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

GOVERNMENT OF THE U.S. VIRGIN ISLANDS DEPARTMENT OF HEALTH, DIVISION OF IMMUNIZATION

IEA Version 1.1

<Insert IEA Date>

Information Exchange Agreement

PURPOSE: The purpose of this Information Exchange Agreement (IEA) is to establish the terms, conditions, and safeguards under which the Data Reporter, Government of the U.S Virgin Islands Department of Health, Division of Immunization (hereafter referenced as the "Non-CDC Organization") will transmit to and receive from the Centers for Disease Control and Prevention (CDC) certain information, records, or data through a system-to-system information exchange between the CDC VTrckS information system and the Non-CDC Organization system(s).

VTrckS API users include state, tribal, local, and territorial jurisdictions, who will submit information from jurisdiction immunization information systems (IIS). Information, records, or data submitted shall adhere to specifications heretofore agreed upon within any related grant, cooperative, data use or other 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 CDC VTrckS system and the Non-CDC Organization system(s) for the purpose of automating the transfer of information between jurisdiction IISs and VTrckS. Consistent with the terms of any existing and related grant, cooperative, data use and/or other agreement, CDC will use information received from the Non-CDC Organization under this IEA:
  - As a request to provide information (including shipping data, vaccine lists, and run status)
  - As a request to process data (including provider master data, inventory on hand reporting, and transactions such as orders, wastage, returns, and transfers) in VTrckS.
- CDC will use the information for the specified purposes for which access to the information is provided, consistent with those agreements and applicable law.
- 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 should adhere to the HHS IT Systems Rules of Behavior.

- This IEA is not intended to conflict with or amend the substantive terms of other previously-signed or underlying data use agreements but only to enable the secure transmission of the data detailed herein this agreement.

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

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 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.

INFORMATION EXCHANGE PROVISIONS:

VTrckS System:
VTrckS is an application that supports a more efficient vaccine ordering and managing process as part of the Vaccines for Children (VFC) program for publicly-

funded vaccines. VTrckS combines vaccine ordering, budget management and contract management into one application. VTrckS hosts the application programming interface (API) that enables information exchange between the Non-CDC Organization and CDC.

Data and Processing: VTrckS serves as a single, centralized data exchange system and concentrator for vaccine ordering and tracking.

System Architecture: VTrckS is an SAP system managed by CDC, as a functional tool and provides a secure space for jurisdictions to manage the vaccine ordering from vaccination provider organizations via API.

Information Exchange Security Framework: All API communication with VTrckS is facilitated via Web services over the Internet. At this time, VTrckS 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. VTrckS 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 through CDC's Secure Access Management System (SAMS) and evaluated by the VTrckS 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 VTrckS system after successful two-factor authentication and confirmation of authorization to upload and/or export data.

Information to be Exchanged: Vaccine shipping data, vaccine lists, run status, provider master data, inventory on hand reporting, and transactions such as orders, wastage, returns, and transfers.

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

- 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).

DOCUMENT SUBMISSION: After signing this IEA, the Non-CDC Organization will complete and submit to CDC a VTrckS API access form (included in your onboarding email) and, as appropriate, will work with CDC to execute this IEA. CDC will provide the Non-CDC Organization digital copies of the VTrckS API specification, VTrckS 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 VTrckS 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 VTrckS 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: VTrckS User Access under this IEA is determined by the CDC VTrckS Business Steward. The access to VTrckS is managed by a least privilege model control and is controlled by multi-factor authentication.

Logical Access Controls: VTrckS user accounts are established by CDC FTE administrators. VTrckS 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.

Users with system-to-system access IDs will need to be aware of how/where the ID will be used by awardee or vendor staff and when the password should be changed. System IDs are still the responsibility of the person and program to which it has been issued and must be handled with the same care as your regular SAMS ID. All IDs, inclusive of system IDs, will need to be removed within 24 hours of the associated user no longer needing access.

Physical and Environmental Security: Currently, VTrckS is hosted in the CDC on-prem data centers. Physical and environmental controls are maintained at the data center provider information technology facilities either in cloud or on-prem. Once VTrckS transitions to a cloud-based infrastructure, the technical and physical controls will be inherited from the cloud provider's FedRAMP HIGH data center, FedRAMP control set, and inclusive of the cloud provider's FedRAMP platform plugins. The cloud provider will leverage 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.

Security Incidents: In furtherance of the operational and technical purposes identified in this IEA and where consistent with applicable federal laws, CDC will limit access to the information obtained from Non-CDC Organization to only those authorized federal employees, contractors, and agents who need such information to perform official duties.

1. CDC will ensure that its employees, contractors, and agents:
    a. Are aware of the requirement to properly safeguard

data furnished by the Non-CDC Organization under this IEA from loss, theft, or inadvertent disclosure;

b. Ensure that laptops, portable storage devices, and any other electronic devices or media containing data are protected (e.g., encrypted); and

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 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:

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 VTrckS technical support team can be reached at VTrckSinfo@cdc.gov.

Program or Policy Issues: The NCIRD Informatics and Data Analytics Branch (IDAB) IIS Info team can be reached at IISinfo@cdc.gov

DURATION: The effective date of this IEA is _____. This IEA will remain in effect for 1 year commencing from the date of the final signature and will be renewed thereafter automatically on a yearly basis.

CERTIFICATION AND PROGRAM CHANGES: Within 30 days after establishing an API connection, 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 submitted to the NCIRD ISSO. Termination of this agreement will result in the Non-CDC Organization losing its ability to exchange information with the VTrckS via ad hoc electronic exchange. All VTrckS 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.

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.

Arunkumar Srinivasan, PhD
Acting Associate Director of Informatics
Fos2@cdc.gov

_____
(Signature Date)

2/25/2026
Justa E. Encarnacion Date
Commissioner, Dept. of Health

4/28/2026
Lisa M. Alejandro Date
Commissioner, Dept. of Property & Procurement

Steven Warren
Acting CDC Chief Information Officer
Scw0@cdc.gov

_____
(Signature Date)

APPROVED LEGAL SUFFICIENCY
Dept. of Justice by:

Date 04/28/2026