

HHS/CDC SENSITIVE INFORMATION – REQUIRES SPECIAL HANDLING



**Department of Health and Human
Services Centers for Disease Control
and Prevention**

**INFORMATION EXCHANGE AGREEMENT (IEA) BETWEEN
CENTERS FOR DISEASE CONTROL AND PREVENTION (CDC)
AND**

**COVID-19 Immunization and Vaccine Administration Data
Reporter**

**U.S. Virgin Islands Department of Health
Immunization Division**

**Through
The Department of Property and Procurement**

IEA Version 1.0

IEA Effective this day 25th of February, 2022

Information Exchange Agreement

PURPOSE: The purpose of this Information Exchange Agreement (IEA) is to establish the terms, conditions, and safeguards under which the Coronavirus Disease 2019 (COVID-19) Immunization and Vaccine Administration Data Reporter, the U.S. Virgin Islands Department of Health, Immunization Division (hereafter referenced as the “Non-CDC Organization”) will transmit to the Centers for Disease Control and Prevention (CDC) certain information, records, or data for the purposes of reporting COVID-19 vaccine administration events through a system-to-system information exchange between the COVID-19 Data Clearinghouse (DCH) information system and the Non-CDC Organization system(s).

COVID-19 Immunization and Vaccine Administration Data Reporters include state, tribal, local, and territorial jurisdictions, federal agencies, pharmacies, and other relevant parties who will submit information from various immunization and vaccine data sources including but not limited to jurisdiction immunization information systems (IIS), pharmacy information systems (PIS), and federal provider organization information systems. Information, records, or data submitted shall adhere to specifications heretofore agreed upon within any related data use or program agreement between the Non-CDC Organization and CDC for this purpose.

By entering into this IEA, both the CDC and the Non-CDC Organization (hereafter referenced as “both parties”) agree to comply with the terms and conditions as set forth in the U.S. Department of Health and Human Services (HHS) Rules of Behavior for the Use of HHS Information and IT Resources Policy (HHS RoB) and all other terms and conditions set forth in this IEA. This IEA is also intended to facilitate mutual cooperation and coordination of both parties to ensure compliance with federal information technology (IT) policies designed to minimize security risks during system access and information exchange.

SCOPE: The scope of this IEA is based on, but is not limited to, the following activities, users, and components:

- Information exchange between the COVID-19 DCH information system and the Non-CDC Organization system(s)
- Consistent with the terms of any existing and related data use and/or program agreement,
 - CDC will use information received from the Non-CDC Organization under this IEA for a range of purposes, as laid out in the underlying agreement, which may include, but is not limited to, rapidly assessing patterns of vaccination among the population; identifying pockets of under-vaccination; 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

IEA between HHS/CDC and U.S. Virgin Islands Department of Health

- impact of COVID-19 on the healthcare system and communities
- CDC will use the information only for the specified purposes for which access to the information is granted. In particular, CDC will use COVID-19 vaccine administration data disclosed by the Non-CDC Organization to monitor and assess vaccine administration events during the whole of government response to COVID-19 public health emergency
- Data access by current and future CDC users, including employees, contractors and subcontractors at any tier; and other federally and non-federally funded users managing, engineering, accessing, or utilizing the CDC Systems where exchanged information may be transferred accordingly.
- This IEA is not intended to conflict with or amend the substantive terms of other previously-signed or underlying agreements but only to enable the secure transmission of the data detailed herein this agreement.

FEDERAL AGENCIES AND PROGRAMS SUPPORTING SYSTEMS AND POLICIES FOR EXCHANGE OF INFORMATION:

HHS: The mission of HHS is to enhance the health and well-being of all Americans, by providing for effective health and human services and by fostering sound, sustained advances in the sciences underlying medicine, public health, and social services.

HHS Office of the Chief Information Officer: The Office of the Chief Information Officer (OCIO) serves HHS by leading the development and implementation of enterprise IT across HHS. The office establishes policies and provides support for IT development and operations management, IT security and privacy, IT investment analysis and e-government initiatives.

HHS Office of Information Security: HHS's enterprise-wide information security and privacy program helps protect HHS against potential IT threats and vulnerabilities. The Program ensures compliance with federal mandates and legislation, including the Federal Information Security Management Act and the President's Management Agenda.

CDC: As an Operating Division of HHS and as part of CDC's mission and objectives, CDC increases the health security of our nation. As the nation's health protection agency, CDC saves lives and protects people from health threats. To accomplish the mission, CDC conducts critical science and provides health information that protects our nation against expensive and dangerous health threats and responds when these arise.

CDC Chief Information Officer (CIO): The CDC OCIO provides all associated IT management and planning activities, such as information security, capital planning and investment control, and architecture. OCIO's purpose is to advance use of IT and information resource management to provide maximum value to CDC programs, partners, stakeholders, and customers as they work to improve public health and

IEA between HHS/CDC and U.S. Virgin Islands Department of Health
administration of the agency.

CDC Chief Information Security Officer (CISO)/Chief Privacy Officer (CPO): The CDC CISO and CPO support the CIO in the implementation of the CDC Cybersecurity Program and Privacy Unit Programs. The CDC CISO and CPO direct, coordinate, and evaluate CDC's Cybersecurity and Information Privacy policies.

CDC Information System Security Officer (ISSO): The CDC ISSO is the liaison for Information Systems (IS) within their assigned area of responsibility. ISSOs implement standard IS policies and collaborate across CDC concerning the CIA of information resources.

CDC Cybersecurity Program (CSPO): CDC's CSPO provides 24/7 privacy, security, and threat protection to safeguard the data and information technology essential to CDC's public health mission. The CDC CSPO has developed policies, standards, procedures, and guidelines that ensure the adequate protection of agency information and comply with federal laws and regulations.

CDC Vaccine Task Force (VTF): The CDC VTF coordinates response efforts for COVID-19 vaccine distribution and implementation, vaccine administration, vaccine administration data monitoring and reporting, and vaccine evaluation.

INFORMATION EXCHANGE PROVISIONS:

COVID-19 Data Clearinghouse System: The COVID-19 DCH is a cloud-hosted data repository that receives, deduplicates, and redacts COVID-19 vaccine administration data that are then used to populate the CDC Immunization Data Lake (IZDL) with a limited dataset for analytics. The DCH hosts the application programming interface (API) that enables information exchange between the Non-CDC Organization and CDC.

Data and Processing: DCH serves as a single, centralized data exchange system and concentrator for COVID-19 vaccine administration event reporting. The system accommodates systems with varying capabilities by accepting standardized COVID-19 vaccine administration reports in varying formats (COVID-19 Vaccination Reporting Specification [CVRS: [Technical Standards & Reporting | COVID-19 Vaccination | CDC](#)] and HL7 VXU Z22: [IIS | Health Level 7 Implementation Guidance | HL7 | Vaccines | CDC](#)). DCH de-duplicates and redacts COVID-19 vaccine administration records received from jurisdictions, federal partners, and pharmacies. DCH then transfers the data to the CDC IZDL where it is processed, derivatized, and exported to CDC COVID Data Tracker (publicly available reports) and HHS Tiberius (reports available for state, tribal, local and territorial [STLT] and federal stakeholders).

System Architecture: The DCH is an Oracle Cloud Infrastructure (OCI) repository provided and managed by HHS that, as a functional tool, provides a secure space

IEA between HHS/CDC and U.S. Virgin Islands Department of Health

for a jurisdiction to upload and transiently store COVID-19 vaccine administration data collected from vaccination provider organizations via electronic health records (EHR) and from pharmacy systems. The DCH is hosted within the HHS shared General Support System (GSS) platform that resides in the Oracle Government Cloud (OC2) environment. This HHS tenancy is shared by CDC and HHS applications and is FedRAMP compliant.

Information Exchange Security Framework: All API communication with the DCH is facilitated via Web services over the Internet. The DCH conveys information, using mutual Transport Layer Security (mTLS), version 1.2 for data encryption, authentication, and message integrity. Mutual TLS guarantees the identity of the server to the client as well as the client to the server and provides a two-way encrypted channel between the server and client. DCH uses Public Key Infrastructure (PKI) to authenticate clients that present valid certificates signed by a trusted certificate authority. To protect the confidentiality of data transmitted from one system to another system, messages are encrypted, using the Hypertext Transfer Protocol Secure (HTTPS) protocol. Mutual TLS with client authentication can detect the following web service threats: message alteration, loss of confidentiality, falsified messages, man in the middle, principal spoofing, forged claims, and replay of message parts.

Information Exchange API: All API transactions submitted by the Non-CDC Organization will be evaluated by the DCH system security modules to determine whether the requesting Non-CDC Organization can be authenticated to open a secure connection. If authenticated, the API request will be evaluated to determine whether the Non-CDC Organization is authorized by CDC to upload or export data from the system. The Non-CDC Organization API request will be processed by the DCH system after successful two-factor authentication and confirmation of authorization to upload and/or export data.

Information to be Exchanged: Immunization and vaccine administration data as specified within any previously executed agreement related to Non-CDC Organization, which include but are not limited to: Data Use and Sharing Agreement to Support the United States Government's COVID-19 Emergency Response Jurisdiction Immunization and Vaccine Administration Data Agreement (Jurisdiction DUA), Federal Memorandum of Agreement for COVID-19 Vaccine Distribution Program (Federal MOA) or COVID-19 Vaccination Program Provider Agreement for Pharmacies (Pharmacy Provider Agreement).

Authority to Exchange Information: By exchanging information with the CDC DCH system, the Non-CDC Organization agrees to be bound by this IEA and use the CDC DCH system in compliance with this IEA.

The authority for this IEA is based on, but not limited to, the following, if and to the extent applicable:

IEA between HHS/CDC and U.S. Virgin Islands Department of Health

- Federal Information Security Modernization Act of 2014 (FISMA);
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Systems*;
- 18 U.S.C. § 641 Criminal Code: Public Money, Property or Records;
- 18 U.S.C. § 1905 Criminal Code: Disclosure of Confidential Information;
- Privacy Act of 1974, 5 U.S.C. § 552a;
- Health Insurance Portability and Accountability Act (HIPAA) of 1996, P.L. 104-191;
- 45 C.F.R. § 155.260 Privacy and Security of Personally Identifiable Information;
- 45 C.F.R. § 155.280 Oversight and Monitoring of Privacy and Security Requirements; and
- Patient Protection and Affordable Care Act of 2010.

This IEA is also in compliance with HHS policies ([Cybersecurity | HHS.gov](https://www.hhs.gov/cybersecurity)).

DOCUMENT SUBMISSION: Prior to signing this IEA, the Non-CDC Organization will complete and submit to CDC a DCH API access form (included in your onboarding email) and, as appropriate, will work with CDC to execute this IEA as an addendum to its currently executed Jurisdiction DUA, Federal MOA or Pharmacy Provider Agreement. CDC will provide the Non-CDC Organization digital copies of the DCH API specification, DCH API User Guide, and associated help references.

TRANSFER OF DATA: Non-CDC Organization will provide the information to CDC under this IEA using the following information exchange method: ad hoc electronic/digital data and/or file transfers via secure web service transport to CDC's DCH system API as approved by HHS and CDC.

SECURITY PROCEDURES:

Security Level: Both CDC and the Non-CDC Organization shall maintain a level of IT security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of the information contained on the system.

Federal and Local Policy and Standards Compliance: CDC will ensure compliance of the DCH with FISMA and other federal IT and data security policies such as the latest Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53) and Risk Management Framework (NIST SP 800-37).

Identification and Authentication: DCH User Access under this IEA is determined by the CDC DCH Business Steward. The access to DCH is managed by a least privilege model control and is controlled by multi-factor authentication.

Logical Access Controls: DCH user accounts are established by CDC FTE

IEA between HHS/CDC and U.S. Virgin Islands Department of Health

administrators. DCH user accounts are bound to the corresponding Non-CDC Organization according to user access request forms completed by both parties prior to account creation by CDC system administrators. Non-CDC Organization users only have access to data submitted by that specific Non-CDC Organization. Logical access controls (credentials, validation, authorization, and accountability) are embedded in the application portal and system infrastructure.

Physical and Environmental Security: Physical and environmental controls are maintained at the cloud provider information technology facilities. In order to comply with FISMA high system security requirements, only US citizens are permitted to provide support for the cloud-hosted environment. The technical and physical controls are inherited from the cloud provider's FedRAMP HIGH data center, FedRAMP control set, and are inclusive of the cloud provider's FedRAMP platform plugins. The cloud provider leverages Federal Information Processing Standards (FIPS) approved encryption technology within the platform both at the disk and attribute level. Authentication utilizes 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. Data center physical security begins at the Perimeter Layer. This layer includes several security features depending on the location, such as security guards, fencing, security feeds, intrusion detection technology, and other security measures.

Firewall, Intrusion Detection Systems, and Encryption: Intrusion detection systems are in place at gateways and throughout the HHS and CDC networks and tenancies. Suspicious activity is reviewed and determined recommendations are formulated and assigned to the system administrators. FIPS 140-2 validated encryption is required for transmission of sensitive information. CDC's Network Security Operations Center monitors the CDC network 24 hours a day, 7 days per week.

NON-CDC ENTITIES (CONTRACTOR/AGENT) RESPONSIBILITIES: In furtherance of the operational and technical purposes identified in this IEA and consistent with applicable federal laws, CDC will limit access to the information obtained from Non-CDC Organization to only those authorized CDC employees, contractors, and agents who need such information to perform official duties. In addition, CDC will comply with the limitations on the use, duplication, and redisclosure of Non-CDC Organization information set forth in other agreements related to sharing of COVID-19 vaccine administration data such as any fully executed jurisdiction data use agreements, federal memorandums of agreement, or pharmacy provider agreements with respect to its contractors and agents.

1. CDC will ensure that its employees, contractors, and agents:
 - a. Properly safeguard COVID-19 vaccine administration data furnished by the Non-CDC Organization under this IEA from loss, theft, or inadvertent disclosure;
 - b. Understand that they are responsible for any COVID-19 vaccine administration data that have been exported from any system

IEA between HHS/CDC and U.S. Virgin Islands Department of Health

- involved in reporting of COVID-19 vaccine administration data at all times, regardless of whether or not the CDC employee, contractor, or agent is at their regular duty station;
- c. Ensure that laptops, portable storage devices, and any other electronic devices or media containing COVID-19 vaccine administration data are protected as specified by CDC (e.g., encrypted); and
 - d. Send emails or otherwise transmit COVID-19 vaccine administration data only if protected as specified by CDC (e.g., encrypted).
2. If an employee of CDC or an employee of CDC's contractor or agent becomes aware of a suspected or actual loss or breach of COVID-19 vaccine administration data, the CDC employee or contractor/agent employee must notify the CDC Cybersecurity Incident Response Team (CSIRT), first by phone to the CDC IT Incident Response 24 x 7 Emergency Number (1-866-655-2245) and then with a follow-up email to csirt@cdc.gov, within 1 hour of discovering the incident.
 3. CDC will report the information loss or breach of data in accordance with HHS and CDC policies and procedures. CDC CSIRT notifies the CDC Senior Official for Privacy (SOP), first by phone and then with a follow-up email, with a summary of the incident, including as much specific information on the data that have been stolen/lost as is available. If the CDC SOP determines that a personally identifiable information (PII) breach has occurred, the CDC CSIRT notifies the HHS Computer Security Incident Response Center (HHS CSIRC), first by phone to 1-866-646-7514, then by a follow-up email to csirc@hhs.gov, including as much specific information on the data that has been stolen/lost as is available. The CDC SOP notifies the CDC CISO. The CDC CISO notifies the CDC CIO. HHS CSIRC replies to the email summary from CDC CSIRT, acknowledging the receipt of the incident notification and assigning an incident ticket number. HHS Privacy Incident Response Team and CDC breach response standard operating procedures begin including an assessment of the impact of the breach and its associated risk level.
 4. If the CDC experiences a loss or breach of data, it will provide notice to individuals whose data has been lost or breached in accordance with the CDC Standard for Responding to Breaches of Personally Identifiable Information (PII) and the HHS Information Sharing Environment (ISE) Privacy Policy (2013-0002). Consistent with applicable law, CDC will bear any costs associated with the notice or any mitigation.

POINTS OF CONTACT:

IEA between HHS/CDC and U.S. Virgin Islands Department of Health

Agreement Issues: National Center for Immunization and Respiratory Diseases (NCIRD) Information System Security Officer (ISSO) can be reached at RDuff@cdc.gov.

To report System Security Incidents: CDC's CSIRT: 1-866-655-2245, and csirt@cdc.gov; HHS CSIRC: 1-866-646-7514 and follow-up email to csirc@hhs.gov.

Information Exchange, System and Technical Issues: VTF DCH technical support team can be reached at dchinfo@cdc.gov.

Program or Policy Issues: The NCIRD Immunization Information Systems Services Branch (IISB) IIS Info team can be reached at IISinfo@cdc.gov

DURATION: The effective date of this IEA is the 25th day of February, 2022. This IEA will remain in effect for 1 year commencing from the date of the final signature or shall last for the duration of the national emergency, whichever is longer. Upon conclusion of the one-year period, Non-CDC Organizations will revert to submitting COVID-19 administration data using the non-API method.

CERTIFICATION AND PROGRAM CHANGES: At least 30 days before the expiration of this IEA, the Non-CDC Organization will certify in writing to CDC that: (1) it is in compliance with the terms and conditions of this IEA; and (2) the information exchange processes under this IEA have been and will continue to be conducted without change. If there are substantive changes in any of the programs or information exchange processes listed in this IEA, the parties will modify the IEA accordingly.

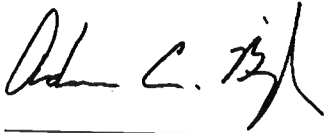
MODIFICATION: Modifications to this IEA must be submitted in writing to the NCIRD Information System Security Officer (ISSO) and agreed to by all parties.

TERMINATION: The parties may terminate this IEA at any time upon mutual written consent with the NCIRD ISSO. Termination of this agreement will result in the Non-CDC Organization losing its ability to exchange information with the DCH via ad hoc electronic exchange. All DCH API access will be revoked when this agreement is terminated. In addition, either party may unilaterally terminate this IEA upon 30 days advance written notice to the other party. Such unilateral termination will be effective 30 days after the date of the notice or at a later date specified in the notice. Non-CDC Organization may immediately suspend the information exchange under this IEA or terminate this IEA if Non-CDC Organization, in its sole discretion, determines that the CDC (including its employees, contractors, and agents) has: (1) made an unauthorized use or disclosure of Non-CDC Organization-supplied data or (2) violated or failed to follow the terms and conditions of this IEA or the other agreement(s). Any data transmitted to CDC prior to termination shall remain in the custody and control of CDC and its use, protection, storage, and disposition shall be subject to applicable federal law.

IEA between HHS/CDC and U.S. Virgin Islands Department of Health

AUTHORIZED SIGNATURES: The signatories below represent that they have competent authority on behalf of their respective organizations to enter into the obligations in this IEA. Signatories should note that the IEA is not authorized until CDC receives a signed DCH API access form.

Centers for Disease Control and Prevention



(Signature Date)

Adam C. Bjork

Acting Associate Director of Science

12/9/2021

(Signature Date)

WITNESSES: GOVERNMENT OF THE VIRGIN ISLANDS

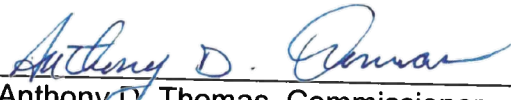
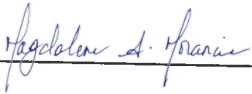
Doreen A Dunlop-Harley



Justa E. Encarnacion, Commissioner
Department of Health

1/29/2022

Date



Anthony D. Thomas, Commissioner
Department of Property and Procurement

2/25/2022

Date

APPROVED AS TO LEGAL SUFFICIENCY

DEPARTMENT OF JUSTICE BY:



Assistant Attorney General

Date 2/25/2022

Agreement No.: G027DOHT22

IEA Version 1.0

DCH IEA Template v1.0