Data Use and Sharing Agreement to Support the United States Government's COVID-19 Emergency Response
Jurisdiction Immunization and Vaccine Administration Data Agreement

This Data Use and Sharing Agreement (DUA) is made between **the Michigan Department of Health and Human Services, located at 333 South Grand Ave, Lansing, Michigan** and the Centers for Disease Control and Prevention (CDC), an agency of the Department of Health and Human Services (HHS), to describe the data use and sharing parameters for certain immunization and vaccine administration data, as further described herein. This DUA: 1) describes the data needed for the monitoring of COVID-19 vaccine uptake; 2) describes the methods and parties within CDC, HHS, and other users who will be authorized to access, display, or share these data; 3) describes platforms for the rapid collection, transmission, use, storage, and maintenance of vaccine administration data available to jurisdictions; 4) establishes the terms and conditions for the sharing, protection, and use of these data with CDC, HHS, and other federal partners; and 5) sets forth the roles and responsibilities of each party.

The DUA is effective as of December 2, 2020.

Background and Purpose

Access to immunization and vaccine administration data is critical to the whole of government response to the Coronavirus Disease 2019 (COVID-19) public health emergency. In furtherance of federal government response efforts, HHS and CDC seek to obtain and utilize these data from various immunization and vaccine data sources, including a jurisdiction's immunization information system (IIS), pharmacies, federal provider organizations, and other relevant parties for a range of purposes, including but not limited to, rapidly assessing patterns of vaccination among the population; identifying pockets of undervaccination; assisting in determining vaccine resource allocation to address the needs of jurisdictions; monitoring vaccine effectiveness and safety; assessing spectrum of illness, disease burden, and risk factors for severe disease and outcomes; and helping to understand the impact of COVID-19 on the healthcare system and communities.

To support these purposes, HHS and CDC, working with partners, have developed a technical architecture to facilitate the transmission of jurisdictional vaccine administration data from various sources to CDC, and then to HHS's Tiberius analytic platform, to generate a comprehensive picture of COVID-19 vaccine uptake nationally. HHS and CDC 1) have developed specifications to describe critical demographic and vaccination elements for COVID-19 vaccine administration to be reported to CDC; 2) have made available a series of platforms and tools for use by data sources to manage, share, and store their immunization data in furtherance of the response; 3) will, consistent with applicable law, enable the secure transmission of extracted data from and across these platforms for further use by jurisdictions, CDC, HHS, and other federal partners in furtherance of the response; 4) as applicable, will assure compliance of these platforms with the Federal Information Security Management Act (FISMA) and other federal data security policies; and 5) will provide operational support to the data sources and other authorized users of the various platforms, as appropriate.

To ensure comprehensive monitoring of vaccine administration, HHS and CDC are requesting the following types of COVID-19 vaccine administration data. A detailed description of these elements, data submission specifications, and relevant systems can be found in Appendices A–D.

1. Record-Level, Identifiable Dataset: This dataset, which will reside in the Data Clearinghouse (DCH), contains identifiable data elements, as defined in Appendix D, and is being requested for specific purposes, including to assess and verify second-dose vaccination, to assess vaccine safety, and to allow for critical vaccine effectiveness monitoring. Identifiable elements are also needed to ensure proper deduplication of information for analytic purposes. Neither HHS nor CDC will have access to or release such identifiable data, including but not limited to names and other identifying information of persons who are the subject of such data, either during the term of this DUA or longer, except as consistent with this DUA or as may be allowed or required by applicable law. Jurisdictions that are unable (due to legal or regulatory restrictions) to submit identifiable data to CDC will be provided with the alternative option of implementing Privacy-Preserving Record Linkage (PPRL) technology when it is available see Appendix E).

2. Record-Level, Redacted Dataset: This dataset, which, after submission, will reside in the Immunization Data Lake (IZ Data Lake) is a condensed version of the identifiable dataset and does not include 16 of the 18 identifiers as defined under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). These data will also be used to monitor vaccine uptake, but a jurisdiction may be unable to fully assess the second-dose vaccination needs of its population, particularly in a case when individuals are vaccinated in multiple states. Therefore, jurisdictions submitting record-level, redacted datasets because of legal or statutory prohibitions against submitting identifiable data to CDC will be provided with the alternative option of implementing Privacy-Preserving Record Linkage (PPRL) technology when it is available (see Appendix E).

Information regarding all variables requested for submission to CDC, Data Security, and Data Access are described throughout this DUA. Consistent with MCL 333.9207(2), Administrative Rule 325.166, only deidentified data, or data that does not identify the subject of the record, will be provided. (https://dtmb.state.mi.us/ORRDocs/AdminCode/976_2011-013CH_AdminCode.pdf)

Authority

HHS and CDC are authorized by Sections 301 and 319D of the Public Health Service Act [42 U.S.C. §§ 241 and 247d-4], as amended, to maintain active surveillance of diseases through epidemiologic and laboratory investigations and data collection, analysis, and distribution.

The jurisdiction entering this DUA agrees that it is authorized under MCL 333.9207(2), Administrative Rule 325.166 to send deidentified data to and through the Vaccine Administration Management System (VAMS), COVID-19 Data Clearinghouse (DCH), Immunization Data Lake (IZ Data Lake), and HHS Tiberius (Tiberius), as those platforms and systems are further defined herein, and/or will obtain consent from any external entities or individuals from whom it collects data to allow for such sharing and use.

In addition, HHS and CDC each is a "public health authority," as defined under 45 C.F.R. §164.501 and as used in 45 C.F.R. §164.512(b), Standards for Privacy of Individually Identifiable Health Information, promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and, as such, covered entities are authorized by 45 CFR 164.512(b) to disclose Protected Health Information (PHI) to CDC and HHS for the public health purposes described herein.

As applicable, the Parties acknowledge that the jurisdiction may be a covered entity or hybrid entity for purposes of HIPAA. As HHS and CDC each is a public health authority for purposes of this DUA, the Parties expressly do not intend to create a HIPAA business associate relationship.

Definitions

For the purposes of this Agreement, the following definitions shall apply and may be used in the main body of the DUA and/or in relevant appendices:

"Authorized User," for purposes of this DUA, means an individual who, as part of directly supporting the whole of government response efforts, has a need for data stored in the DCH, the IZ Data Lake, and/or the Tiberius platforms in furtherance of the purposes and uses set forth herein. Authorized Users will generally be employees, contractors, and/or other agents specified by jurisdictions or federal agencies engaged in the response for purposes of addressing critical public health and emergency response activities, including assessing infrastructure needs and resource allocation. Authorized Users must adhere to applicable federal law and to any applicable provisions set out in this DUA with respect to the data stored in the respective platforms, which are further defined herein and described in Appendices A–D.

"Covered Data" means the information that is being shared by the jurisdiction with each relevant platform as further described in Appendices A–D, but that is generally categorized into four primary datasets: the IIS data (coming directly from an IIS or through VAMS), the DCH data, the IZ Data Lake data, and the Tiberius data. HHS and CDC acknowledge that the Covered Data to which each agency will have access is the minimum amount of information necessary to accomplish public health or emergency response needs. A list of Covered Data elements for each dataset is provided in Appendices A–D.

Covered Data may be used by Authorized Users within the parameters set forth in this DUA. The data elements listed in Appendices A–D will be updated periodically as more information on COVID-19 immunization is available. The overall DUA will remain unaffected by subsequent updates to the Appendices; jurisdictions will be notified of any such updates as soon as practicable and be afforded an opportunity to coordinate with HHS and CDC on implementation of the updates. Appendices A–D also provide the mode and method of secure transmission of the data from the jurisdiction's IIS or similar system(s) directly to the DCH; from the DCH to the IZ Data Lake; and from the IZ Data Lake to Tiberius. This information includes the potential availability and use of a privacy-preserving record linkage (PPRL) tool, which may be made available by HHS or CDC, either directly or by and through a contractor (Appendix E). Of note, data entering the DCH through the Immunization (IZ) Gateway will be governed by agreements between the IIS jurisdiction and the Association for Public Health Laboratories (APHL).

"Immunization Information System" or "IIS" are confidential, population-based, computerized databases that record all vaccine doses administered by participating healthcare providers to persons residing within a given geopolitical area.

"Jurisdiction" means the state, territorial, or local health jurisdiction operating under either statutory or regulatory authority to obtain and use health-related data for population health protection. For the purposes of this document, jurisdictions are funded under CDC-RFA-IP19-1901 317 Notice of Funding Opportunity. For the purposes of this DUA, the jurisdiction is the data source that, by and through an IIS and/or similar system(s) created to serve a range of administrative functions related to vaccines, provides Covered Data as set forth herein. Generally, the IIS or similar system(s) will collect data from public and private health care provider organizations (e.g., electronic health records [EHRs], health information systems [e.g., vital statistics, state Medicaid agencies, etc.], and pharmacies).

"Redacted Dataset" means the exclusion of direct identifiers of an individual, but with minimum necessary elements related to vaccine administration management as further defined in Appendix D.

"Party" means a state, territorial, or local jurisdiction or CDC; **"Parties"** means state, territorial, or local jurisdictions and CDC.

"Privacy-Preserving Record Linkage (PPRL)" means the process whereby personally identifiable information (PII) is redacted from a patient/customer record using a one-way, irreversible encryption algorithm to create one or more unique tokens that replace PII elements and allow data systems to match patient/customer records. PPRL is an industry standard that has been implemented and integrated across several data collection sectors where an individual's privacy must be maintained (e.g., health care, biomedical research, payment and claims, retail, intelligence, social research, and public health). For COVID-19 vaccination reporting, PPRL offers jurisdictions a mechanism to meet applicable jurisdiction regulations where data sharing with partners such as HHS and CDC may be limited (Appendix E).

"**Provider**" means an individual health professional or health facility organization licensed to provide healthcare diagnosis and treatment. For the purpose of this DUA, a provider is also a health professional who administers COVID-19 vaccine.

"Vaccine Administration Management System" or "VAMS" means the CDC-provided and supported web-based application that provides an option for a jurisdiction to plan and execute COVID-19 vaccine administration in temporary, satellite, or mobile vaccination settings.

"Vaccine Ordering Data" are data from the Vaccine Tracking System (VTrckS), CDC's vaccine order management system, which supports routine vaccination and will also be used for all COVID-19 vaccine ordering (Appendix B). VTrckS receives data from jurisdiction IISs and from providers.

"Vaccine Inventory Data" are data reported to CDC's VaccineFinder website, which helps: 1) the public find providers who offer select vaccines-2) healthcare providers to list their vaccination locations in a centralized, searchable database, and 3) collects vaccine supply data from providers. Jurisdictions have the ability to choose to report on behalf of all providers in the jurisdiction.

"Vaccine Administration Data" are demographic and vaccine-related data elements collected by vaccination providers at the point of vaccination. The primary purposes of these data include (but are not limited to): 1) monitoring the number of COVID-19 doses administered among populations; 2) assessing national COVID-19 vaccination coverage; and 3) assessing vaccine safety and effectiveness. IISs are the primary source of vaccine administration data for many jurisdictions, providing information on an individual's first dose of vaccine to inform the appropriate second dose. **The provisions outlined**

within this DUA specifically address vaccine administration data and its transmission from the jurisdiction to the DCH, transmission from the DCH to the IZ Data Lake, and to the Tiberius platform.

Description of Data Requested and Transmission Specification

COVID-19 Vaccine Reporting Specification (CVRS) Document (Appendix D)
The jurisdiction agrees to data for all persons receiving a COVID-19 vaccine in the jurisdiction, subject to the terms and conditions included in this DUA and applicable to that platform. Data elements required for submission by the jurisdiction include all variables as outlined in the current CDC COVID-19 Vaccine Reporting Specification (CVRS).

CVRS defines the COVID-19 vaccine administration data reporting requirements for the DCH. This specification addresses how a jurisdiction, by and through its IIS and/or similar system, will report vaccine administration data to the DCH. The jurisdiction is expected to include all variables as listed in the CVRS document as specified (e.g., in the same order as listed in the data dictionary, Appendix C). Columns should be present for all variables, including those variables that are not populated. If values for a variable(s) are not captured and stored at the jurisdiction at the record level, the jurisdiction should not try to derive this information to complete the field prior to submitting data to the DCH. The jurisdiction should follow all parameters as outlined in the CVRS file specifications, including reporting requirements.

The CVRS document and comprehensive data dictionary documents will be updated periodically to incorporate revisions to code sets, such as when new vaccines are introduced. In the future, the specification will also be expanded to include and additional mechanisms for reporting (e.g., data transport via the IZ Gateway). All mechanisms will use the same file format but will vary in what identifying information is provided. The jurisdiction agrees to comply with all specifications as defined in the CVRS document and implement changes outlined in the CVRS as expeditiously as possible, provided however that the jurisdiction will submit only deidentified data. Jurisdictions will be notified of changes or updates to the CVRS document as soon as possible, and such changes will be updated online and can be accessed at the following location.

Data Access and Use

HHS and CDC, working with their partners, have created a technical architecture (Appendix A) containing various platforms to facilitate the management, sharing, storage, and analysis of vaccine administration data. In accordance with this agreement, the Jurisdiction acknowledges and agrees that HHS, CDC, and Authorized Users may use the Covered Data transmitted through the technical architecture, including the DCH, IZ Data Lake, and Tiberius platforms as described in this DUA and Appendix B, in furtherance of response activities related to the COVID-19 pandemic. This includes, at a minimum, the following activities, which jurisdictions shall complete as applicable to the platform and consistent with this DUA:

a. As applicable to the platform and consistent with this DUA, analyze and visualize the Covered Data, to which they have access, to improve the monitoring of vaccination and vaccine-related activities for the COVID-19 pandemic response, including vaccine safety and assessment of vaccine effectiveness;
b. As applicable to the platform and consistent with this DUA, share the Covered Data and/or analyses thereof with official federal, state, local, tribal, and territorial government health agencies or their agents and/or entities collaborating with them, as the health agencies

conduct their public health and vaccination response responsibilities consistent with their statutory authorities;

c. Develop analytic methods using the Covered Data to identify immediate public health events or concerns at the federal, state, territorial, and local level that warrant further public health investigation or immediate public health intervention actions;

d. Enable Authorized Users, including public health and emergency response officials, to query the Covered Data within the HHS- and CDC-provided data platforms as may be necessary to carry out critical public health functions;

e. Share specified data elements with Tiberius for the visualization of vaccine administration data; and

f. Publish findings and conclusions related to their analyses of the data provided. As appropriate, publications will acknowledge Jurisdiction as the source of the data in any such publication. Given the emergent nature of the response, HHS and CDC may not be able to inform or seek approval from Jurisdiction for such publications but will coordinate as soon as possible and practicable. Information will be reported and published in aggregate.

Data access and permissions for all Covered Data as described in this DUA are further described in Appendix B. This includes data access and permissions for Authorized Users at CDC and HHS. In addition, data that are transmitted from the IZ Data Lake to Tiberius will adhere to all aspects of a signed Memorandum of Agreement (MOA) between CDC and HHS (Appendix F). The MOA: 1) describes the framework through which HHS and its platform partners will rapidly obtain, integrate, use, store, and maintain a local copy of data provided by CDC into the Tiberius platform; 2) establishes the terms and conditions for sharing, protection, and use of CDC COVID-19 vaccine distribution, administration, and inventory data in Tiberius provided hereunder and further described below; and 3) sets forth the roles and responsibilities of each party.

This MOA between HHS and CDC is effective as of September 29, 2020. Additional information about data use terms, asset protection, data disposition, terms of agreement, amendment, and termination of the agreement are further described in Appendix F.

Data Confidentiality and Security

Data confidentiality, security, and access processes specific to the DCH, IZ Data Lake, and Tiberius are further described in Appendix B. However, as a general matter, HHS and CDC agree to the following:

Confidentiality: Where Covered Data provided pursuant to this DUA are identifiable or potentially identifiable, HHS and CDC agree to maintain the confidentiality of the Covered Data to the fullest extent required by federal law, which includes, as applicable, the Privacy Act of 1974; standards promulgated pursuant to HIPAA, and the Freedom of Information Act (FOIA), including exemptions provided thereunder.

HHS and CDC further agree to not disclose such Covered Data, including but not limited to names and other identifying information of persons who are the subject of such Covered Data, either during the term of this DUA or longer, except as consistent with this DUA or as may be allowed or required by applicable law. Where required by law and/or where practicable, HHS and CDC agree to notify the Jurisdiction before releasing Covered Data to a third party pursuant to a judicial, governmental, or other request under law, to allow the Jurisdiction the opportunity to state any objection to the disclosure of the Covered Data.

Security: As applicable to the platform, HHS and CDC will establish appropriate administrative, technical, procedural, and physical safeguards to ensure the confidentiality and security of Covered Data in their custody and control, consistent with federal requirements under FISMA and other applicable federal laws. The safeguards shall provide a level and scope of security that is not less than the level and scope of security established by applicable law for the type of data provided under this DUA and are intended to protect Covered Data from unauthorized access, disclosure, use, or modification. This includes setting permissions to access or edit data commensurate with the level of sensitivity of the data. Should there be a data breach and unauthorized disclosure of Covered Data, consistent with applicable legal requirements, an Authorized User must notify appropriate response teams within CDC, which will, in turn, will notify the relevant jurisdiction of the incident as soon as practicable, and, to the extent allowed by federal law, will coordinate with Jurisdiction in responding to the incident.

Transfer: Transfer or transmission of the Covered Data by and through the various platforms in the control of HHS and CDC shall be done in accordance with acceptable practices for ensuring the protection, confidentiality, and integrity of the contents, commensurate with the level of sensitivity of the Covered Data. The Parties may coordinate to implement methods to achieve these outcomes consistent with procedures already in place for similar data exchanges. If encrypted identifiable information is transferred electronically through means such as the Internet, then said transmissions will be consistent with the rules and standards promulgated by applicable legal requirements regarding the electronic transmission of identifiable information.

Storage: Covered Data will be maintained and stored in compliance with the HHS and CDC security policies and procedures and consistent with applicable federal law. Where Covered Data are identifiable or potentially identifiable or are privileged, sensitive, or confidential, such records and data shall be secured in an encrypted, password-protected electronic folder with access restricted to Authorized Users for purposes as set forth in this DUA.

Access: HHS and CDC may provide Covered Data access to appropriate employees, contractors, and other Authorized Users, as further provided in this DUA. HHS and CDC agree to establish appropriate administrative, technical, and physical safeguards to prevent unauthorized access to the Covered Data. Where Covered Data provided pursuant to this Agreement are identifiable or potentially identifiable or are privileged, sensitive, or confidential, HHS, CDC, and their Authorized Users shall access Covered Data on secured devices only.

Data Maintenance, Deletion, or Storage Requirements after Termination

Unless explicitly stated otherwise in the DUA, ownership of Covered Data shall remain with the Jurisdiction. However, the Parties agree that the Covered Data provided under this DUA and in the custody and control of HHS and CDC are subject to applicable federal law.

Accordingly, HHS and CDC agree to maintain, store, protect, archive, and/or dispose of Covered Data in accordance with federal law. When HHS and/or CDC acts as an Authorized User, as federal agencies, the disposition of records in their custody and control is governed by the Federal Records Act and may only be accomplished in accordance with schedules for destruction as provided under law. At a minimum, the Jurisdiction agrees that an archival copy of the Covered Data may be retained by HHS and CDC to comply with relevant records retention requirements and/or for the purposes of research integrity and verification. Obligations under law to maintain and secure Covered Data will survive termination of this DUA.

IT and Data Architecture

HHS and CDC are expanding the capacity of the following secure, certified, cloud-based data management platforms:

Vaccine Ordering and Inventory Systems (Appendix B)

a. Vaccine Tracking System (VTrckS): The Vaccine Tracking System (VTrckS) is the Centers for Disease Control and Prevention's (CDC) vaccine order management system, which will support:
    i. Vaccine allocation
    ii. Ordering
    iii. Reporting throughout the vaccine distribution process, from vaccine order placement through distribution
    iv. Tracking vaccine shipments
b. VaccineFinder: The VaccineFinder website helps the public find providers who offer select vaccines; allows healthcare providers to list their vaccination locations in a centralized, searchable database; and collects vaccine supply data from providers

Vaccine Administration and Reporting Systems (Appendix B)

a. *Vaccine Administration Management System (VAMS):* Vaccine Administration Management System (VAMS) is a web-based application that supports planning and execution for temporary, mobile, or satellite COVID-19 vaccination clinics. Use of VAMS is optional.

b. *IZ Gateway*: The IZ Gateway is a cloud-based message routing service intended to enable data exchange between IISs, other provider systems, and the IZ Data Lake. The IZ Gateway enables centralized data exchange and eliminates the need for multiple, individual, point-to-point connections. Use of the IZ Gateway is encouraged but not required and is further set out in agreements between a jurisdiction and APHL.

c. *COVID-19 Data Clearinghouse (DCH)*: The DCH is a cloud-hosted data repository that receives, deduplicates, and redacts COVID-19 vaccination data that are then used to populate the IZ Data Lake with a limited dataset for analytics. The DCH may also be used by the Jurisdiction and/or healthcare providers to enable appropriate administration and dosing for individuals receiving vaccines. For example, if populated with identified data or identified data that have been redacted using privacy-preserving record linkage (PPRL) software, then the DCH would allow healthcare providers to search for a patient, see what brand of COVID-19 vaccine they received, and see when they received their first dose of COVID-19 vaccine to ensure dose matching and appropriate vaccination intervals to complete the vaccination series.

d. *Immunization (IZ) Data Lake*: The IZ Data Lake is a cloud-hosted data repository to receive, store, manage, and analyze a limited dataset for COVID-19 vaccination data.

Miscellaneous

1. Data Disposition: As noted above, Covered Data that have been provided to HHS and CDC under this DUA will be archived, stored, protected, or disposed of in accordance with relevant federal records retention requirements.
2. Funding: This DUA is not an obligation or a commitment of funds or a basis for a transfer of funds. This DUA does not create an obligation or commitment to transfer data, but rather is a statement of understanding between the parties concerning the sharing and use of Covered Data. Expenditures by each party are subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. To the extent funds provided by CDC under a cooperative agreement are used by a jurisdiction in furtherance of these activities, the terms of that cooperative agreement will be read, consistently with the terms of this DUA. Any conflict discovered must be raised with CDC for resolution.
3. Settlement of Disputes: Disagreements between the parties arising under or relating to this DUA will be resolved by consultation between the parties and referral of the dispute to appropriate management officials of the parties whenever possible.
4. Applicable Laws: U.S. federal law shall govern the construction, interpretation, and performance of this DUA.

Term of Agreement, Amendment, and Termination:

1. The term of this DUA shall be one year commencing from the date of the final signature or shall last for the duration of the national emergency, whichever is longer. The DUA may be renewed upon mutual written consent of the Parties.
2. Except as otherwise expressly provided herein, this DUA may be amended only by the mutual written consent of the authorized representatives for each Party. However, the Parties acknowledge that changes and updates to the Appendices may occur during the term of the DUA; the Parties agree that such changes and updates are incorporated upon issuance.
3. This DUA may otherwise be terminated with ninety (90) days' advance written notice by either party.
4. Any notice required under this DUA must be in writing and sent by electronic mail (iisinfo@cdc.gov) with written acknowledgement of receipt to the email address for each Party provided below.
5. Each Party represents that the individual signing below on behalf of the party has the authorization to bind the party indicated to this DUA. This DUA may be signed in counterparts and signatures provided electronically will be deemed originals.

CENTERS FOR DISEASE CONTROL AND PREVENTION AND JURISDICTION

By: ________________________
Name: ____________________
Title: ________________________
Date: __________________________
Email: _______________________

By: Bob Swanson
Name: Bob Swanson
Title: Director, Division of Immunization
Date: 12/2/2020
Email: SwansonR@Michigan.gov

By: ________________________
Name: ____________________
Title: ________________________

By: Cynthia Green-Edwards
Digitally signed by Cynthia Green-Edwards
Date: 2020.12.02 16:12:09 -05'00'
Name: Cynthia Green-Edwards
Title MDHHS Chief Compliance Officer

Date: ___________________________

Email: ________________________

Date: December 2, 2020

Email: EdwardsC@michigan.gov

Description of Appendices

Appendix A: Vaccine Administration Technical Architecture Diagram

Appendix B: Overview of COVID-19 Vaccine Reporting Systems

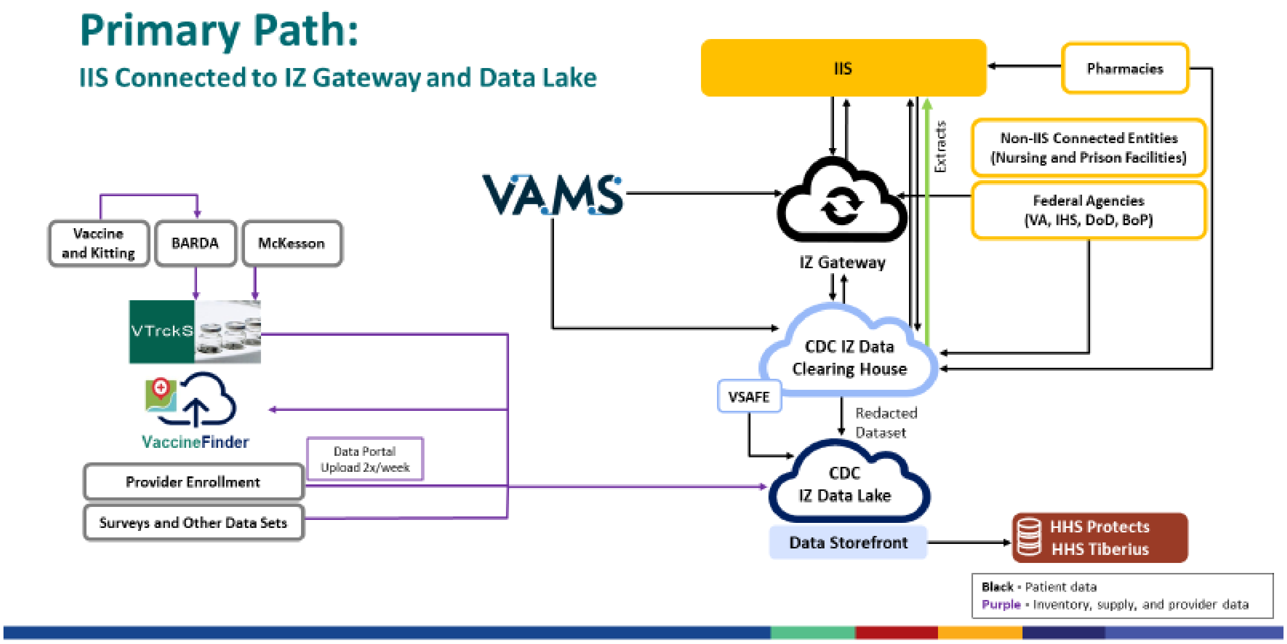
Appendix C: COVID-19 Comprehensive Data Dictionary

Appendix D: COVID-19 Vaccination Requirement Specification (CVRS) Instructions Document and File Specification

Appendix E: Description of Privacy-Preserving Record Linkage

Appendix F: Memorandum of Agreement (MOA) between Tiberius and CDC

Appendix A: Vaccine Administration Technical Architecture Diagram


Primary Path:
IIS Connected to IZ Gateway and Data Lake
IIS
Pharmacies
Extracts
Non-IIS Connected Entities (Nursing and Prison Facilities)
Federal Agencies (VA, IHS, DoD, BoP)
VAMS
IZ Gateway
Vaccine and Kitting
BARDA
McKesson
VTrckS
VaccineFinder
Data Portal Upload 2x/week
Provider Enrollment
Surveys and Other Data Sets
CDC IZ Data Clearing House
VSAFE
Redacted Dataset
CDC IZ Data Lake
Data Storefront
HHS Protects
HHS Tiberius
Black - Patient data
Purple - Inventory, supply, and provider data

Appendix B: Overview of COVID-19 Vaccine Reporting Systems

This document provides an overview of the COVID-19 vaccine reporting systems and their interactions with one another, including information regarding Data Sharing, Access, and Security. The description of "Systems for Vaccine Ordering and Supply," including VTrckS and VaccineFinder, is intended to provide additional context for the vaccine system landscape. These systems are covered by their own DUA, MOUs, and relevant agreements. The description of "Systems for Vaccine Administration and Reporting" is intended to provide additional information regarding the systems covered under this DUA.

Systems for Vaccine Ordering and Supply

Vaccine Tracking System (VTrckS)

Overview

The Vaccine Tracking System (VTrckS) is the Centers for Disease Control and Prevention's (CDC) vaccine order management system, which will support:

- Vaccine allocation
- Ordering
- Reporting throughout the vaccine distribution process, from vaccine order placement through distribution
- Tracking vaccine shipments

Data Sharing

VTrckS can receive or exchange data with the following systems:

- **VTrckS ExIS Portal**: used by jurisdictions and federal and commercial partners to submit vaccine orders, enrolled provider master data, as well as vaccine inventory, return, and wastage information into VTrckS
- **Jurisdiction IISs**: download vaccine shipment data from VTrckS
- **McKesson** (VTrckS current logistics contractor): receives orders from VTrckS, directs vaccine manufacturers to ship vaccines, and transmits vaccine shipment details from providers to VTrckS
- **Immunization (IZ) Data Lake**: receives data feeds from VTrckS related to provider data, orders, shipments, inventory, and allocations
- Data elements related to VTrckS that will be received by or exchanged with the systems mentioned above can be found in the COVID-19 Comprehensive Data Dictionary.

Access and Security

VTrckS is owned by CDC and hosted in CDC data centers. The system has been in use by all immunization programs for vaccine ordering and management since 2010. VTrckS is built using SAP Enterprise Resources Platform (ERP), which is one of the most widely used supply chain management technologies available today. All system infrastructure is built utilizing virtual machine architecture with full redundancy in case of any disasters (e.g. natural disasters, calamities, system malfunctions). VTrckS has a full Authority-to Operate issued by the CDC Security Office and meets federal security standards as established by the National Institute of Standards and Technology (NIST). The system has a robust security profile and provides role-based access to its users. Access to the system is through the CDC

Secure Access Management System and requires different levels of authentication depending upon user groups. Over the last few years, the system has undergone multiple independent security reviews, which have greatly helped in further enhancing its security profile.

VaccineFinder

Overview

The VaccineFinder website helps: 1) the public find providers who offer select vaccines, 2) healthcare providers list their vaccination locations in a centralized, searchable database, and 3) collect vaccine supply data from providers. Approved COVID-19 vaccination providers will be able to report on-hand COVID-19 vaccine inventory each day through VaccineFinder to CDC. Vaccination providers can report manually via a secure online portal (web form or data file upload) or via an automated secure data transfer.

The COVID-19 Vaccination Program Provider Agreement requires providers to report supply information as directed by CDC. Organizations or provider locations receiving COVID-19 vaccines should report supply levels daily to VaccineFinder using the online COVID Locating Health Provider Portal. The following process outlines onboarding for VaccineFinder via the COVID Locating Health Provider Platform, which will be made available on November 16, 2020:

1. COVID-19 vaccination providers must be registered in VTrckS. Providers will receive an email from the new COVID Locating Health Provider Portal with instructions for completing the enrollment process. This email will be sent to the organization's email address submitted in the provider enrollment form.
2. Organizations will determine if they report daily on-hand inventory supply on behalf of all their provider locations, or if provider locations are responsible for reporting this information. The reporting structure identified by each organization must be maintained for the duration of the COVID-19 vaccination program
    - Provider locations designated as inventory reporting entities by their organizations will receive instructions for completing the COVID Locating Health Provider Portal enrollment process.
3. Organizations enrolled in the new COVID Locating Health Provider Portal can view their approved provider location details and update inventory within the portal. Provider locations identified as inventory reporting entities will enroll to access their COVID Locating Health Provider Portal account and report daily inventory of COVID-19 vaccines.
4. Additional detailed steps for onboarding will be available on November 16, 2020.

Data Sharing

- **IZ Data Lake:** VaccineFinder sends inventory/supply data to the IZ Data Lake and receives provider enrollment data from the IZ Data Lake.
- All data elements related to VaccineFinder that will be received by or exchanged with the systems mentioned above can be found in the COVID-19 Comprehensive Data Dictionary.

Access and Security

The VaccineFinder provider portal is being developed and maintained by Boston Children's Hospital HealthMap in partnership with CDC and Castlight. Castlight operates in a highly regulated industry and aligns access and security requirements with industry security standards. This includes annual validation of its SOC 2 Type 2 (SSAE 18) by an independent third party; SOC 2 maps controls to HIPAA and HITECH frameworks. From this annual, a SOC 2 report is generated. The SOC 2 report also provides detailed controls to support security, availability, and confidentiality. In addition, the report includes routine independent penetration testing; routine internal evaluation and maintenance of a Security Information Event Management (SIEM); and anti-virus solutions. The report also abides by the least access principle, endpoint data loss prevention (DLP), routine vulnerability scanning, and incident response team. These activities are reviewed and validated by an independent third-party auditor.

The VaccineFinder Locating Health provider portal is securely accessed with log-in and password credentials. This platform is hosted on Amazon Web Services and maintains best practice standards by the Boston Children's Hospital Innovation and Digital Health Accelerator. IISs and pharmacy partners will identify system users who will have access to update inventory supply information in VaccineFinder. Additionally, pharmacy partner organizations will have the ability to manage role-based user access at registration. Each partner organization will have access to provider location details within the organization, and each location will only have access to data it submitted.

Systems for Vaccine Administration and Reporting

COVID-19 Data Clearinghouse

Overview

The COVID-19 Data Clearinghouse (DCH) is a cloud-hosted data repository that receives, deduplicates, and deidentifies (to the parameters of a "redacted dataset," described in the "definitions" section of the DUA) COVID-19 vaccination data that are then used to populate the IZ Data Lake with redacted dataset analytics.

One use of the DCH space is as follows: if populated with identified data or identified data that has been redacted using privacy-preserving record linkage (PPRL) software, then the DCH will allow healthcare providers to search for a patient, see w which COVID-19 vaccine product they received, and see when they received their first dose to ensure dose matching and appropriate vaccination intervals to complete the vaccine series. In addition, data in the DCH are deduplicated and redacted prior to their transmission to the IZ Data Lake.

Data Sharing

The COVID-19 DCH receives data from:

- **VAMS (if applicable)**: Sends vaccine administration data to the DCH, where it is redacted, stored, and sent to the IZ Data Lake to meet CDC reporting requirements. In addition, jurisdictions may download their identified VAMS dataset for incorporation into their IISs. Note: A complete list of data elements (including those that are identified) that will be sent to the DCH from VAMS are included in the CDC COVID-19 Vaccination Reporting Specification Document (CVRS Document, Appendix D).

- **IIS:** Sends file extracts to the DCH via file upload or application program interface (API); a limited dataset is sent to the IZ Data Lake to meet CDC reporting requirements. Data element requirements and file specification guidance can be found in the CVRS Document, Appendix D.
- **Federal Agencies and Pharmacies:** Send file extracts to the DCH via file upload or API; redacted data are sent to the IZ Data Lake to meet CDC reporting requirements.

Access and Security

The DCH is owned by HHS and hosted within an Oracle Cloud Infrastructure (OCI) U.S. Government Cloud tenancy. The infrastructure that supports the tenancy, such as storage, virtual networking, and computing, carries a Joint Authorization Board Provisional Authority to Operate (JAB P-ATO) at the FedRAMP High level from GSA (https://www.gsa.gov/technology/government-it-initiatives/fedramp). The DCH will be accredited for system security and authority to operate within CDC's IT boundaries based on the National Institute of Standards and Technology's (NIST) Risk Management Framework. The systems that are built within the Oracle Cloud tenancy, for example, the Virtual Machines that run the application and support systems, such as Security Information Event Management (SIEM), anti-virus, vulnerability scanning, and incident response, are not part of the FedRAMP accredited boundary. The systems outside of the FedRAMP boundary will be evaluated by HHS and CDC as part of the HHS/CDC ATO process. Data will not be submitted into the DCH (either through VAMS or direct extracts from the jurisdiction) until the system is fully functional and ready to accept the data. Information is forthcoming on the go-live date for the DCH, and jurisdictions will be informed through established communications.

The system will be independently audited against the criteria to maintain information integrity as well as system availability at the highest tier specified by the U.S. Government for its federally operated systems. The system will be certified to host personally identifiable information (PII) as well as protected health information (PHI). Oracle Cloud Infrastructure, but not the components within the HHS tenancy, carries a third-party HIPAA attestation to provide reasonable assurance that the infrastructure includes administrative, physical, and technical safeguards relevant to the HIPAA Security Rule, Breach Notification Rule, and the applicable parts of the Privacy Rule (see 45 CFR § 164.3 for relevant security standards for the protection of PHI). CDC and HHS will not be authorized to view identifiable portions of PHI stored in the DCH, but redacted PHI will be transferred to the IZ Data Lake. This information will be used to track and report progress of COVID-19 vaccine administration over time.

IISs and federal agency and pharmacy partners will identify system users who will have access to submitted data and data submission summaries. Additionally, partners will have the ability to manage role-based user access. Each partner will only have access to data it submitted or to data that are submitted from clinic applications, like VAMS, which is specifically routed for the partner.

Immunization (IZ) Data Lake

Overview

The IZ Data Lake is a CDC cloud-hosted secure data repository to receive, store, manage, analyze, and share redacted COVID-19 vaccination data.

Data Sharing

- **Data Clearinghouse:** Sends limited dataset of vaccine administration data to the IZ Data Lake from IISs, pharmacies, federal agencies, and VAMS.

- **Jurisdictions:** Share provider enrollment data with IZ Data Lake via file upload to the IZ Data Lake Partner Portal.
- **VTrckS:** Sends provider, shipment, and ordering data to the IZ Data Lake.
- **VaccineFinder:** Receives provider enrollment data from the IZ Data Lake and shares vaccine supply information with the IZ Data Lake.
- **CDC Internal Dashboards:** Receive secure views from the IZ Data Lake to visualize COVID-19 vaccine administration data.
- **Data Storefront and Tiberius:** Hubs that analyze, aggregate, and visualize data from the IZ Data Lake. The Data Storefront is internal to CDC and will analyze and aggregate information from the IZ Data Lake. Tiberius is an HHS platform that sits external to CDC and will visualize data from the IZ Data Lake. The relationship between Tiberius and CDC is described in Appendix F. Information regarding the data that will be provided to Tiberius is currently under development. It will include, at a maximum, variables described within the CVRS. CDC will share these specifications with jurisdictions as soon as they are derived.

Access and Security

IZ Data Lake: Is owned and operated by CDC and is hosted in CDC's FedRAMP Azure Infrastructure. The IZ Data Lake does not receive or store PHI. The datasets received and managed in the IZ Data Lake include redacted dataset on administration data from the DCH, ordering and inventory data from VTrckS, and provider enrollment data from jurisdictions. The data are encrypted as per the NIST FIPS-140-2 standards both in motion and at rest. The storage and access to the information are governed under the DUA. Access to the data is provided via a CDC Data Governance process that enforces DUA for all data products for all IZ Data Lake consumers, including HHS. The data in the IZ Data Lake will be used to report out to CDC programs and the Tiberius platform on the coverage and distribution of COVID-19 vaccine across the nation.

IZ Gateway

Overview

The IZ Gateway is a cloud-based message routing service intended to enable data exchange between IISs, other provider systems, and the IZ Data Lake. The IZ Gateway enables centralized data exchange and eliminates the need for multiple, individual, point-to-point connections. Use of the IZ Gateway is encouraged, but not required, and is governed by agreements between a jurisdiction and the Association for Public Health Laboratories (APHL).

Data Sharing

The IZ Gateway enables data exchange based on the level of onboarding chosen by the jurisdiction or organization and the associated legal agreements. Options include:

- Cross-jurisdictional data exchange and queries
- Multijurisdictional providers sharing data with multiple IISs via a central connection
- Routing of VAMS data to the appropriate IIS
- IISs reporting to the DCH

Access and Security

The IZ Gateway system is owned by CDC and hosted on the APHL Informatics Messaging System (AIMS). AIMS is built in an AWS FedRAMP Moderate Hosting environment that has undergone GSA evaluation and accreditation through a third-party assessment organization (3PAO). Both FedRAMP packages are available for request and review on the FedRAMP marketplace page. The Federal Information Security Management Act (FISMA) moderate level system designation is in alignment with Federal Information Processing Standards (FIPS) 199 and National Institute of Standards and Technology (NIST) T 800-37 Risk Management Framework. Associated corresponding security control sets defined in NIST Special Publication 800-53 were employed as part of the CDC system authorization and accreditation processes.

Access to the IZ Gateway API is limited to known data trading partners who have been issued digital certificates. CDC staff does not have access to any PII or PHI.

In addition, the IZ Gateway will obtain a signed, interim Authorization to Operate (ATO) before moving to production, completing the full ATO as soon as possible thereafter. An ATO represents CDC management's approval to place a system into operation. An ATO is granted after an IT system fully complies with the Certification and Accreditation (C&A) process. The C&A process includes documenting the system's security certification, security accreditation, E-authentication, and business continuity planning. The ATO also assigns the appropriate FIPS PUB 199 level, which guides additional details within the process. FIPS PUB 199 enables agencies to meet the requirements of FISMA and improves the security of federal information systems.

Vaccine Administration Management System

Overview

The Vaccine Administration Management System (VAMS) is a web-based application that supports planning and execution for temporary, mobile, or satellite COVID-19 vaccination clinics. Use of VAMS is optional. VAMS version 1.0 manages identification of priority populations through designated employers and organizations, recipient scheduling, clinic setup, vaccine inventory, and recipient notifications, and stores data for analytics and dashboards.

Data Sharing

DCH: Receives data from VAMS in accordance with jurisdiction preferences for using VAMS to meet CDC reporting requirements and jurisdiction preferences for retrieval of VAMS information by the IIS. The VAMS data are redacted, stored, and sent to the IZ Data Lake to meet CDC reporting requirements. CDC staff does not have access to any identifiable VAMS data.

Access and Security

The VAMS system is owned by CDC and hosted on Salesforce and AWS FedRAMP Moderate Hosting environments, which have undergone GSA evaluation and accreditation through a third-party assessment organization (3PAO). Both FedRAMP packages are available for request and review on the FedRAMP marketplace page. FISMA moderate level system designation is in alignment with Federal Information Processing Standards (FIPS) 199 and National Institute of Standards and Technology (NIST) T

800-37 Risk Management Framework. Associated corresponding security control sets defined in NIST Special Publication 800-53 were employed as part of the CDC system authorization and accreditation processes.

Access to the VAMS application requires multi-factor authentication for all users and associated roles. Roles and associated recipient data visibility are enforced by Salesforce role-based permissions, with role assignment managed by VAMS platform administrators, jurisdictional administrators, and clinic administrators. Roles have been configured to reduce the amount of available PII and PHI available to users to the greatest extent possible while still providing adequate information required to support recipient vaccination processes. CDC staff does not have access to any PII or PHI in the VAMS application.

Appendix C: Comprehensive Data Dictionary for CDC Vaccine Administration Requirements for COVID-19 Vaccine Monitoring: Available via hyperlink. Any updates or changes made thereto are incorporated by reference in this DUA.

Appendix D: COVID-19 Vaccination Reporting Specification Document (CRVS): Available via hyperlink. Any updates or changes made thereto are incorporated by reference in this DUA.

Appendix E: Privacy-Preserving Record Linkage

Currently, there is no consistent way for public health jurisdictions to share vaccine administration data with each other because of two major constraints. First, these data are considered PII and/or PHI and may be subject to a jurisdiction's laws and regulations that may prohibit or limit the sharing of such information outside the jurisdiction. Second, though most people will complete their vaccine series in the same jurisdiction, some individuals may cross jurisdictions before completion of the series. There are currently no optimal technical solutions to link vaccine administration data electronically across jurisdictional boundaries.

Privacy-preserving record linkage (PPRL) provides a practical way for jurisdictions to exchange information on vaccine administration with federal agencies, while preserving and protecting PII and PHI. By creating tokenized, deduplicated data, PPRL can link an individual's COVID-19 vaccination records to inform second dose delivery decisions without sharing PII across jurisdictional boundaries (Figure 1). PPRL has the potential to optimize vaccine administration efforts and streamline processes and resolve orphaned data issues within the IIS by providing record-linking without the need to exchange PII.

PPRL can also enable CDC to associate vaccine administration data from multiple sources (e.g., epidemiologic, laboratory, and immunization data) to a specific individual without receiving any PII that might compromise that person's privacy.

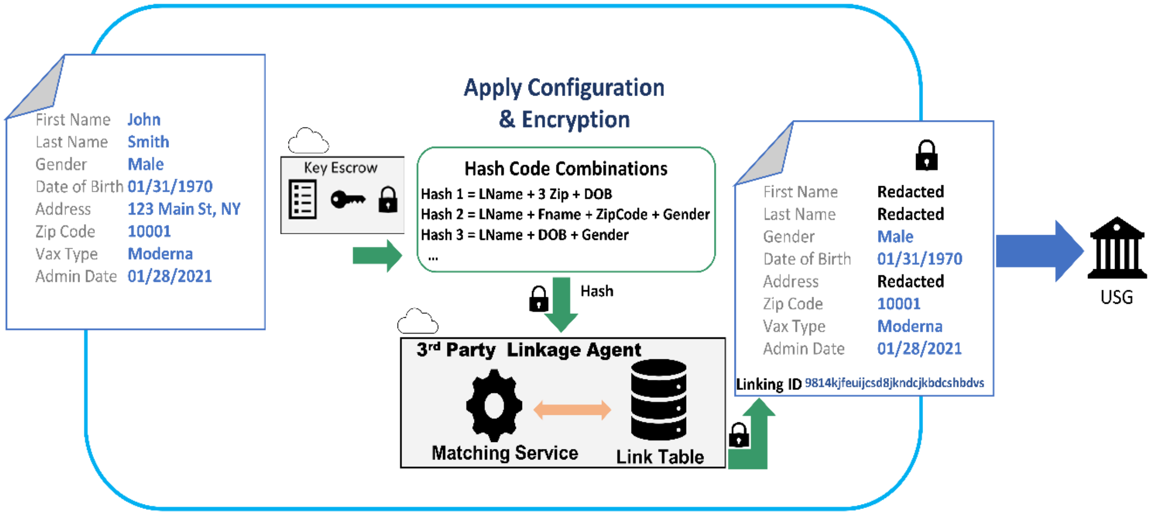
In the PPRL process, PII is hashed using a one-way, irreversible encryption algorithm to create one or more tokens in a series of prescribed steps prior to transmission beyond an organizational boundary for matching. Hashing works by passing a piece of data through a mathematical function to convert the data into a multi-character code that can be used by computers to match records in the same way that personally identifiable data would be used; the code(s) act as new record identifiers that are used to match with other records similarly converted to codes. The process of hashing results in the creation of unique information based on the PII data of interest that prevents an outside party from recovering the PII, while allowing for the establishment of links across organizations to share PII when necessary.

PPRL offers more than one protocol for establishing links. In a "direct" protocol, each party hashes and encrypts its PII and shares the hashed tokens directly with the other party to compare matches. In a "blind" protocol, a third party known as a "linkage agent" is provided access to the hashed data but is unable to view PII. The linkage agent then compares the obfuscated information to establish linkages using the tokens (see Figure below).

Commercial implementations of PPRL services operating in the health domain need to demonstrate that the tokens created are deidentified per the HIPAA standard. This includes demonstrating ability to resist cryptanalytic attacks, dictionary attacks, and statistical attacks (e.g., frequency attacks, collusion attacks).

Jurisdictions will be notified by HHS and/or CDC if and when PPRL is available, by and through HHS, CDC, or an HHS or CDC service provider, to jurisdictions for use in furtherance of this DUA.

Figure 1. Tokenization/Unique ID Creation



First Name John
Last Name Smith
Gender Male
Date of Birth 01/31/1970
Address 123 Main St, NY
Zip Code 10001
Vax Type Moderna
Admin Date 01/28/2021

Hash Code Combinations
Hash 1 = LName + 3 Zip + DOB
Hash 2 = LName + Fname + ZipCode + Gender
Hash 3 = LName + DOB + Gender
…

First Name Redacted
Last Name Redacted
Gender Male
Date of Birth 01/31/1970
Address Redacted
Zip Code 10001
Vax Type Moderna
Admin Date 01/28/2021
Linking ID 9814kjfeuijcsd8jkndcjkbdcshbdvs

Appendix F: Memorandum of Agreement (MOA), HHS Tiberius and CDC