Privacy Impact Assessment (PIA): CDC - CDCReady - QTR2 - 2025 - CDC8713773

Created Date: 5/29/2025 8:01 PM Last Updated: 6/27/2025 8:00 AM

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 - CDCReady - QTR2 - 2025 - CDC8713773	**PIA ID:**	3244505
Name of Component:	CDC - CDCReady	**Name of ATO Boundary:**	CDCReady
Overall Status:		**PIA Queue:**	
Submitter:		**# Days Open:**	49
Submission Status:	Re-Submitted	**Submit Date:**	6/25/2025
Next Assessment Date:	N/A	**Expiration Date:**	1/1/2100
Office:		**OPDIV:**	CDC
Security Categorization:	Moderate	**OpDiv PIA ID:**	CDC8713773
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.	
5:	Is the system or electronic information collection, agency or contractor operated?	Agency

PTA

PTA

PTA - 2:	Indicate the following reason(s) for this PTA. Choose from the following options.	PIA Validation (PIA Refresh)
PTA - 2A:	Describe in further detail any changes to the system that have occurred since the last PIA.	N/A
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 purpose of the CDCReady system hosted in the Office of the Chief Information Officer (OCIO) Azure General Support System (GSS) cloud environment is to create and develop a unified technical structure capable of seamlessly and securely coordinating swift, efficient, and effective emergency responses. The Division of Emergency Operations (DEO) within the Office of Readiness and Response (ORR) has a need to modernize and consolidate its portfolio of systems into a single, cloud-based solution. The foundation for this cloud-based system is CDCReady.

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.	CDCReady will process Name, Age, Sex, Work Email Address, Date of Birth, Work Phone Number, Certificates, Military Status, Photographic Identifiers, Mailing Address, Device Identifiers, Employment Status, Passport Number, and Citizen Status. CDCReady will display a dashboard of system information needed to operate and manage incidents in an emergency. The displayed dashboard will be used to alert teams and individuals on issues or events around the world that will be easily identifiable using searchable criteria for building deployment and preparedness for emergency staff.
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.	CDCReady will share, analyze, and process information needed to operate and manage incidents in an emergency. CDCReady will process Name, Age, Sex, Work Email Address, Work Phone Number, Certificates, Military Status, Photographic Identifiers, Mailing Address, Device Identifiers, Employment Status, Passport Number, and Citizen Status. CDCReady collects names, email addresses, dates of birth, military status, and employment status from national, state, international, and private health care-related agencies to share, analyze, and process information in the form of calendars, charts, maps, documents, and related links by subject matter experts responding to Emergency Operations Center (EOC)-managed incidents. Individuals/Teams that respond to health-related events will receive search criteria for use within CDCReady. CDCReady search criteria will be based on national, state, city, and/or providences for one/multiple countries, states, within varying date ranges. CDCReady event responders will use this data (i.e., Maps for threat locations, health information alerts, and daily reporting purposes) for specific event-related issues. All events durations are predetermined by Health and Human Services (HHS) and in accordance with the leadership of HHS and the CDC.
PTA - 7:	Does the system collect, maintain, use or share PII?	Yes
PTA - 7A:	Does this include Sensitive PII as defined by HHS?	Yes
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)?	No

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 purpose of the CDCReady site hosted in the Office of the Chief Information Officer (OCIO) Azure General Support System (GSS) cloud environment is to create and develop a unified technical structure capable of seamlessly and securely coordinating swift, efficient, and effective emergency responses. The cloud-based CDCReady platform provides analytics and visualization capability to coordinate various business functions performed by DEO for response and incident management into a single web-based platform. CDC Active Directory and SAMS are the only approved methods of authentication. CDCReady is only accessible internally via https://cdcreadydev.cdc.gov/
PTA - 10:	Does the website have a posted privacy notice?	No
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 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?	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.	Name Email Address Phone numbers Certificates Military Status Date of Birth Photographic Identifiers Mailing Address Devices Identifiers Employment Status Passport Number Other - Free text Field - Citizen Status, Age, Sex, Work Email, Address, Work Phone Number
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors
PIA - 3:	Indicate the approximate number of individuals whose PII is maintained in the system.	201 - 500
PIA - 4:	For what primary purpose is the PII used?	The primary purpose for using the PII is to analyze and manage emergency data. Employees working within the CDC Director's Emergency Operations Center (EOC) will receive communication via email, phone call, or in person. This enables the creation of charts, maps, and reports during emergency incidents or events.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	The secondary use of PII will be to send alerts to users, teams, and leadership while building deployment and preparedness.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	Not Applicable
PIA - 6A:	Cite the legal authority to use the SSN, Truncated SSN, and/or Taxpayer ID.	Not Applicable

PIA - 7:	Identify legal authorities governing information use and disclosure specific to the system and program.	Sections 311, 361-368 of the Public Health Service Act; also, 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347. This system maintains records on the conduct of activities (e.g., quarantine, isolation) that fulfill HHS's and CDC's statutory authority under sections 311, 361-368 of the Public Health Service Act to prevent the introduction, transmission and spread of communicable diseases. Records in this system have various uses by agency personnel offices, including screening qualifications of employees; determining status, eligibility, and employee's rights and benefits under pertinent laws and regulations governing Federal employment; computing length of service; and other information needed to provide personnel services. These records may also be used to locate individuals for personnel research.
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.	CDCReady will share, analyze, and process information needed to operate and manage incidents in an emergency. CDCReady will process Name, Age, Gender, Work Email Address, Work Phone Number, Certificates, Military Status, Photographic Identifiers, Mailing Address, Device Identifiers, Employment Status, Passport Number, and Citizen Status. CDCReady collects names, email addresses, dates of birth, military status, and employment status from national, state, international, and private health care-related agencies to share, analyze, and process information in the form of calendars, charts, maps, documents, and related links by subject matter experts responding to Emergency Operations Center (EOC)-managed incidents. Individuals/Teams that respond to health-related events will receive search criteria for use within CDCReady. CDCReady search criteria will be based on national, state, city, and/or providences for one/multiple countries, states, within varying date ranges. CDCReady event responders will use this data (i.e., Maps for threat locations, health information alerts, and daily reporting purposes) for specific event-related issues. All events durations are predetermined by Health and Human Services (HHS) and in accordance with the leadership of HHS and the CDC. Users are authenticated to the system via Active Directory (AD). AD is a separate system covered by its own PIA.
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.	OPM/GOVT 1, General Personnel Records

PIA - 9:	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains Online Government Sources Within the OPDIV
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.	Not Applicable; PII not being collected directly from the public
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.	There is no method for individuals to opt-out of the collection or use of their PII, users give consent during the orientation process on collection and the use of PII. CDCReady users who accept access to the system are notified that they will be sharing PII information with other CDCReady information system users to complete assignments and tasks on behalf of the Emergency Operations Center. If a user decides to opt-out of the collection or use of their PII, their access to CDCReady will be revoked. Logical access to CDCReady is a voluntary decision of users and is not mandatory by the organization.
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.	When major changes occur within the system such as disclosure and/or data uses change from time of original collection, CDCReady system administrators will immediately notify users and obtain new consent from individuals affected. Employees working within the CDC Director's Emergency Operations Center (EOC) will receive communication via email, phone call, or in person on changes to the system, and will be allowed to give new users consent or disclosure to their PII used to support the Emergency Operations Center's mission.

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.	CDCReady users concerned that their PII has been inappropriately obtained, used, disclosed, or it is inaccurate will notify the system administrators of their concerns in writing by selecting the link for 'Support Requests' https://ccdcreadydev.cdc.gov/support/Request Individuals affected will be asked to specify the corrective action being sought and the reasons for requesting a correction providing supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant.
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.	CDCReady audit process reviewing PII within the system is continuously being performed by the Division of Emergency Operations support helpdesk as changes occur including adding or removing user accounts. Accuracy: The security/technical Steward will perform governing reviews annually, check for updates, errors are then reviewed and signed by the Business Steward, Information System Security Officer, and the DEO Deputy Director. Personally Identifiable Information (PII) in the system is sufficiently kept accurate for the purpose of charts, reports, and analysis as needed. Availability: CDCReady administrators with DEO support staff will ensure PII data within the system is captured correctly in a timely manner that allows reliable access to information for the center. Access to the system is managed by AD or CDCReady super administrators as users are added/removed from the system depending on role change, job reassignment, and retirement. The DEO support staff relies on communication via phone or email to be notified an account needs modification. Integrity: All CDCReady users will display integrity to data that Information is properly modified or destroyed, and that no dispute occurs by individuals performing task as PII is not improperly or inadvertently modified or destroyed. Outdated, unnecessary, irrelevant, incoherent, and inaccurate PII is removed from the system by EOC leadership as details are discovered. Changes to the data will be captured within audit logs and can be viewed by CDCReady System Administrators.
PIA - 17:	Identify who will have access to the PII in the system.	Users Administrators 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.	Users - CDCReady users will have the flexibility to create reports for analysis, create rosters and contact personnel in the event of a public health emergency using data contained within the web portal. Data collected and disseminated is to support and use by the Emergency Operations Center managed with access control lists. Administrators - Super Administrators have full access to data and functions within the system. To assign tasks, add/update/remove users, and monitor performance. Contractors - Direct Contractors will have access as Full-Time Equivalents to support the EOC with given tasks.
PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	CDCReady will be a role-based security system to prevent a level of activity without collusion. Role separation will be clearly delineated by action to be performed, and administrative rights will be monitored via audit logs. Access will depend on assignment level, users including direct contractors will only have access to PII associated to assigned tasks controlled by system administrative team.
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.	Access to CDCReady, a cloud-based application or web application will be granted to users when assigned to the team depending on user functions and information which will be essential to perform tasks. CDCReady Administrators will apply the model of least privilege access that is controlled as roles or assignments for users change.
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.	CDCReady administrators, developers, users including direct contractors, and program managers are required to take the CDC Security and Privacy Awareness Training annually.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	CDC Records Management Training, CDC Role-Based Training are some of the types of training offered Online or via conferences annually. Roles and responsibilities are identified within the Incident Management System (IMS) and training will be offered by the CDCReady support team periodically. IMS Training provides EOC users more in-depth knowledge and teach them further skills and competencies for users performing specific tasks more securely. IMS Training provides Emergency Operation Center (EOC) users more in-depth knowledge, skills, and competencies that help users perform specific duties as process changes related to business and operations occur.

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).	CDCReady records will be processed following the guidelines in place regarding Data Retention and Disposal of PII in accordance with the CDC Records Control Schedule (RCS), General Record Schedule (GRS), and the National Archives and Records Administration (NARA). CDCReady 'Retention and Disposal' Section records are covered by General Records Schedule 4.2 and retained for 5 years after termination from National Defense Executive Reserve (NDER) Program. In general, records are retained until there is no further administrative need to retain them, or the individual leaves the jurisdiction of the operating office, and are then either destroyed, or, if appropriate, are combined with the Official Personnel Folder, which is forwarded to the hiring Federal agency or, if the employee is leaving Federal service, to the National Personnel Records Center as per the records retention policy for CDC and CPR. More specifically, records are retained per the following records retention guidelines: Input data: Non-electronic, manually entered data are retained for 5 years. Data entered by users via web forms or electronic feeds from other systems are disposed of when no longer needed. System data: Created for business purposes that may be required for follow up or reference for a moderate period of time are retained in accordance with Records Schedule N1-442-09-1, item 3. Output data: Printouts derived from electronic records created on an ad-hoc basis for reference purposes or to meet day-today business needs are retained for 5 years. All other types of output data are disposed of when no longer needed.

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: Includes a system undergoing or has acquired a successful Security Assessment and Authorization, an Authorization to Operate, a system security plan, contingency plan, and risk assessment that help secured PII. CDCReady undergoes regular scheduled test and storage backups for better operability, provide annual Security and Privacy Awareness and Records Management Training, Role-Based Training, and provide proper use for information following the Rule of Behavior policy in accordance with applicable CDC policies. Technical controls: CDCReady users are authorized by system administrators that have undergone background checks, identify proofing, and require a Smart Card to gain access to the CDC network on user role-based authorization. The controls include authentication, firewalls, encryption, anti-malware on systems protected by CDC perimeter firewall, monitored by intrusion detection systems, anti-virus scans, Nessus scans and AppScan vulnerability scans, and unauthorized users do not have access to the system. Physical Controls: CDCReady will be secured in the system using physical controls. The facility where the infrastructure is hosted has multi-layered protection including security guards, secure doors requiring proxy card entry pads, and CCTV monitor. The controls will include protecting cables, devices, power equipment in case of an emergency power/system shutoff, water/fire damage or other natural hazards.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	6/25/2025
Privacy Analyst Comments:		**Privacy Analyst Days Open:**	

SOP Review

SOP Review Status:	Approved	**SOP Signature:**	
SOP Comments:	Approved on behalf of Beverly Walker.	**SOP Review Date:**	6/25/2025
		SOP Days Open:	0

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	6/27/2025
Agency Privacy Analyst Review Comments:	Reviewer: Nestor Villafuerte 6/27/2025 The PIA is ready for SAOP review and approval.	**Agency Privacy Analyst Days Open:**	2

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	Archer Signature Page.docx
SAOP Comments:	6/27/2025 Approved on behalf of the SAOP.	**SAOP Review Date:**	6/27/2025
		SAOP Days Open:	0

Supporting Document(s)

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
PIA - 1	Data Feed Service, piafrmcdc	5/29/2025	Please include all PII items included within PTA 5. E.g. Age, Sex, Work Email, Address, Work Phone Number are missing.	
PIA - 10C	Data Feed Service, piafrmcdc	6/24/2025	Please explain why it is not applicable.	
PIA - 10C	Data Feed Service, piafrmcdc	6/25/2025	Updated N/A justification	
PIA - 1	VILLAFUERTE, NESTOR	6/26/2025	Does the system have an ATO date?	
PIA - 1	BLAND, CRYSTAL	6/27/2025	See ATO Date below. The ATO Expiration is 8/9/2025. *ATO Date:8/10/2022	

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:	6/27/2025 8:00 AM	**History Log:**	View History Log