US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/07/2020

OPDIV:

CDC

Name:

NCIRD Immunization Datalake and Data Storefront (IZDL)

PIA Unique Identifier:

P-5819692-165822

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

Describe the purpose of the system.

NCIRD Immunization Datalake and Data Storefront (IZDL) is a cloud hosted data repository which receives, stores and manages Coronavirus 2019 (COVID-19) vaccination data for dose administration, inventory and distribution.

As part of the event data provisioning pipeline, the solution performs data validations, translations, transformations, de-duplications, record linkages, de-identification and application of program specific business algorithms. In addition, the tool generates bulk exports and responds in real time to external data queries from other applications such as the Vaccine Adminstration Management System (VAMS). VAMS is a separate system with its own PIA.

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

Data collected includes name, address, phone, date of birth, and emergency contact name and phone; patient demographics including gender and race; 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.

The system also collects clinic information inclusive of clinic address, clinic point of contact name and phone number, clinic vaccination inventory information (lot number, dosages, manufacturer, serial numbers, expiration dates); appointment information for Scheduling including time and location of appointment; and credentials of clinicians (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).

Users authenticate into this system via Secure Access Management System (SAMS). SAMS is a separate system with its own PIA.

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

IZDL is a cloud hosted data repository to share vaccine data. The components support the exchange of immunization data between immunization information systems (IISs), provider organizations, and consumer applications. IZDL can streamline time and resource intensive data exchange on-boarding. It also replaces multiple one-to-one connections with centralized routing. In addition, services to generate bulk exports and responding in real time to external data queries from applications include Vaccine Administration Management System (VAMS) that is anticipated to be available.

Data collected includes name, address, phone, date of birth, and emergency contact name and phone; patient demographics including gender and race; 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.

The system also collects clinic information inclusive of clinic address, clinic point of contact name and phone number, clinic vaccination inventory information (lot number, dosages, manufacturer, serial numbers, expiration dates); appointment information for Scheduling including time and location of appointment; and credentials of clinicians (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).

Patient name, email address, phone number, medical notes, date of birth, mailing address, emergency contact name, emergency contact phone number, gender, race, and medical history are used for patient record identification. This data is also used to identify and follow-up with patients who have been vaccinated as well as any who may experience adverse reactions stemming from immunizations. Patient PII may also be used for determining efficacy of the impact of the vaccine on other preventable diseases by comparing immunization rates to disease case data.

Clinic information is used to contact facilities who may need or have available vaccine for dispensing.

Users authenticate into this system via Secure Access Management System (SAMS). SAMS is a separate system with its own PIA.

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

Gender

Race

Professional Credentials

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?

Patient name, email address, phone number, medical notes, date of birth, mailing address, emergency contact name, emergency contact phone number, gender, race, medical history are used for patient record identification within the system.

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

Patient social and geographic demographics are used to identify and follow-up with patients who have been vaccinated as well as any who may experience adverse reactions stemming from immunizations. Patient PII may also be used for determining efficacy of the impact of the vaccine on other preventable diseases by comparing immunization rates to disease case data.

Clinic contact information is used to contact facilities who may need or have available vaccine for dispensing.

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)). Public Readiness and Emergency Preparedness Act (42 U.S.C. 247d-6d).

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.

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

"NCIRD determined the information collection activities conducted under this project qualify for the NCVIA-conferred PRA waiver as they come under the activities authorized under NCVIA, Section 2102(a)(7) of the Public Health Service Act (42 U.S.C. 300aa-2(a)(7)), "Evaluating the need for and the effectiveness and adverse effects of vaccines and immunization activities."

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

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

N/A

Describe the procedures for accounting for disclosures.

The IZDL 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). Users can contact IZDLHelpDesk@cdc.gov for additional information.

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

There is no process in place to notify individuals that their personal information is being collected because IZDL is not the system that directly collects the information. The information is received through other information systems, i.e., VAMS. VAMS is a separate system with its own PIA.

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 PII. The data is other systems, such as VAMS. The information is received through other information systems, i.e., VAMS. VAMS is a separate system with its own PIA.

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 which would also be published for public notice.

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.

For external recipients or employers they can contact IZDLHelpDesk@cdc.gov for additional information.

CDC employees may contact the CDC Computer Security Incident Response Team (CSIRT) in the event that there is a potential misuse of PII data, at 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 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 the IZDL.

Data accuracy and relevancy will be maintained through usage of standard configuration of field values inclusive of pick-lists, 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:

To check for relevancy/accuracy and updates.

Administrators:

IZDL 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 IZDL 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).

The IZDL Development Team is responsible for any additional training for end users on the IZDL platform. Users will be presented awareness language when entering the IZDL platform and have access to the privacy notice as a direct link from the home page.

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 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.