10-3-2021

STATE OF CONNECTICUT
DATA SHARING AGREEMENT
Between

_____

_____

_____

And

_____ ("Data Integration Hub")

WHEREAS, this Data Sharing Agreement ("DSA") is by and between the _____ ("Data Integration Hub"), and _____, and _____ ("Participating Agency" or "Participating Agencies"), and _____ ("Data Recipient") together referred to as "Party" or "Parties," and is effective as of the last date of the signature shown below ("Effective Date");

WHEREAS, Data Integration Hub is operating as the centralized data matching service for Participating Agencies (as defined in the Enterprise Memorandum of Understanding and its Appendices ("E-MOU"), which is attached hereto and incorporated herein);

WHEREAS, Participating Agencies wish to share data with the Data Integration Hub for data matching services, in accordance with the terms and conditions of this DSA and approved under the terms and conditions of the E-MOU, and share the Resultant Data with the Data Recipient;

WHEREAS, the Department of Labor ("DOL") has access to data matching software which can be utilized to match and link longitudinal data from state agencies from state agencies and other organizations for the purpose of facilitating data requests;

WHEREAS, the Parties wish to participate in the P20 WIN Project entitled: _____.

NOW, THEREFORE, the Parties, in consideration of mutual promise and obligations set forth here, the sufficiency of which is hereby acknowledged, and intending to be legally bound, agree as follows:

I. DEFINITIONS

Definitions in the E-MOU are applicable herein. If there is a definition in this document of a word or a term that is also defined in the E-MOU, the definition in the Data Sharing Agreement shall apply and prevail:

Anonymized Data (**"Anonymized Data"**) refers to Data that cannot be linked back to an individual and, as such, are not useful for monitoring the progress and performance of individuals; however, such Data can be used for other research or training purposes.

Data Recipient (**"Data Recipient"**) means any person, entity or organization that is a party to an approved Data Sharing Agreement that receives Data sets from Participating Agencies for legitimate state purposes.

De-identification of Data or **De-Identified Data** ("**De-identification of Data**" or "**De-identified Data**") refers to the process of removing or obscuring any PII in a way that minimizes the risk of unintended disclosure of the identity of individuals and information about them. Specific steps and methods used to de-identify information may vary depending on the circumstances, but should be appropriate to protect the confidentiality of the individuals. While it may not be possible to remove the disclosure risk completely, de-identification is considered successful when there is no reasonable basis to believe that the remaining information provided through a single release or through a combination of multiple releases can be used to identify an individual. De-identified Data is the result of the De-identification of Data.

Resultant Data ("Resultant Data") is the Data provided by the Participating Agencies and the Data Integration Hub to the Data Recipient pursuant to a Data Sharing Agreement signed by two (2) or more Participating Agencies. Resultant Data includes original Data files received for analysis from Participating Agencies and a crosswalk of unique generic identifiers used to connect the analyzed data together. It also includes the working documents and derivative tables that are created from this analyzed data before the documents and tables have been reviewed according to the DSA and subsequently approved as appropriately aggregated for access to Users beyond those names in the DSA.

II. RESPONSIBILITIES OF PARTICIPATING AGENCIES

A. Specific Duties of Participating Agencies When Transmitting Data. Whenever a Participating Agency Transmits data to the Data Integration Hub, the Participating Agency shall do so in compliance with applicable federal and state law and the E-MOU. Furthermore, the Participating Agency will abide by all of the specific requirements contained in the Data Sharing Request Form, which is attached and incorporated as Exhibit A, including but not limited to the confidentiality and privacy requirements contained in applicable law.

B. Compliance with E-MOU. Except to the extent prohibited by applicable federal and state law, Participating Agencies shall comply fully with all provisions of the E-MOU.

C. Users. A Participating Agency shall require that all of its Users perform Data Transmittal only in accordance with the terms and conditions of the E-MOU and the applicable Specifications, including without limitation those governing the authorization, use, confidentiality, privacy, and security of data.

D. Agreements with Users. A Participating Agency shall have established written documentation that each of its Users shall, at a minimum: (i) comply with all federal and state laws; (ii) reasonably cooperate with the Operating Group and Data Integration Hub on issues related to the E-MOU; (iii) transmit data only for a permitted purpose; (iv) use and disclose data received from another Participating Agency or User in accordance with the terms and conditions of this DSA; (v) as soon as learning that a Breach or potential Breach has occurred, report such breach to the Operating Group for the Data Governing Board so that the Data Governing Board can proceed according to the terms and conditions of the E-MOU; (vi) refrain from disclosing to any other person any passwords or other security measures issued to the User for the Data Sharing process; and (vii) cooperate with any external audits. Each User shall sign a User Acknowledgement Form, either one developed by the Participating Agency or the Data Integration Hub or the one attached and incorporated herein as Exhibit B. Notwithstanding the foregoing, for Users who are employed by a Participating Agency or who have agreements with a Participating Agency which became effective prior to the Effective Date, compliance with this Section may be satisfied through written policies and procedures that address items (i) through (vi) of this Section so long as the Participating Agency can document that there is a written requirement that the User must comply with the policies and procedures.

E. Agreements with Vendors. To the extent that a Participating Agency uses vendors, in connection with the Participating Agency's Transmittal of Data, the Participating Agency affirms that it has established agreements with each of its vendors that require the vendor to, at a minimum: (i) comply with applicable federal and state law; (ii) protect the privacy and security of any data to which it has access; (iii) as soon as reasonably practicable after determining that a breach occurred, report such breach to the Participating Agency; (iv) not re-disclose information without the written consent of the Participating Agency; (v) agree to the same restrictions on the access, use, and disclosure of Data as contained herein; (vi) reasonably cooperate with the other Participating Agencies to the E-MOU on issues related to the E-MOU; (vii) sign a form that meets the requirements of Exhibit B; and (viii) cooperate with any external audits.

F. Compliance with Laws. The Participating Agencies shall fully comply with all applicable federal and state laws.

G. Disclaimers.

1. Reliance on a System. Each Participating Agency acknowledges and agrees that (i) the data provided to the Data Integration Hub is drawn from numerous sources; (ii) the data is specific to the point in time when drawn, and (iii) it can only confirm that, at the time of the data Transmittal, the data is an accurate representation of data contained in, or available

through, the Data Integration Hub. Nothing in the DSA shall be deemed to impose responsibility or liability on a Participating Agency related to the clinical accuracy, content or completeness of any data provided pursuant to the Data Integration Hub. Furthermore, Data Recipient may not rely upon the availability of a particular Participating Agency's data.

2. Carrier Lines. The Participating Agency acknowledges that the Transmittal of data between Participating Agencies, the Data Recipient and the Data Integration Hub is to be provided over various facilities and communications lines, and data shall be transmitted over local exchange and Internet backbone carrier lines and through routers, switches, and other devices (collectively, "carrier lines") owned, maintained, and serviced by third-party carriers, utilities, and Internet service providers, all of which may be beyond the Participating Agency's control. Provided the Participating Agency uses reasonable security measures, no less stringent than those directives, instructions, and specifications contained in the E-MOU, its Specifications, and applicable federal and state law, the Participating Agency assumes no liability for or relating to the integrity, privacy, security, confidentiality, or use of any data while it is transmitted over those carrier lines, which are beyond Participating Agency's control, or any delay, failure, interruption, interception, loss, Transmittal, or corruption of any data or other information attributable to Transmittal over those carrier lines which are beyond Participating Agency's control. The use of the carrier lines is solely at the Participating Agency's risk and is subject to all applicable federal and state law. If a Breach occurs and it is determined that it happened because of a carrier issue, the Participating Agency responsible for the Transmittal of Data is the responsible party for the Breach notification. However, data should be encrypted using current industry standard algorithms agreed on by the parties involved before transmission occurs.
3. Collecting Data. Each Participating Agency has collected the confidential data from Individuals. Accordingly, the Participating Agency is solely responsible for ensuring that all legal requirements have been met to collect data on Individuals whose confidential data are being provided to the Data Integration Hub and the Data Recipient.
4. Data Accuracy. Each Participating Agency will identify and document for the Data Recipient any known limitations or data accuracy issues that have potential to impact the Project described in Exhibit A.

H. All Participating Agencies and the Data Integration Hub agree that Data will be encrypted at rest and in motion, and any and all backups will be encrypted.

III. RESPONSIBILITIES OF DATA INTEGRATION HUB

A. For any data sharing, the Data Integration Hub agrees to store and access all data obtained from the providing Participating Agency on secure computers and in secure files to which access is restricted to authorized persons only and in an area that is physically safe from unauthorized persons at all times. All personnel authorized to access data shall be fully trained and advised of the confidential nature of the information and the safeguards required protecting the information and have followed the procedures in section II.D (Agreements with Users).

B. The Data Integration Hub agrees to monitor all authorized users to ensure such Users observe the confidentiality requirements outlined in the E-MOU.

C. Users will not store or transmit data on a portable storage device, such as but not limited to, a USB flash drive, cell phone, portable laptop, external hard drive or through unencrypted e-mail with the exception of system backup tapes and files. System backup tapes and files will be encrypted to prevent data loss.

D. The Data Integration Hub will have policies and procedures regarding data security that protect against violations of federal and state law, when the data is at rest and during transmission. The Participating Agency reserves the right to request the Operating Group to assist in an audit or assessment regarding access to Participating Agency's data therein.

E. The Data Integration Hub shall comply with the following access and security requirements:
    1. Limited Access. The Data Integration Hub will limit access to the Participating Agency's confidential data to staff who have signed the Confidentiality Agreement attached and incorporated herein as Exhibit C and are working on a specific data sharing project with the Participating Agency pursuant to the terms of the E-MOU.
    2. Use. The Data Integration Hub shall use the Participating Agency's data solely for the purpose approved by the Participating Agency. The Data Integration Hub shall only disclose the Participating Agency's data to staff with the authority to handle the data in furtherance of the Participating Agency's approved purpose and pursuant to this Data Sharing Agreement ("DSA").
    3. Data Deletion. The Data Integration Hub shall retain the Participating Agency's Data used for matching for a period no later than ten (10) business days after the match has been completed pursuant to this DSA and specified in Exhibit A, unless all the Parties agree in writing to extend the retention time. The match has been completed when the Representatives of the Parties (as listed in Section XII herein) have agreed in writing that the match results are optimal.

F. Anonymization of Data
    1. Criteria for Anonymized Data. The Participating Agencies have determined that anonymized data shall remove all personal identifiers which can be used to distinguish or trace an Individual.
    2. Cell Suppression Policy. The Data Integration Hub agree that approved projects including data from the Participating Agency in the creation of any dissemination materials (e.g., project updates, tables, reports, presentations) must adhere to the cell size suppression stated herein:
        a. No cell (e.g., grouping of individuals, patients, students, clients) with less than ___ observations may be displayed.

b. No use of percentages or other mathematical formulas may be used if they result in a cell displaying less than ___ observations.
c. Individual level records may not be published in any form, electronic or printed.
d. Reports and analytics must use complementary cell suppression techniques to ensure that cells with fewer than ____ observations cannot be identified by manipulating data in adjacent rows, column or other manipulations of any combination of dissemination materials generated through an approved project. Examples of such data elements include but are not limited to geography, age groupings, race/ethnicity, sex, or birth or death dates.

IV. TRANSFER OF DATA FROM PARTICIPATING AGENCIES AND DATA INTEGRATION HUB TO DATA RECIPIENT

The Participating Agency will submit to the Data Integration Hub, or otherwise permit the Data Integration Hub staff to electronically access, the data associated with approved data sharing or data linking projects as evidenced by the documents attached to this DSA and required pursuant to the E-MOU and its Appendices. Confidential Data will be transferred electronically to the Data Integration Hub and to the Data Recipient only via encrypted files and in accordance with the security requirements outlined in the E-MOU and the State of Connecticut's cybersecurity policies.

V. DATA INTEGRATION HUB'S RIGHTS TO SHARE/RE-DISTRIBUTE THE DATA

Except as expressly provided in this DSA and the E-MOU, the Data Integration Hub shall not distribute any Data submitted by the Participating Agency without the Participating Agency's written approval.

VI. RESPONSIBILITIES OF DATA RECIPIENT

A. Permitted Data Sharing Project: Approved Use and Data Elements

This DSA pertains to the P20 WIN Project entitled: _____. This P20 WIN Project was approved by all Participating Agency(s) and the Data Recipient on _____ (Date) and the approved Data Sharing Request Form is attached and incorporated hereto as Exhibit A.

The approved Data Sharing Request Form details the permitted use of the Resultant Data as well as the approved data to be included in the Data Sharing project. This DSA pertains only to the use of data elements identified in Exhibit A, and the Data Recipient has requested or obtained appropriate Institutional Review Board (IRB) request or approval, whichever is available, attached as Exhibit D, if relevant and appropriate.

Furthermore, the Participating Agencies and the Data Recipient will abide by all applicable and specific federal and state law confidentiality and privacy requirements as outlined in Exhibit A.

The Data Recipient shall not use the Resultant Data for any purpose independent of, separate from or not directly connected to the purpose(s) specifically approved by the Participating Agencies(s) in Exhibit A.

B. Data Sovereignty and Accuracy

The Data Recipient acknowledges that it must use the Resultant Data in accordance with the approved Data Sharing Request Form (Exhibit A) and pursuant to the IRB request or approval (Exhibit D), if relevant and appropriate, and that the Data Recipient may only receive and use the Resultant Data for the purposes approved by the Participating Agencies.

The Data is current as of the date and time compiled and can change. The Participating Agencies providing data do not ensure 100% accuracy of all records and fields. Some data fields may contain incorrect or incomplete data. The Data Integration Hub and the Participating Agencies providing the data cannot commit resources to explain or validate complex matching and cross-referencing programs; the Data Integration Hub does provide documentation for each data matching process about the rules used in the match and the match rate. The Data Recipient accepts the quality of the data they receive. Questions by the Data Recipient related to the Resultant Data completeness (i.e. approved data elements in the attached Exhibit A) or matching accuracy shall be in writing and sent to the Operating Group within ten (10) business days of receipt of all data sets. Data that has been manipulated or reprocessed by the Data Recipient is the responsibility of the Data Recipient. The Data Integration Hub cannot commit resources to assist Data Recipient with converting data to another format.

C. Data Transfer

Resultant Data outlined in Exhibit A will be transferred to the Data Recipient through a secure transmission, that meets state and federal laws, such as file transfer protocol provided or approved by the Data Integration Hub. The Data Recipient will be provided secure access to the secure transmission and will be allowed to download the Resultant Data file(s) for a limited period of time after which access to the secure transmission will be removed or the data files will be deleted.

D. Safeguarding Data

1. Security Controls. The Data Recipient shall implement and maintain the data security controls specified in the Data Sharing Request Form (Exhibit A) that has been approved by the Participating Agencies that provided the data.
2. Cell Suppression Policy. The Data Recipient agrees that any use of the data in the creation of any dissemination materials (including but not limited to a manuscript, table, chart, study, report, presentation, etc.) concerning the specified purpose must adhere to the cell size suppression policy as follows:

This policy stipulated that no cell (e.g. grouping of individuals, patients, clients, recipients, etc.) with less than ____ observations may be displayed. This is the most stringent cell size allowable among the Participating Agencies that provided the data for the P20 WIN Project specified in this DSA.

No use of percentages or other mathematical formulas may be used if they result in a cell displaying less than ____ observations.

Individual level records may not be published in any form, electronic or printed.

Reports and analytics must use complementary cell suppression techniques to ensure that cells with fewer than ____ observations cannot be identified by manipulating data in adjacent rows, columns or other manipulations of any combination of dissemination materials generated through this P20 WIN Project. Examples of such data elements include, but are not limited to geography, age groupings, sex, or birth or death rates.

E. Any person or entity that processes or receives the Resultant Data, and its agents, vendors and independent contractors must be obligated, by written contract, to adhere to the terms of this DSA and agree to follow the data security controls approved in the attached Exhibit A and the E-MOU, prior to being granted access to Resultant Data, and to sign the Confidentiality Agreement, attached as Exhibit C. The following named individuals, and only these individuals, will have access to the Resultant Data shared pursuant to this DSA:

NAME	POSITION	ORGANIZATION	EMAIL ADDRESS	TELEPHONE

The Data Recipient will notify the Operating Group of the name, role and organization for additions and/or replacements of persons listed above. The Operating Group will share such addition/replacements of persons with the Participating Agencies and shall obtain written approval from the Participating Agencies involved in the Data Request that the new person(s) are approved to have access to the Resultant Data before access to the Resultant Data is provided.

F. Accountability: Unauthorized Access, Use, or Disclosure

The Data Recipient shall take all steps necessary to prevent any use or disclosure of Resultant Data not authorized by this DSA. The Data Recipient will report any unauthorized access, use or disclosure of the Resultant Data to the Operating Group and to the particular the Participating Agencies from which the data originated as soon as learning or had reasonable belief of the unauthorized access, use, or disclosure. The Data Recipient shall follow the reporting requirements contained in Exhibit A. In the event that the Operating Group determines or has a reasonable belief that the Data Recipient has made or may have made use of or disclosed Resultant Data in a manner that is not authorized by this DSA, the Operating Group may, at its sole discretion, require the Data Recipient to perform one or more of the following, or such other actions as the Operating Group, in its sole discretion, deems appropriate, including but not limited to:

1. Promptly investigate and report to the Operating Group the Data Recipient's determinations regarding any alleged or actual unauthorized access, use, or disclosure;
2. Immediately cease use of and disallow access to the Resultant Data by all Users;
3. Promptly resolve any issues or problems identified by the investigation:
4. Submit a formal response to an allegation of unauthorized access, use, or disclosure;
5. Submit a corrective action plan with steps designed to prevent any future unauthorized access, use, or disclosures; and
6. Return all data or destroy data it has received under this DSA.

The Data Recipient understands that as a result of the Operating Group's determination or reasonable belief that unauthorized access, use, or disclosures have occurred, the Participating Agencies may refuse to release further Data to the Data Recipient for a period of time to be determined by the Participating Agencies.

G. Project Reporting Requirements

1. Pre-Publication Data Review . Data Recipients are required to share P20 WIN Project Data findings with the Operating Group at a minimum of ten (10) business days prior to any release beyond the list of Users identified in Section VI, above. The Operating Group shall secure written confirmation from the Participating Agencies that Data are properly aggregated for release, Data are labeled correctly, that confidential Data are not disclosed and that Data are consistent with the requirements in Section V.D.2. The Participating Agencies can request prior review of specific dissemination materials (e.g. presentations, publications) from the Data Recipient.
2. Project Acknowledgement. All publicly-released materials resulting from the P20 WIN Project referenced in this DSA shall include the following acknowledgement:

> "This work would not be possible without data provided by the P20 WIN participating agencies. The findings do not necessarily reflect the opinions of the State of Connecticut or the organizations and agencies contributing data."

Final Publication. Subsequent to the Pre-Publication Data Review discussed in V.G.1. above, the Data Recipient shall provide the Operating Group with an electronic copy of all published work resulting from the P20 WIN Project associated with this DSA within 30 days of publication

H. Data Retention and Destruction

The Data Recipient agrees to destroy all Resultant Data and any derived data not submitted as part of the reporting requirements under Section F., by the Project End Date, stated in Section XI below, in accordance with the methods established by the "Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals," as established by the United States Department of Health and Human Services (HHS). The Data Recipient may request an extension of the Data Retention Period by submitting a written request that includes a justification to the Operating Group. This extension request must be submitted at least thirty (30) days prior to the P20 WIN Project end date.

When retention of the Resultant Data is no longer justified, the Data Recipient agrees to destroy the Resultant Data and send a completed "Certification of Project Completion and Destruction or Retention of Data" form, which is attached hereto and incorporated herein as Exhibit F, to the P20 WIN Project's designated person in the Operating Group. The Data Recipient agrees not to retain any Resultant Data, or any parts thereof, or any derivative files that can be used in concert with other information after the aforementioned file(s) and the data are destroyed unless all of the Participating Agencies grant written authorization. The Data Recipient acknowledges that such date for retention of Resultant Data is not contingent upon action by the Data Integration Hub.

I. Financial Understanding

The Data Recipient agrees to pay a fee of $_____ to be invoiced upon secure transfer of the Resultant Data, based on the schedule adopted by the P20 WIN Executive Board. Payment is expected to be executed within thirty (30) days of receipt of invoice and the fee is payable to State of Connecticut, Treasurer.

VII. MODIFICATION; ASSIGNMENT; ENTIRE AGREEMENT

This DSA may not be modified except by written agreement of the Parties. This DSA may not be assigned or transferred without the Parties' prior written consent. Subject to the foregoing, this DSA will be binding upon and inure to the benefit of, and be enforceable by, the Parties and their successors and assigns. Notwithstanding anything to the contrary, each Party has the right to disclose the terms and conditions of this DSA to the extent necessary to establish rights or enforce obligations under this DSA.

VIII. NO FURTHER OBLIGATIONS

The Parties do not intend that any agency or partnership relationship be created by this DSA. No Party has any obligation to provide any services using or incorporating the data unless the Participating Agencies agree and approves of this obligation under the terms of the E-MOU. Nothing in this DSA obligates the Participating Agencies to enter into any further agreement or arrangements related to the disclosure of information or data.

IX. COMPLIANCE WITH LAW; APPLICABLE LAW

The Parties agree to comply with all applicable federal and state laws and regulations in connection with this DSA. The Parties agree that this DSA shall be governed by the laws of the State of Connecticut, without application of conflict of laws principles.

X. SOVEREIGN IMMUNITY

Nothing in this E-MOU waives the State of Connecticut's sovereign immunity from suit and all of the protections under sovereign immunity.

XI. TERM

The term of this DSA is from Effective Date to _____ (the "Project End Date"). A Party may terminate this DSA upon sixty (60) days' written notice to the other Parties. The terms of this DSA that by their nature are intended to survive termination will survive any such termination as to data provided, and performance of this DSA, prior to the date of termination, including Sections I through VIII.

XII. REPRESENTATIVES

The contacts for purposes of this Agreement are:

For PARTICIPATING AGENCY:

_____

Name
Title
Contact Information

For DATA INTEGRATION HUB

_____

Name
Title
Contact Information

For PARTICIPATING AGENCY:

_____

Name

For DATA RECIPIENT

_____

Name

Title
Contact Information

Title
Contact Information

IN WITNESS WHEREOF, the undersigned have executed this Data Sharing Agreement as of the Effective Date.

DATA INTEGRATION HUB

By: _____
Name:
Title:

PARTICIPATING AGENCY

By: _____
Name:
Title:

PARTICIPATING AGENCY

By: _____
Name:
Title:

DATA RECIPIENT

By: _____
Name:
Title: