access to their cases, but no access to any other information not associated with their site. Low impact: non-organizational user access is limited to only cases belonging to their site. They have full access to their cases, but no access to any other information not associated with their site, mitigating the risk of unauthorized disclosure.
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.	Other - Free text Field - County, Race, Sex, State, Ethnicity
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Patients 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?	PII is used to geographically and demographically locate the incident of disease and categorize it by impacted demographic groups.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	This information will be used for research purposes to better inform the public on how to prevent and/or treat these diseases.
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.	Government Sources State/Local/Tribal
PIA - 10:	Is there an Office of Management and Budget (OMB) information collection approval number?	Yes
PIA - 10A:	Provide the information collection approval number.	0920-0978
PIA - 10B:	Identify the OMB information collection approval number expiration date.	4/30/2025
PIA - 10C:	Explain why an OMB information collection approval number is not required.	N/A
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.	State or Local Agency/Agencies
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	Determine the population-based incidence of community- and healthcare-associated CDI among participating EIP sites; 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 EIP CDI surveillance infrastructure.
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)).	N/A. No agreement other than CDC rules of behavior. State partners provide the data to the CDC, and the CDC shares it back to the participating states in the form of reports the state partners use for data analysis.
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.	Prior notice is not given to the individuals because the data is provided by the State and Local Health Departments, and any prior notice would be given by these entities. CDC collects this data whenever a case antibiotic resistant bacteria is reported by a partner health agency, as required.
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.	There is no option to object to the collection of the information. Local health regulations require these types of confirmed laboratory test results to be reported. The information collected by this system comes from State

		and Local Public Health departments whenever a case antibiotic resistant bacteria is reported by a partner health agency.
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.	If there were major changes to the system, it would not be possible to notify and obtain consent from the individuals whose PII is in the system, because the system does not collect any identifiable information that would allow CDC to contact them.
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.	There is not a redress process in place because of the nature of the data that the system maintains; there is no direct identifier or contact information collected. The individual can, however, contact the health facility where the PII was collected, and any redress rights would be exercised at the state and local levels where the information is collected.
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.	CDI Program in conjunction with the participating external EIP sites (State/Local/Tribal activities) do an 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.
PIA - 17:	Identify who will have access to the PII in the system.	Administrators Developers 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.	Administrators have access to PII for maintenance and support. Developer's Direct contractors have access to PII for maintenance and support of the system like system upgrades and bug fixes. Direct contractors working as developers or system administrators have access to PII for maintenance and support of the system like system upgrades and bug fixes.

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The Business Steward determines which system users access PII according to their need to administer or correct errors in the system and role based controls are established for these individuals. Since access to PII is only needed for administration and maintenance, only system administrators and developers are given roles to access to PII if CDI change management identifies a potential problem with the data received.
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.	Least privilege methods are employed to ensure that those with access to PII can only access the minimum amount necessary to perform their job. Ways of creating least privilege include limiting specific users to only being able to read data, read and enter data, or give administrators full access to the database.
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 personnel annually receive security and privacy awareness training on an annual basis.
PIA - 22:	Describe training system users receive (above and beyond general security and privacy awareness training).	System users also receive annual role-based training.
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).	Records are retained and disposed of in accordance with the CDC Scientific and Research Project Retention Schedule N1-442-09-001. 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.
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 controls include A data use agreement put in place between CDI and Emerging Infections Program Web Service Web Service to ensure correct use of information received. Additionally, both systems will be hosted within the CDC Application Hosting Branch and under the Standard operating procedures and security imposed by the CDC. Technical controls include the implementation of encryption. Database security is used to allow the CDI application access to the repository to consume the information received by the web service.

Physical controls included security guards at gate to access facility, card key access and physical locks to data rooms.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	3/17/2025
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	JWO Signature.docx
SOP Comments:	Resigned due to Executive Order 14168	**SOP Review Date:**	3/17/2025
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	3/18/2025
Agency Privacy Analyst Review Comments:	Reviewer: Shanai Shobowale	**Agency Privacy Analyst Days Open:**	1

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	
SAOP Comments:		**SAOP Review Date:**	4/7/2025
		SAOP Days Open:	20

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
No Records Found				