Privacy Impact Assessment (PIA): CDC - VAMS - QTR3 - 2024 - CDC8505500

Created Date: 7/11/2025 4:01 PM Last Updated: 7/11/2025 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 - VAMS - QTR3 - 2024 - CDC8505500	**PIA ID:**	3476347
Name of Component:	CDC - Vaccine Administration Management System	**Name of ATO Boundary:**	Vaccine Administration Management System
Overall Status:		**PIA Queue:**	
Submitter:	Data Feed Service, piafrmcdc	**# Days Open:**	296
Submission Status:	Re-Submitted	**Submit Date:**	10/25/2024
Next Assessment Date:	N/A	**Expiration Date:**	7/9/2028
Office:		**OPDIV:**	CDC
Security Categorization:		**OpDiv PIA ID:**	CDC8505500
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.	3/31/2024
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.	Name Email Address Phone numbers Date of Birth Mailing Address Other - Free text Field - Gender, Race, Nurse, Medical Doctor, Medical Records (Non-PHI)
PIA - 2:	Indicate the categories of individuals about whom PII is collected, maintained or shared.	Employees/ HHS Direct Contractors 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 (Name, Date of Birth (DOB)) is used for recipient record identification within the system. The primary purpose is for recipient record search and recipient unique identification.
PIA - 5:	Describe any secondary uses for which the PII will be used (e.g. testing, training or research).	PII is also used for tracking vaccination data, determine patient eligibility and contacting patient if needed.
PIA - 6:	Describe the function of the SSN, Truncated SSN, and/or Taxpayer ID.	The last 4 digits of the social are used as an additional identifier by certain jurisdictions with associated reporting requirements, e.g., Puerto Rico.
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.	Public Health Service Act, section 301, "Research and Investigation," (42 U.S.C. 241); sections 304, 306 and 308(d) which discuss authority to grant assurances of confidentiality for health research and related activities (42 U.S.C. 242 b, k, and m(d)).
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.	Date of Birth, and Name.
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.	09-90-2001, Records Used for Surveillance and Study of Epidemics, Preventable Diseases and Problems
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.	Pursuant to section 319 of the Public Health Service (PHS) Act, 42 U.S.C. 247d, Secretary Alex M. Azar, II determined that, as the result of the confirmed cases of 2019 Novel Coronavirus (2019-nCoV), now known as Coronavirus Disease 2019 (COVID-19), a public health emergency (PHE) has existed nationwide since January 27, 2020. As a result of the PHE, he Secretary also determined pursuant to section 319(f) of the PHS Act that circumstances of the PHE necessitate a waiver from the requirements of the Paperwork Reduction Act, 44 U.S.C. § 3501 et seq., effective as of the date of this notice. The waiver is justified to collect information to support the Department of Health and Human Services' investigation of and response to the COVID-19 pandemic. This waiver applies to information to be collected by the Centers for Disease Control and Prevention from individuals, healthcare providers, states, and other partners in order to a facilitate rapid response to the PHE.
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.	For Public Health Intervention
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)).	Not Applicable
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.	The VAMS team will maintain records of disclosure requests, documenting the requests (inclusive of date, nature, and purpose of disclosure) and maintain documentation at least 5 years after disclosure or the life of the record (whichever is longer). Individual requests for disclosure can be made to the VAMS team through email using the VAMS Help Desk (vamshelp@cdc.gov) and the VAMS Team will provide details of all disclosures excluding civil and criminal law enforcement.
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 to opt-out of the collection of an individual's PII. The system relies on this information to associate vaccine requests and fulfillments by providers. Providing an opt-out would not allow the VAMS platform to accurately track dissemination of vaccines from providers and industry partners. Recipient and organizations can opt-out by not leveraging the platform, coordinating with their employers, or contacting the help desk to ask for their account to be disabled. Consent is not explicitly captured when a recipient is uploaded from a Third-Party clinic account, however it is expected that the third-party users have a consent process in place and VAMS requires they acknowledge "all pre-vaccination activities have been completed" to administer a vaccine. The system relies on this information to associate vaccine requests and fulfillments by providers. Recipient and organizations can opt-out by not leveraging the platform, coordinating with their employers, or contacting the help desk to ask for their account to be disabled.

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.	No major system changes are expected. However, any significant change would cause an updated PIA to be performed and published. Additionally, significant changes regarding records disclosures or types, could also trigger the need for a modification to the controlling SORN(s) noted in this document. Individuals are provided a consent and notification banner at time of system access consisting of the following: This warning banner provides privacy and security notices consistent with applicable federal laws, directives, and other federal guidance for accessing this Government system, which includes all devices/storage media attached to this system. This system is provided for Government-authorized use only. Unauthorized or improper use of this system is prohibited and may result in disciplinary action and/or civil and criminal penalties. At any time, and for any lawful Government purpose, the government may monitor, record, and audit your system usage and/or intercept, search and seize any communication or data transiting or stored on this system. Therefore, you have no reasonable expectation of privacy. Any communication or data transiting or stored on this system may be disclosed or used for any lawful Government purpose.
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.	External recipients or employers are able to escalate privacy related incidents to the CDC VAMS support team or project owner through website-based contacts or the VAMS Help Desk (vamshelp@cdc.gov). Alternatively, CDC employees or recipients may contact the CDC Computer Security Incident Response Team (CSIRT) in the event that there is a potential misuse of PII data, via 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.	PII reviews are conducted through the design review process when implementing individual attributes in each increment. PII attribute read and write permissions are role-based and attributes will be reviewed by the development team, CDC Project Owner, and System Security and Privacy Officer (SSPO) through each increment of development to determine that the appropriate roles have least privilege permission to access sensitive attributes as identified above to protect the integrity of the data contained in VAMS. Data accuracy and relevancy will be maintained through usage of standard configuration of field values inclusive of picklists, date ranges, and a minimization

		of free text where possible. Reports will be run incrementally throughout the program lifecycle (pre-production, post-production, and incrementally through operations & maintenance (O&M) to review data elements for anomalies and review data validation governing fields. Integrity: PII attribute read and write permissions are role-based and are reviewed by the development team, CDC Project Owner, and the Systems Security and Privacy Officer (SSPO) during each increment of development. Reviews ensure that appropriate roles have least privilege permission to access sensitive attributes, protecting the integrity of the data contained in VAMS. Availability: Reports are run incrementally throughout the program lifecycle (pre-production, post-production, and incrementally through operations & maintenance (O&M)). These reports help in reviewing data elements for anomalies and ensuring data validation governing fields. Accuracy: Data accuracy is maintained using standard configuration of field values including the use of picklists, date ranges, and minimization of free text where possible. Relevancy: The design review process includes periodic reviews of PII when implementing individual attributes in each increment, ensuring that data remains relevant and up to date.
PIA - 17:	Identify who will have access to the PII in the system.	Users 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.	Users: Employers can view PII that has been entered on their specific company roster (name/email); Clinics administrators can see PII but not PHI; Health Care providers can see PII to perform their duties. Administrators: VAMS Administrators will have access in order to perform Tier 3 support and evaluate records and cases.

PIA - 19:	Describe the administrative procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	PII visibility in the platform is enforced through role definition and role management. Roles were evaluated and defined in conjunction with the CDC project manager and associated business offices through creation of user stories and incorporated in design.
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 system enforces least privilege that allow users access to only the information they need to carry out a task. Encryption is implemented both at rest and in transits. To mitigate exposure to the PII data, user PII data are encrypted, and users are disassociated from the PHI data elements. PII data are also obscured. Authentication will enforce multi-factor authentication for all users along with account management policies inclusive of account creation, account disablement, and session time outs to limit data access.
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.	Internal CDC personnel are required to take security awareness training related to review, use, and dissemination of sensitive data. Internal personnel are also required to undergo suitability determination in advance of accessing IT resources. External personnel (clinics or employers) will be presented awareness language when entering the VAMS platform and have access to the privacy notice as a direct link off the home page.
PIA - 22:	Describe the training system users receive (above and beyond general security and privacy awareness training).	The VAMS development team is responsible for additional providing instructional usage documentation and training for end users on the VAMS platform. Training is developed to train end users, including the user manual, job aids, design documents, and other artifacts.
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).	General Records Schedule 5.2: Transitory and Intermediary Records. Records required only for a short time (generally less than 180 days) and that are not required to meet legal or fiscal obligations, or to initiate, sustain, evaluate, or provide evidence of decision-making. Destroy when no longer needed for business use, or according to agency predetermined time period or business rule.

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 - administrative controls include review of accounts and access to PII data elements on a recurring basis, inheriting computer security awareness training controls for CDC staff, least privilege through role definition, development of incident response planning, and account management policies inclusive of account creation and termination. PII stored will be limited in the user interface leveraging role-based access. Technical - the technical and physical controls are inherited from the Salesforce Platform and AWS FedRAMP data centers, FedRAMP control set, and inclusive of AWS/Salesforce FedRAMP platform plugins. Salesforce will leverage the Salesforce Shield module to support encryption of PII data within the platform both at the disk and attribute level while AWS will leverage the AWS Key Management Service (KMS). Encryption in transit and at rest will be enforced for all fields collecting PII data elements within the technical constraints of each platform. However, there are known limitations to specific field types (i.e. pick lists, checkboxes). To mitigate exposure to the PII data in these fields, the user data will be encrypted and disassociated from the PHI data elements. Authentication will enforce multi-factor authentication for all users along with account management policies inclusive of account creation, account disablement, and session time outs to limit data access. Physical - data center physical security begins at the Perimeter Layer. This layer includes a few security features depending on the location, such as security guards, fencing, security feeds, intrusion detection technology, and other security measures.

Review & Comments

Privacy Analyst Review

OpDiv Privacy Analyst Review Status:	Approved	**Privacy Analyst Review Date:**	10/29/2024
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:**	10/31/2024
		SOP Days Open:	6

Agency Privacy Analyst Review

Agency Privacy Analyst Review Status:	Approved	**Agency Privacy Analyst Review Date:**	7/10/2025
Agency Privacy Analyst Review Comments:		**Agency Privacy Analyst Days Open:**	252

SAOP Review

SAOP Review Status:	Approved	**SAOP Signature:**	
SAOP Comments:		**SAOP Review Date:**	7/10/2025
		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	9/19/2024	Truncated SSN was not listed in the PTA. Please correct there or here. Additionally, please deselect "Medical Records (PHI)" and, in the free text field, type "Medical Records (Non-PHI)". Additionally, please add demographic information such as gender and race.	
PIA - 16	Data Feed Service, piafrmcdc	9/19/2024	Please remove mention of PHI if this system is not subject to HIPAA. Additionally, please change acronym from ISSO to SSPO.	
PIA - 8A	Data Feed Service, piafrmcdc	10/23/2024	Please confirm which PII is actually used to retrieve records in this system. Only list the direct identifiers used.	

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:	7/11/2025 4:01 PM	**History Log:**	View History Log