Centers for Disease Control and Prevention
National Syndromic Surveillance Program
Data Sharing and Use Agreement

Purpose: This Agreement ("**Agreement**") between the **Centers for Disease Control and Prevention ("CDC")**, an agency within the Department of Health and Human Services ("HHS"), having its primary offices at 1600 Clifton Road, Atlanta GA 30333 and the **County of Tarrant, Texas ("Jurisdiction"),** through its **Tarrant County Public Health Department ("TCPH")** having its primary offices at 1101 S. Main Street, Fort Worth Texas 76104, establishes the basic terms and conditions concerning contribution of data by Jurisdiction to the National Syndromic Surveillance Program's (NSSP) BioSense Platform and access, sharing, protection and use of the Data Received by the NSSP BioSense Platform that are submitted by the Jurisdiction.

Background: Syndromic surveillance is a process that regularly and systematically uses health, public health, and health-related data in near real-time to make information on the health of a community available to public health officials and government leaders for decision making and enhanced responses to hazardous events and outbreaks.

In response to the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 and the Pandemic and All-Hazards Preparedness Reauthorization Act of 2013, the CDC developed and modified the BioSense Program to establish an integrated system of nationwide public health surveillance for the early detection and prompt assessment of and response to potential bioterrorism-related illness. As of November 2011, the BioSense Program developed a distributed computing environment, which included analytic tools, under state and local advisement. The program has since evolved into the NSSP, which is a collaboration among individuals and organizations from the local, state, and federal levels of public health, including departments of health; other federal agencies, including the Department of Defense (DoD) and the Department of Veterans Affairs (VA). NSSP currently includes a community of practice and a cloud-based syndromic surveillance computing platform (the NSSP BioSense Platform) that hosts data submitted by the Jurisdiction and computing applications that include analytic tools and services.

As part of its role under this Agreement, CDC will provide the cloud-based environment for the NSSP BioSense Platform either directly or by and through a contract with a vendor ("CDC Contractor") for participating Jurisdictions to facilitate receipt, storage, and management of the Jurisdictions' syndromic surveillance data. In addition, either directly or working with a CDC Contractor, CDC: 1) has developed and will operate the NSSP BioSense Platform, including providing role-based access to the Platform; 2) will continue to provide tools and services therein; 3) will assure compliance of the platform and the available tools and services with the Federal Information Security Management Act (FISMA) and other federal data security policies, to the extent they apply; 4) will provide operational support to the participating Jurisdictions and other authorized users of the NSSP BioSense Platform by conducting processing, quality control, aggregation, sharing, and analysis of data submitted to the BioSense Platform; 5) will support the NSSP community of practice; and 6) will conduct national and HHS regional syndromic surveillance and public health emergency response activities. The NSSP BioSense Platform provides participating Jurisdictions with the ability to contribute, access and share data that will support existing and potential expansion of its public health surveillance systems.

Authorities: CDC is authorized by the Public Health Service Act, Sections 301, 317 and 319D (as amended) (42 U.S.C. 241, 247b and 247d-4, as amended) to maintain active surveillance of diseases through epidemiologic and laboratory investigations and data collection, analysis, and distribution and to coordinate with states, locals and other appropriate public health partners with respect to the maintenance and collection of such data.

TCPH is authorized to share the data they submit and store on the BioSense Platform pursuant to this Agreement with the CDC pursuant to the provisions set forth in Chapter 81 of the Texas Health and Safety Code and consistent with the terms of this Agreement. Further, the Parties agree and understand that, to the extent Jurisdiction is a recipient of a grant or cooperative agreement funding activities governed by this Agreement, nothing contained in this Agreement shall be read to conflict with the terms and conditions of that underlying grant or cooperative agreement.

CDC is a "public health authority" as defined at 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"). To the extent Jurisdiction is a covered entity under HIPAA, the Jurisdiction is permitted to disclose Protected Health Information (PHI), as defined by 45 CFR 160.103, to CDC without patient authorization, as a disclosure to a public health authority authorized by 45 CFR §164.512(b).

Definitions: For purposes of this Agreement, the following definitions shall apply:

"NSSP BioSense Platform" means the cloud-based syndromic surveillance computing platform that receives, and processes data submitted to the Platform and hosts analytic tools and services.

"Data Received by the NSSP BioSense Platform" means an organized collection of data submitted or contributed to NSSP by the Jurisdiction, by any Users, or any Data Providers or other entities within the Jurisdiction. Current data definitions and exchange standards are available at https://www.cdc.gov/nssp/technical-pubs-and-standards.html. A 120-day notice will be given, and the community of practice will be engaged prior to requiring compliance with any changes to definitions or standards.

"Data on the NSSP BioSense Platform" means the public health and/or health-related information available to users through the NSSP BioSense Platform, including Data Received by the NSSP BioSense Platform and additional fields derived from submitted data elements.

"Data Provider" means a hospital, health professional, health facility, health information exchange or other source that submits data to the NSSP BioSense Platform either directly to the Platform or indirectly, e.g., through submission to the Jurisdiction or other agent that submits data to the platform.

"Individually Identifiable Information" means information, such as patient name or social security number, that identifies an individual or with respect to which there is a reasonable basis to believe the information can be used to identify an individual.

"Jurisdiction" means the local or state health jurisdiction operating under either statutory or regulatory authority to obtain and use public health and/or health-related data for population health protection.

"NSSP" means the National Syndromic Surveillance Program (formerly known as the BioSense Program), which is a collaboration among public health agencies and partners that supports the use and timely exchange of syndromic surveillance data for improved nationwide all-hazard situational awareness for public health decision making and enhanced responses to hazardous events and outbreaks.

"Party" means State or Local Jurisdiction or CDC; "Parties" means State or Local Jurisdiction and CDC.

"Syndromic surveillance" means regular and systematic uses of health, public health and health-related data, including patient encounter, laboratory, and pharmacy data from healthcare settings such as emergency departments, urgent care, ambulatory care and inpatient settings, in near real-time for improved all-hazard situational awareness, public health decision making and enhanced responses to hazardous events and outbreaks at local, state, regional and national levels of public health.

User" means any authorized user of Data on the NSSP BioSense Platform. Users will be provided role-based access and be required to adhere to rules of behavior when provided access to the Platform. Users will generally be employees, contractors, affiliates and/or other agents of a state, local, territorial or tribal jurisdiction or of HHS and CDC; other federal agencies as part of or in furtherance of their public health authorities or mission (e.g., VA, DOD, the Indian Health Service (IHS)); or other entities with federal legal authority to have access to the Platform or Data on the NSSP BioSense Platform. Contractors or other legal agents or affiliates of the respective federal agencies listed above and granted access as Users will be made aware of any rules or terms associated with access to the NSSP BioSense Platform and will be expected to comply with those to the same extent as federal employees.

Agreement Principles:

1) Jurisdiction agrees to participate in the NSSP by contributing data to the NSSP BioSense Platform and utilizing the Platform in accordance with the terms and conditions herein and any applicable rules of behavior for access to the Platform. Prior to allowing a Data Provider to submit data to the NSSP BioSense Platform (directly or through the Jurisdiction), the Jurisdiction shall work with the Data Provider to ensure that: a) Data Provider shall not take any actions that are inconsistent with this Agreement; b) Data Provider shall not submit data to the NSSP BioSense Platform that it is not authorized to submit; and c) Data Provider submission of data will comply with applicable federal, state, and local laws and requirements. The Jurisdiction shall define and finalize the exact nature and form of any necessary agreement with the Data Provider.

2) The Jurisdiction represents and warrants that it has authority to enter into this Agreement and to submit the Data Received by the NSSP BioSense Platform to the NSSP BioSense Platform as contemplated by this Agreement and for its intended uses (as described below in section 3), and that doing so will not violate any law or regulation applicable to the Jurisdiction in which it resides or any agreement or arrangement to which the Jurisdiction is a party.

3) Jurisdiction acknowledges and agrees that the Data Received by the NSSP BioSense Platform may be used and/or disclosed for the following purposes:

    a. Operational Support

As a part of accessing and using the NSSP BioSense Platform, tools and services, and for purposes of providing operational support for NSSP as described below, Jurisdiction understands and agrees that designated staff in CDC (which includes more specifically CDC's Division of Health Informatics and Surveillance (DHIS)) and, as applicable, the CDC Contractor will have routine access to the secure individual patient record-level Data Received by the NSSP BioSense Platform from the Jurisdiction and/or its Data Providers. The operational support is intended to support the Jurisdiction so that it can best utilize the data, analytic tools, and other functions of the NSSP BioSense Platform. CDC agrees to regularly communicate information on operational activities to the Jurisdiction.

Operational support includes processing data, conducting data quality control activities, creating surveillance categorization algorithms, assuring proper aggregation of data, establishing and supporting mechanisms that allow Jurisdictions to set permissions and share data, and ensuring proper operation and functioning of permission tools and data analysis and visualization tools, as further set out below:

- Data processing includes such activities as de-encrypting electronic health record messages submitted by data providers, creating up-to-date individual patient visit records from multiple electronic record messages submitted for the same patient visit, and categorizing records based on submitted demographic, clinical data, and facility data;
- Quality control includes assessing messages and records for accuracy, completeness, consistency, timeliness, and validity and developing and implementing data quality control processes;
- Creating and refining syndromic surveillance categorization algorithms means using chief complaint, diagnoses, and other clinical data to create syndromes, sub-syndromes and other event codes;
- Assuring proper data aggregation includes grouping individual patient records into local, state, regional and national aggregate counts to support use of dashboards and analytic tools;
- Data sharing and permissions means administering permissions for national level users and Jurisdictions' administrators, and ensuring that permissions tools and granted access control is working properly; and
- Data analysis and visualization means assuring that tools and dashboards, such as ESSENCE, R Studio, and SAS, that provide data reporting, querying, analysis, and visualization function properly.

b. Syndromic Surveillance at the National and U.S. Department of Health and Human Services (HHS) Regional Levels

As a part of accessing and using the NSSP BioSense Platform, tools, and services, for purposes of syndromic surveillance at national and HHS regional levels, Jurisdiction understands and agrees that Users will have routine access through dashboards and analytic tools to views of Data Received by the NSSP BioSense Platform from the Jurisdiction aggregated to HHS regional and national levels. In addition, in order to evaluate clusters or patterns that indicate an event of potential public health concern, Users will have limited views of selected individual patient record level data elements (HHS region, age-group, gender, syndrome, sub-syndrome, date without time, patient class and disposition). A 30-day notice will be given, and the community of practice will be engaged prior to changes being made to this list in future. Such views will exclude data elements that identify hospitals, zip codes,

counties, states, and individually identifiable information such as birthdate. These surveillance activities include routine analysis of regional and national level trends, evaluation of multi-regional events, and special surveillance during events of public health interest at national and regional levels.

c. National and regional syndromic surveillance products
As a part of accessing and using the NSSP BioSense Platform, tools and services, Jurisdiction understands and agrees that CDC will develop products focused on national and regional level syndromic surveillance. This includes, but is not limited to, the development of publications, public use datasets, publicly accessible dashboards, and publicly available summary data tables. CDC may invite collaborators and co-authors from Jurisdictions to participate in the development of such products. CDC may also share products with Jurisdictions for review and comment in advance of release/publication. If shared, Jurisdiction agrees to perform the review in a timely manner for publication and/or dissemination of the product. Such final products will be shared with the NSSP community of practice, other health agencies or partners and published on the NSSP web site or in scientific or health professional journals. Except as may be required by federal law or as otherwise provided for in this Agreement, such products will not identify jurisdictions below the HHS regional level and will not include Individually Identifiable Information.

d. Collaborative Projects with CDC
As a part of accessing and using the NSSP BioSense Platform, tools and services, Jurisdiction understands and agrees that its Jurisdiction NSSP data steward will be responsible for administering access to Jurisdiction Data on the NSSP Biosense Platform for collaborative projects. If the Jurisdiction elects to participate in a collaborative project with CDC, and potentially other Users of Data Received by the NSSP BioSense Platform, the steward will use web-based NSSP BioSense Platform tools under the steward's control to provide specific Users with access for a specified time period to specific sets of the Jurisdiction's data at a level consistent with the proposed project. Collaborative projects may include: a) coordinating syndromic surveillance at the national and regional levels with surveillance data at the Jurisdiction level, b) evaluating unusual clusters or patterns that indicate an event of potential public health concern, c) allowing CDC or other Jurisdictions to provide technical assistance, d) evaluating the NSSP program or the NSSP BioSense Platform, and e) developing improved methods for conducting syndromic surveillance. Examples of evaluation and methods development projects include examining different methods for analyzing and detecting a disease outbreak or developing or revising syndrome definitions. During the process of initiating and conducting collaborative projects, CDC and Jurisdiction collaborators will coordinate on the publishing of products based on the projects. Such final products may be shared with the NSSP community of practice, other health agencies or partners and may be published on the NSSP web site, or in scientific or health professional journals. Such products will not contain any Individually Identifiable Information. In addition, data suppression rules will be used to prevent possible identification. This may include strategies such as publication of tables combining characteristics that could be used to identify an individual, e.g., age, sex, race, ethnicity, and geographic location.

e. Public Health Emergency Response Activities
The Parties acknowledge that in the event of a national emergency declared under applicable laws, in a public health emergency (PHE) or an event significantly likely to

become a PHE, as provided in 42 U.S.C. §247d, in response to an emergency declared under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. §5121 et seq., or where the CDC Director has activated the CDC Emergency Operations Centers, certain data in the custody and control of CDC may be necessary to respond to the event. As part of its response to that event, CDC may access and use the Data Received by the NSSP BioSense Platform, including secure individual patient record-level data, for the purpose of monitoring and responding to the PHE. Such access and use by CDC will be consistent with CDC's authorities under applicable federal law, including the Privacy Act of 1974 and the Freedom of Information Act. CDC's use and sharing of such data will be on a need-to-know basis, will be a minimum amount necessary to support a coordinated response to the event, and will protect individual privacy and confidential business or financial information to the fullest extent allowed by federal law. CDC further agrees that it will notify Jurisdiction of the need to use this data as soon as practicable prior to its use for this purpose and, where practicable and appropriate, will work collaboratively with Jurisdiction throughout the response to ensure appropriate coordination and access to developed analyses and reports.

Generally, CDC's use of such data will be to inform situational awareness, predictive modeling, and strategic, tactical, and policy decision making; to help track the spread and intensity of the illness or condition and identify areas that are highly impacted by it; to determine where federal resources (e.g., technical, financial, or in-kind assistance) should be routed to jurisdictions in need; to understand the spectrum of illness, disease burden, risk factors for severe disease, and outcomes; and to understand the impact of the illness or condition on healthcare systems and communities. This includes: analyzing and visualizing the data to improve the detection of, monitoring of, and response to the illness or condition; consistent with federal law, sharing the minimum necessary data and analyses thereof with appropriate officials in federal, state, local, tribal, and territorial governmental health agencies or other agencies and entities conducting their public health and emergency response responsibilities, including CDC contractors or legal agents; developing analytic methods to identify immediate public health events or concerns at the federal, state, local, tribal and territorial level that warrant further public health investigation or immediate public health intervention actions; and enabling Users, including public health and emergency response officials, to query the data within secure CDC and HHS data platforms as may be necessary to carry out critical public health functions for use and release as may be needed for the response.

4) Confidentiality of data submitted
Minimum required data elements will be submitted to the NSSP BioSense Platform by Data Provider or Jurisdiction. Jurisdiction agrees and acknowledges that the data submitted to NSSP BioSense Platform may include certain hospital, physician, or other health care provider identifiers and may contain individual patient record level data elements (e.g., HHS region, age-group, gender, syndrome, sub-syndrome, date, patient class and disposition). Jurisdiction agrees that it is the responsibility of the Jurisdiction to obtain any permissions required in order to submit such data to the NSSP BioSense Platform.

5) Open Records Laws

Jurisdiction acknowledges and understands that the data it submits to the NSSP BioSense Platform, including data accessed by CDC, other jurisdictions and users may be subject to state and federal (e.g., Freedom of Information Act (FOIA)) open records laws. To the extent data submitted to the NSSP BioSense Platform may be subject to the applicable open records laws for the state of origin for Jurisdiction, Jurisdiction is responsible for compliance with such law. Jurisdiction acknowledges that CDC, as a federal agency, must ensure compliance with FOIA with respect to data in its custody and control at the time of the request.

6) Asset Protection:
The Parties agree that the data provided under this Agreement and in the custody and control of the CDC is subject to applicable federal laws. To that end, CDC will protect the privacy and confidentiality of any Individually Identifiable Information that may be contained in the Data Received by the NSSP BioSense Platform and for which access is provided under this Agreement consistent with the Privacy Act of 1974, to the extent applicable, applicable standards promulgated pursuant to HIPAA, and all applicable laws, regulations, and policies. In furtherance of activities set forth in this Agreement and consistent with applicable laws, policies, and procedures to ensure the privacy and confidentiality of such data, CDC may provide data access to appropriate employees, contractors, and other Users. CDC Users of data, including contractors authorized access to the Platform, are expected to comply with applicable federal laws and CDC policies with respect to the use, safeguarding and maintenance of such data and will be made aware of the principles set forth in this Agreement. CDC will not attempt to identify records contained in the data submitted under this Agreement or link these data with data from other Jurisdictions for identification purposes, except as may be provided for in this Agreement. CDC will coordinate with the Jurisdiction and Data Provider to respond to any data requests from individuals who are not authorized users, e.g., FOIA requests. Every effort will be made to protect the privacy and confidentiality of Individually Identifiable Information, but CDC cannot assure that Individually Identifiable Information will not be released in all cases. However, CDC will work collaboratively with the Jurisdiction and Data Provider to ensure that all Parties are aware of and, when possible, a part of deciding what Data Received by the NSSP BioSense Platform, if any, will be released.

The Jurisdiction is responsible for limiting the submission of Individually Identifiable Information, encrypting data prior to submission to the NSSP BioSense Platform and for maintaining the security of any encryption techniques used. Creation of the data submitted to the NSSP BioSense Platform and encryptions will be done in compliance with applicable federal and state law and corresponding regulations. The Jurisdiction should work with the Data Provider to ensure that data are submitted in accordance with current data definitions and exchange standards, available at https://www.cdc.gov/nssp/technical-pubs-and-standards.html.

Without limitation to any other provision of this Agreement, CDC agrees not to disclose, display or otherwise make available any Jurisdiction proprietary information to any third party, in any form, except to public health officials in connection with the purposes established herein or as otherwise required under FOIA or other federal law. The Jurisdiction will clearly indicate in writing any information that it considers to be company proprietary, trade secret or confidential business information.

CDC further employs the following measures in order to ensure strong privacy and security controls to protect the Data on the NSSP BioSense Platform:

a. Secure NSSP BioSense Platform: The Platform is hosted by a Federal Risk and Authorization Management Program (FedRAMP) approved provider. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. The NSSP BioSense Platform meets CDC certification and accreditation standards to assure that it is Federal Information Security Modernization Act (FISMA) compliant and is supported by the timely maintenance of security updates, anti-virus updates, malware updates, and hardware/application vulnerability reviews and remediation. Servers are housed in access-controlled, physically secured locations. These locations prevent the unauthorized physical and logical access of servers and network devices, ensuring that only those authorized to maintain the servers are allowed access to them.

b. Authentication: All non-federal NSSP BioSense Platform Users use a one factor authentication (password) to access the Platform services and data. In addition, CDC and CDC contractor Users are also required to provide a second level of authentication: when the user's credentials are confirmed, the service requested is checked to verify that the User has permission to access the internal application servers.

c. Need-to-Know Access: Access controls within the NSSP BioSense Platform ensure that data submitted to the Platform are not only restricted to authorized Users, but also that those Users are restricted to the data they are authorized to access as provided in this agreement. Consistent with CDC's policies, unauthorized access or breaches will be reported to CDC Information Systems Security Officers (ISSO) immediately. Consistent with CDC's policies and procedures, CDC will keep relevant jurisdictions informed of any such rare event.

d. Data Encryption: Data in transit are encrypted from the transmitting system to the NSSP BioSense Platform, and they are encrypted for storage within the data transformation and warehousing process. This encryption is managed by CDC and its contractor and is consistent with Federal requirements.

7) Secure Access
The NSSP BioSense Platform's Access & Management Center (AMC) allows a Jurisdiction's NSSP data steward (site administrator) to perform administrative functions, including controlling access to data, creating and managing User accounts, changing passwords, creating data sharing rules and allowing data sharing. Jurisdictions are responsible for managing Users, access to their site's data, and access to NSSP BioSense Platform tools using the AMC. All Users must acknowledge agreement to the "BioSense Platform Code of Conduct" when first accessing User accounts and at the time of password change.

8) Ownership of Data
The data source shall retain ownership of the data it contributes to the NSSP BioSense Platform. Additional terms regarding access and control of these data, asset protection and applicable and governing laws are defined in separate clauses (including but not limited to 3, 5, 6, and 7) of this Agreement.

9) Data Disposition:
Data Received by the NSSP BioSense Platform, including data that have been used for National and Regional Surveillance and shared with CDC for Collaborative Projects under this Agreement, will be archived, stored, protected, or disposed of in accordance with relevant federal records requirements.

10) Severability

If any term or condition of this Agreement is held invalid, such invalidity shall not affect the validity of the other terms or conditions of this Agreement, provided, however, that the remaining terms and conditions can still fairly be given effect.

11) Funding:

This Agreement is not an obligation or a commitment of funds, or a basis for a transfer of funds, and 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 its availability of funds and resources pursuant to applicable laws, regulations, and policies. Further, the Parties agree and understand that, to the extent Jurisdiction is a recipient of a grant or cooperative agreement funding activities governed by this Agreement, nothing contained in this Agreement shall be read to conflict with the terms and conditions of that underlying grant or cooperative agreement.

12) Settlement of Disputes**:**

Disagreements between the parties arising under or relating to this Agreement will be resolved by consultation between the parties and referral of the dispute to appropriate management officials of the parties whenever possible.

13) Applicable Laws:

U.S. federal law shall govern the construction, interpretation, and performance of this Agreement.

14) Notices:

Any notice, demand or other communication required or permitted to be given under the Agreement shall be in writing and shall be deemed delivered to a Party: (i) when delivered by hand or nationally recognized overnight courier; or (ii) six (6) days after the date of mailing if mailed by United States certified mail, return receipt requested postage prepaid, in each case to the address of such Party set above.

15) Term of Agreement, Amendment, and Termination:

a. Except as otherwise expressly provided herein, this Agreement may be amended only by the mutual written consent of the authorized representatives for each party.

b. This Agreement may otherwise be terminated with ninety (90) days advance notice upon written notice by either party. Upon termination of this agreement, to the extent consistent with federal law, a jurisdiction will have the option to remove its data from NSSP BioSense Platform by requesting appropriate forms from NSSP help desk and completing an established process for data removal.

COUNTY OF TARRANT
STATE OF TEXAS

By: _____

Name: Tim O'Hare

Title: County Judge

Date: _____

Centers for Disease Control and Prevention
U.S. Department of Health and Human Services

By: _____

Name: Jennifer Adjemian, PhD

Title: Division Director
Division of Health Informatics and Surveillance
Office of Public Health Data, Surveillance and Technology, Centers for Disease Control and Prevention

Date:_____

09152023

APPROVED AS TO FORM:

Kimberly Colliot Wesley
Criminal District Attorney's Office*

*By law, the Criminal District Attorney's Office may only approve contracts for its clients. We reviewed this document as to form from our client's legal perspective. Other parties may not rely on this approval. Instead those parties should seek contract review from independent counsel.