US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/13/2020

OPDIV:

CDC

Name:

Immunization Gateway (IZ Gateway)

PIA Unique Identifier:

P-5909992-340208

The subject of this PIA is which of the following?

General Support System (GSS)

Identify the Enterprise Performance Lifecycle Phase of the system.

Implementation

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.

Immunization Gateway (IZ Gateway) supports a centralized technical infrastructure, enabling the exchange of patient level data. IZ Gateway supports a bi-directional data exchange facilitating the connection of state immunization information systems (IIS) with each other, multiple IIS with providers, and multiple IIS with consumer applications.

IZ Gateway also enables the submission to and access of COVID-19 vaccine data by CDC for use in informing public health decisions and interventions.

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

IZ Gateway provides a means by which messages from participating systems (IIS, provider/pharmacy and consumer applications) regarding immunization events can be routed within the technical ecosystem; i.e., system to system messages that support unsolicited updates to IIS (e.g., when an immunization event has occurred), and responses to queries (e.g., when a provider needs to determine an appropriate next dose). These messages include patient name, email, date of birth, gender, phone number, and mother's maiden name) and immunization event data (event date & immunization details).

User ID and password are not utilized for access to or stored by the system.

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

IZ Gateway is a critical component in the infrastructure CDC is establishing to ensure CDC obtains real-time or near real-time data on vaccine use and distribution when a COVID-19 vaccine becomes available. Z Gateway supports the exchange of immunization data between immunization information systems (IIS), provider organizations and consumer applications. Additionally, the IZ Gateway provides a mechanism by which IIS data can be shared among IIS, as well as IIS and providers, or IIS and consumers for routine immunization purposes.

IZ Gateway provides a means by which messages from participating systems (IIS, provider/pharmacy and consumer applications) regarding immunization events can be routed within the technical ecosystem; i.e., system to system messages that support unsolicited updates to IIS (e. g., when an immunization event has occurred), and responses to queries (e.g., when a provider needs to determine an appropriate next dose). These messages include patient name, email, date of birth, gender, phone number, and mother's maiden name) and immunization event data (event date & immunization details).

Data from the IZ Gateway are transmitted to participating systems and subsequently used for public health program management, to make informed clinical decisions and to provide information required to complete an individual’s vaccination history.

User ID and password are not utilized for access to or stored by the system.

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

Mother's Maiden Name

E-Mail Address

Phone Numbers

event date and immunization details gender

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

Patients

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

When a healthcare provider requests that data be returned from more than one jurisdiction, the data is used to perform a cross-jurisdictional data query to ensure accuracy in identifying the patient.

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

PII is used to make informed clinical decisions and to provide information required to complete an individual’s vaccination history.

Identify legal authorities governing information use and disclosure specific to the system and program.

Public Health Service Act, sec. 301, Research and Investigation (42 U.S.C. 241); 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?

No

Identify the sources of PII in the system.

Government Sources

State/Local/Tribal

Non-Governmental Sources

Other

Identify the OMB information collection approval number and expiration date

N/A

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

Vaccination tracking

Private Sector

Used by pharmacies and providers to make informed clinical decisions and to complete an individual’s vaccination history.

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

Data Use Agreement (DUA) between the IIS’s jurisdiction and the Association of Public Health Laboratories (APHL). APHL hosts the IZ Gateway system in the APHL Informatics Messaging System (AIMS).

Business Associate Agreement (BAA) between the Provider organization (HIPAA-covered entity) and APHL.

This is outside of IZ Gateway's system boundaries, but pertinent to data transfer that utilizes the IZ Gateway:

Public Health IIS Interjurisdictional Memorandum of Understanding (MOU) between any 2 IIS (jurisdictions).

IIS-Jurisdiction Specific Provider Agreement (JSPA) between a provider organization and the IIS jurisdiction.

Describe the procedures for accounting for disclosures.

N/A

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

Not applicable. Notice is the responsibility of the individual jurisdictional IIS or provider/pharmacy that collects information directly from an individual and supplies it to IZ Gateway. These jurisdictional IIS are outside of IZ Gateway boundaries.

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.

IZ Gateway is not the source system. The tool is used to route messages between IIS and/or provider/pharmacy. It is the responsibility of the IIS jurisdiction or provider/pharmacy to provide methods for individuals to opt-out of the use or collection of their PII. These applications are outside of IZ Gateway boundaries.

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

IZ Gateway is not the source system. The tool is used to route messages between IIS and/or provider/pharmacy. It is the responsibility of the individual jurisdictional IIS or provider/pharmacy that collects information directly from an individual and supplies it to IZ Gateway to provide appropriate processes to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system.

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.

IZ Gateway does not itself have a defined redress process. The tool is used to route messages between IIS and-or provider/pharmacy. Any redress processes are defined by the individual jurisdictional IIS and providers, and it is their responsibility to handle any concerns that might arise from impacted individuals. Those systems are outside of IZ Gateway boundaries.

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

Periodic PII reviews, if any, are to be performed at the jurisdictional/provider level.

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

Users:

Patient record entry, reconciliation and queries

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

The individual ISS jurisdictions review and/or determine who has access at the state level. The system's Business Steward (CDC) reviews user access on a quarterly basis to determine if access is still required.

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.

The ISS jurisdictions review and/or determine who has access at the state level, ensuring that role-based access and least privilege controls are employed.

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.

The system is owned by CDC. All CDC personnel are required to take Privacy and Security Awareness Training at least annually.

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

N/A

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 Secuirty 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 Security Controls are inherited from the Amazon Web Services (AWS) Platform FedRAMP data center, FedRAMP control set, and inclusive of AWS FedRAMP platform plugins. 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 Security Controls 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.