US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/24/2020

OPDIV:

CDC

Name:

Vaccine Administration Management System (VAMS)

PIA Unique Identifier:

P-1518627-001990

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Planning

Is this a FISMA-Reportable system?

No

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

No

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

The purpose of the Vaccine Administration Management System (VAMS) is to facilitate the clinical management, distribution and administration of the Coronavirus Disease 2019 (COVID-19) vaccine, and to enable the reporting of the COVID-19 vaccine information to State Immunization Programs, the Centers for Disease Control and Prevention (CDC), electronic health records (EHRs) and consumers. The application is configured to meet the COVID-19 outbreak response needs.

Describe the type of information the system will collect, maintain (store), or share.

Data collected by VAMS includes recipient person and contact information including full name, address, phone, date of birth, and emergency contact name and phone; recipient demographics including gender and race; recipient current and past medical history including previous and current medical conditions, allergies, nursing status (pregnant/nursing/nursing home), vaccination history; insurance provider, group, and plan number; clinic information inclusive of clinic address, clinic point of contact name and phone number, clinic vaccination inventory, inventory information (lot number, dosages, manufacturer, serial numbers, expiration dates); appointment information for Scheduling including time and location of appointment; requesting Organization Name, Category, Address, and associated Point of Contact (Name, Phone, Email) and role holder (business contact information) including business contact name, email, role, and credentials (e.g. Registered Nurse (R.N), Medical Doctor (M.D.), Nurse Practitioner (N.P.), (Physician Assistant (P.A.), Licensed Practical Nurse (L.P. N.), or Other).

Access to the system is accomplished by internal users using PIV card with authentication by Active Directory (AD);or the Secured Access Management System (SAMS). AD and SAMS are separate systems with their own PIAs. External users access via User ID and Password.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

VAMS will not only enable the agency to better manage, distribute, and deliver vaccines during the initial phase of the response, but also give CDC the ability to monitor and rapidly alert in the case of adverse reaction caused by different vaccine preparations. The system has two purposes: (1) To facilitate the clinical management, distribution and administration of the COVID-19 vaccine; and (2) To facilitate the reporting of the COVID-19 vaccine information to state immunization programs, CDC, EHRs and consumers.

Data collected includes recipient person and contact information including full name, address, phone, date of birth, and emergency contact name and phone; recipient demographics including gender and race; recipient current and past medical history including previous and current medical conditions, allergies, nursing status (pregnant/nursing/nursing home), vaccination history; insurance provider, group, and plan number; clinic information inclusive of clinic address, clinic point of contact name and phone number, clinic vaccination inventory, inventory information (lot number, dosages, manufacturer, serial numbers, expiration dates); appointment information for Scheduling including time and location of appointment; requesting Organization Name, Category, Address, and associated Point of Contact (Name, Phone, Email) and role holder (business contact information) including business contact name, email, role, and credentials (e.g. Registered Nurse (R.N), Medical Doctor (M.D.), Nurse Practitioner (N.P.), (Physician Assistant (P.A.), Licensed Practical Nurse (L.P. N.), or Other).

The recipient information is provided by employers and recipients (individuals) and is then used for vaccine scheduling and appointment support purposes.

Access to the system is accomplished by internal users using PIV card with authentication by Active Directory (AD) or the Secured Access Management System (SAMS). AD and SAMS are separate systems with their own PIAs. External users access via User ID and Password with authentication via SAMS.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Date of Birth

Name

E-Mail Address

Mailing Address

Phone Numbers

Medical Notes

Socioeconomic status

Gender

Race

Medical history

Professional Certifications

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees

Public Citizens

Patients

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

PII is used for patient record identification within the system.

Describe the secondary uses for which the PII will be used.

PII is also used for tracking vaccination data for patients.

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)).

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-90-2001, Records Used for Surveillance and Study of Epidemics, Preventable Diseases

09-20-0136, Epidemiologic Studies and Surveillance of Disease Problems

Identify the sources of PII in the system.

Online

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

OMB Clearance not required. The Paperwork Reduction Act requirement waived by the National Childhood Vaccine Injury Act [Public Law 99-660, section 321- Title III].

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

State or Local Agencies

For Public Health Intervention - State agencies require vaccination data associated with given Recipients with

Describe any agreements in place that authorizes the information sharing or disclosure.

N/A

Describe the procedures for accounting for disclosures.

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.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

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.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

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 method to opt-out of the collection of an individual's PII. The system relies on this information in order 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.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

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.

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.

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.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

PII and PHI 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 Information Systems Security Officer (ISSO) 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.

Identify who will have access to the PII in the system and the reason why they require access.

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/PHI to perform their duties.

Administrators:

VAMS Administrators will have access in order to perform Tier 3 support and evaluate records and cases.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Rationale will be evaluated during the software design process to determine which system identified roles require access to PII. Access and data accessibility along with role creation/administration processes will be reviewed with the ISSO in advance of platform administrators creating or assigning roles within the VAMS platform. A minimal set of administrators will be able to see PII attributes and developers and other roles not requiring PII visibility will be limited.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

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.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

CDC personnel are required to take security and privacy awareness training at least annually.

Describe training system users receive (above and beyond general security and privacy awareness training).

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.

The VAMS development team is responsible for additional training for end users on the VAMS platform.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

Records are maintained in accordance with National Archieves and Records Administration (NARA) General Records Schedule (GRS) 20.2a.4 and CDC Scientific and Research Project Records Records Control Schedule (Big Bucket). Records will be retained and deletion privileges are limited to platform administrators only. Records will not be deleted unless explicitly requested through an opt-out process by an individual. Audits of system administrator deletions will be reviewed at least annually to validate compliance with the retention policy.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

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 FedRAMP data center, FedRAMP control set, and inclusive of Salesforce FedRAMP platform plugins. Encryption of data exists within the platform both at the disk and attribute level. 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 number of security features depending on the location, such as security guards, fencing, security feeds, intrusion detection technology, and other security measures.

Note: web address is a hyperlink.

Session Cookies that do not collect PII.