Privacy Impact Assessment (PIA): CDC - ECP - QTR1 - 2025 - CDC8644966

Created Date: 4/8/2025 4:01 PM Last Updated: 4/8/2025 4:01 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

General Information

PIA Name:	CDC - ECP - QTR1 - 2025 - CDC8644966	**PIA ID:**	2984686
Name of Component:	CDC - Edge Computing Platform	**Name of ATO Boundary:**	Edge Computing Platform
Overall Status:		**PIA Queue:**	
Submitter:	Data Feed Service, piafrmcdc	**# Days Open:**	21
Submission Status:	Submitted	**Submit Date:**	3/17/2025
Next Assessment Date:	04/06/2028	**Expiration Date:**	4/6/2028
Office:		**OPDIV:**	CDC
Security Categorization:		**OpDiv PIA ID:**	CDC8644966
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.	3/31/2025
5:	Is the system or electronic information collection, agency or contractor operated?	

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.
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?
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.
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.
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.
PTA - 7:	Does the system collect, maintain, use or share PII?
PTA - 7A:	Does this include Sensitive PII as defined by HHS?
PTA - 8:	Does the system include a website or online application?
PTA - 8A:	Are any of the URLs listed accessible by the general public (to include publicly accessible log in and internet websites/online applications)?

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.
PTA - 10:	Does the website have a posted privacy notice?
PTA - 11:	Does the website contain links to non-federal government websites external to HHS?
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?
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?
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?
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 websites 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?
PTA - 21:	Does this system use artificial intelligence (AI) tools or technologies?

PIA

PIA

PIA - 1:	Indicate the type(s) of personally identifiable information (PII) that the system will collect, maintain, or share.	Social Security Number Name Email Address Phone numbers Medical records (PHI) Military Status Date of Birth Biometric Identifiers Medical Records Number Legal Documents Passport Number Driver License Number Other - Free text Field - "medical information", "ethnicity", and "sex"
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Patients
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?	Date of Birth (DOB) is collected to understand relationship between age and safety. -Medical information (medical notes, medical records number, biometric identifiers) is collected to understand the safety and health risks of certain tasks and/or environments. -The user's medical record number, legal documentation, medical history, medical test results, medical and psychiatric treatment codes, name, military status, demographics, and medical notes are obtained to assist with tracking the applicants' status, research studies, and to make eligibility determinations. This information helps the World Trade Center Health Program (WTCHP) decide whether the enrollee is qualified to become a member of the WTCHP. -Enrollee data is also used to track and modify health care, administration, financial account information, and medical treatments. -Social Security Number (SSN), Date of Birth (DOB), passport number, and driver's license are collected to verify the enrollee's identity and can be used to provide cross reference with the National Institute of Occupational Safety and Health (NIOSH) World Trade Center Health Program (WTCHP). -Demographic information like an individual's ethnicity and/or sex is collected to understand the role of ethnicity and sex in worker safety. -- -Contact information is to ensure that program participants can be contacted. -Employment status is to understand how a worker's role and industry employment relates to safety. -Other non-personal identifiable information (PII) related data include the types of injuries/fatalities involved in incidents for safety incident type classifications, general time and physical location information related to incident to understand environmental context. Also, desensitized narratives, from surveys, that may help clarify what the root causes and contributing factors were for the incident. Injury context is collected in order to organize each safety incident into quantifiable data that can be analyzed. Edge Computing Platform (ECP) collects external users' business contact information (email and phone number) for account set up and user support.

PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	The PII will only be used for the purposes outlined in the primary purpose section of PIA-4, with no secondary uses.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	Individuals Social Security Numbers (SSNs) are collected to verify the enrollee's identity and can also be used to provide cross reference with the National Institute of Occupational Safety and Health (NIOSH) World Trade Center Health Program (WTCHP).
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	Executive Order 9397
PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	5 USC 301 and Pub. L. 78–410
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.	Social Security Number Name Date of Birth Email Address Phone Number Address Passport 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.	**SORN 09-20-0117 Medical and Test Record Results of Individuals Involved in NIOSH Laboratory Studies** Federal Register :: Privacy Act of 1974; System of Records
PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Online
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.	An OMB Information Collection Approval number is not required because this system is not collecting information from the public. In PIA 2, patients is selected, and members of the public is not.

PIA - 11:	Is the PII shared with other organizations outside the system's Operating Division?	No
PIA - 11A:	Identify with whom the PII is shared or disclosed.	
PIA - 11B:	Please provide the purpose(s) for the disclosures described in PIA - 11A.	
PIA - 11C:	List any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	
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.	
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 notifying individuals that their information will be collected and how they can opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.	Portal users provide their information as a condition for creating an account. If a user chooses not to provide their information, an account will not be created and they will be unable to use the system. When logging in to the system, users also acknowledge the warning banner thus accepting the fact that PII will be collected. If a user chooses not to provide their information, they are unable to continue.
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.	The edge computing platform displays a banner notifying users that personally identifiable information (PII) is being collected upon login and participation. Users consent to this by proceeding. Similarly, the CDC also uses comparable banners.
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.	Privacy concerns can be sent to privacy@cdc.gov and potential misuse can be reported at csirt@cdc.gov.
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.	Administrators run data integrity audits on a monthly basis, and all applicable Auditing and accountability controls are in place.
PIA - 17:	Identify who will have access to the PII in the system.	Administrators
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?	
PIA - 18:	Provide the reason why each of the groups identified in PIA - 17 needs access to PII.	Administrators require access to PII to effectively perform their job functions within their specific roles. Role-Based Authentication (RBA) is enforced, ensuring proper separation of duties. Admins are responsible for maintaining the system and need this access to address issues and implement updates. Without this access, system maintenance and improvements would not be possible.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Role-based authentication and separation of duties are implemented to restrict access to PII, ensuring that only authorized individuals can view or manage sensitive information.

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.	The principle of least privilege and separation of duties is enforced through Role-Based Access Control (RBAC) via the CDC Active Directory. Only users with a legitimate need for access to PII are granted permission to view this data, while those without such a need are restricted from accessing it.
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.	Security Awareness Training (SAT) is mandatory for all administrators and general users and is required to be completed on an annual recurring basis. CDC Security Awareness Training
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	Users with elevated privileges are also required to complete the CDC Role Based Training (RBT), CDC Information Security for IT Administrators. RBT is an additional training above what is required for a general user and must be completed on an annual recurring basis by all system administrators. CDC Information Security for IT Administrators
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).	The Edge Computing Platform (ECP) follows the CDC record retention policy. GRS 3.1: General Technology Management Records. 010, Information technology development project records. Disposition instruction: temporary. Destroy 5 years after project is terminated. Disposition authority: DAA-GRS2013-00050006.
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: Edge computing platform follows the personal identifiable information processing and transparency policy. This is inherited from OCIO Program. The CDC Privacy Unit determines and documents the authority in accordance with the CDC IT Security Program Implementation Standards, APPENDIX K: CDC IT Security Organizationally-Defined Minimum Numbers and Time Periods that permits, in accordance with the CDC IT Security Program Implementation Standards, APPENDIX K: CDC IT Security Organizationally-Defined Minimum Numbers and Time Periods the processing of personally identifiable information; and NIST Requirement b. The CDC Privacy Unit restricts in accordance with the CDC IT Security Program Implementation Standards, APPENDIX K: CDC IT Security Organizationally-Defined Minimum Numbers and Time Periods the processing of personally identifiable information to only that which is authorized. The Senior Official for Privacy must approve each CDC privacy impact assessment. The approved privacy impact assessment defines

the personally identifiable information that is authorized for collection and processing.

Technical:

The CDC Privacy Unit implements tools or mechanisms as defined in the CDC IT Security Program Implementation Standards, APPENDIX K: CDC IT Security Organizationally-Defined Minimum Numbers and Time Periods for individuals to consent to the processing of their personally identifiable information prior to its collection that facilitate individuals' informed decision-making. Consent is verified via the submission and the approval of the system privacy impact assessment.

On the privacy impact assessment, the system owner must identify the method for how individuals can opt-out from providing their personally identifiable information.

At an organizational level, visitors to the CDC's digital media channels may review the CDC Privacy Policy at https://www.

cdc.gov/privacy to understand how CDC manages consent.

CDC does not collect any personally identifiable information (PII) when visitors visit any of CDC’s digital medial channels unless they choose to provide that information to CDC.

The CDC Privacy Unit, in collaboration with the Office of Communication, provides notice via the CDC Privacy Policy for CDC's Digital Channels at www.
cdc.

gov/privacy to individuals about the processing of personally identifiable information that: NIST Requirement a.

Is available to individuals upon first interacting with CDC at www.cdc.gov, within CDC mobile apps, and directly from individuals at the time of collecting their personally identifiable information within a written Privacy Act statement; and subsequently at a frequency defnined in the CDC IT Security Program Implementation Standards, APPENDIX K: CDC IT Security Organizationally-Defined Minimum Numbers and Time Periods NIST Requirement b.

Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language.

The CDC Privacy Unit, in collaboration with the CDC center/institute/office, ensures that language on the Privacy Notice is reviewed and cleared in

accordance with plain language principles.

NIST Requirement c.

Identifies the authority that authorizes the processing of personally identifiable information.

During the Privacy Notice review and approval process, the CDC Privacy Unit validates and approves the authority for processing personally identifiable information.

NIST Requirement d.

Identifies the purposes for which personally identifiable information is to be processed.

During the Privacy Notice review and approval process, the CDC Privacy Unit validates and approves the purposes for which personally identifiable information is to be processed.

NIST Requirement e.

Identifies information defined in the CDC IT Security Program Implementation Standards Appendix K: CDC IT Security Organizationally-Defined Minimum Numbers and Time Periods.

Physical:

The CDC Enterprise: CDC C/I/Os' are responsible for developing a list of authorized personnel who are required to access areas (other than general access). The programs are responsible for maintaining the list of authorized personnel and updating OSSAM of any changes in access. OSSAM is responsible for issuing credentials, and updating credentials with appropriate access for approved individuals. OSSAM also maintains the list of approving officials for all restricted card readers (for access to other than general areas). This is different from the general access that is requested on cardkey request forms. The OSSAM Cardkey section then verifies with the program approving official that the individual in question is indeed approved for access to the area. NIST Requirement b. The CDC Enterprise: Credentials are issued in accordance with the CDC policy Issuance and Utilization of PIV Credentials, and Homeland Security Presidential Directive 12. Primary security badge and cardkey issuance, updates, and deletions are performed through the OSSAM Physical Security Branch (PSB). As a part of the standard in-processing for CDC, the sponsoring official submits both an identification (ID) badge and cardkey request to the PSB, ID Badge/Cardkey operations. This control provides added protection to CDC sensitive and critical IT infrastructure, such as computer rooms, where access is not granted until authorization is granted by the authorizing official for the area (DSO, OCIO, or a program official with designated responsibility for the area).

NIST Requirement c. The CDC Enterprise: Once an employee/user has been granted access authorization, the employee with approved access is listed on an access roster that is maintained within the cardkey database. An access roster can be generated on demand by a program manager for review and concurrence of current employee status. OSSAM Program managers review rosters at varying frequencies depending on the sensitivity of the asset. Rosters are also updated and reviewed by program managers every 365 days which is within the organizational defined frequency defined in Appendix K: CDC IT Security Organizationally-Defined Minimum Numbers and Time Periods. However, any changes that occur (termination, loss of access) are reported to OSSAM and access will be updated immediately. Personnel no longer requiring access to CDC facilities are removed from access rosters through an administrative function that uses Navigator, SmartCard Management System(SCMS) and PACS interface (PSOB is notified for emergency situations) notification via PSOB to ID Badge/Cardkey operations. OSSAM Program managers make these changes immediately. Personnel onboarding/outboarding through HR are auto-populated through Smart Card Managment System and Physical Access control System integration. In the event of emergency PIV deactivation requirment, PSOB personnel deactivate PIV manually through HHS Identity.

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:**	
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				

Admin Section

Is OpDiv Privacy Analyst Approved ?:	1	**Is OpDiv Privacy Analyst Return ? :**	0
		Is SOP Return ?:	0
Is Agency Privacy Analyst Approve ?:	1	**Is Agency Privacy Analyst Return ?:**	0
Is SAOP Approved?:	1	**Is SAOP Return ?:**	0
Total Approved:	4	**Total Return:**	0
Total Approval Required:	4		

Miscellaneous Fields

Last Updated:	4/8/2025 4:01 PM	**History Log:**	View History Log