The Linked Information Network of Colorado

Data Sharing Agreement

1. Preamble

This Data Sharing Agreement ("Agreement"), is by and between _____ ("Provider") and The Governor's Office of Information Technology, ("OIT"), with its principal place of business at 601 East 18th Avenue, Denver, CO 80203 and is effective as of the last date of signature shown below (the "Effective Date").

WHEREAS, OIT will act as the linking hub of The Linked Information Network of Colorado (LINC).

WHEREAS, Provider wishes to share data with OIT in accordance with the terms and conditions of this Agreement and approved under the terms and conditions of the LINC Enterprise Memorandum of Understanding (EMOU) executed by OIT on July 26, 2019 and the Provider's Joinder Agreement executed by Provider on [DATE], the validity of which are acknowledged and incorporated herein as Attachment A.

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

2. Transfer of Data from Provider to OIT

Provider will submit to OIT, or otherwise permit OIT's LINC staff to electronically access, the data associated with approved LINC Projects in accordance with the LINC EMOU. Confidential Data will be transferred electronically only via encrypted files and in accordance with OIT's data security standards and the State of Colorado's cybersecurity policies (http://www.oit.state.co.us/ois/policies).

3. OIT's Rights to Share/Redistribute the Data

Except as expressly provided in this Agreement and the LINC EMOU, any data submitted to LINC by the Provider will not be further distributed without Provider's written approval.

4. Data Access, Security, Use, and Deletion.

OIT will comply with the following access and security requirements:

a. Limited Access. OIT will limit access to the Confidential Data to LINC Data Integration Staff who have signed the Confidentiality Agreement in Attachment B and are working on a specific LINC Project with the Provider under the terms of the LINC EMOU. Only Anonymized Data will be provided to LINC Data Recipients of approved LINC Projects as defined in the accompanying LINC EMOU.

b. Secure Storage. OIT agrees to proceed according to requirements, contained in (FISM) NIST SP800-39, Managing Information Risk. Furthermore, OIT shall be responsible for

maintaining a secure environment compliant with applicable State and Federal policies, standards and guidelines, and other Applicable Law that supports the Transmission of Data in compliance with the Specifications. OIT shall follow the specifics contained in (FISM) NIST SP800-47, Security Guide for Interconnecting Information Technology Systems and shall use appropriate safeguards to prevent use or disclosure of Data other than as permitted by the LINC EMOU, the (FISM) NIST SP800-47, and Applicable Law, including appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of that Data. Appropriate safeguards shall be those required by Applicable Law related to Data security, specifically contained in (FISM) NIST SP800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

c. Use. OIT shall use the Confidential Data solely for purposes approved through the LINC EMOU ("Purpose"). OIT shall only disclose the Confidential Data to LINC Data Integration Staff who have the authority to handle the data in furtherance of the Purpose. OIT will only provide approved LINC Project Data to LINC Data Recipients who have signed the LINC Data Use License in Attachment C.

d. Data Deletion. For approved LINC Projects that require data matching once, OIT shall retain the Provider's Confidential Data for LINC projects for a period of three months after providing the Anonymized Data to the LINC Data Recipient. After this three-month period, all Confidential Data will be deleted by OIT, unless otherwise directed by the Provider in writing to hold the data for an extended time period. For approved LINC Projects requiring multiple data matches over the life of the project, OIT shall retain an encrypted file that contains only the data necessary for matching and the unique LINC identifier. This encrypted identity file will be destroyed three months after the last required data match for the approved LINC Project. OIT shall retain the Anonymized Data related to the approved LINC project for the life of the project period as identified in the Data Use License (DUL).

5. Anonymization of LINC Project Data

a. Criteria for Anonymized Data. Only Anonymized Data may be released to LINC Data Recipients for approved LINC Projects. The Provider has determined that Anonymized Data shall remove all personal identifiers which can be used to distinguish or trace an individual's identity. These include

b. Cell Suppression Policy. OIT agrees that LINC Projects including data from the Provider in the creation of any dissemination materials (manuscript, table, chart, study, report, presentation, etc.) must adhere to the cell size suppression policy as follows. This policy stipulates that no cell (e.g., grouping of individuals, patients, clients) with less than XX observations may be displayed. Also, no use of percentages or other mathematical formulas may be used if they result in a cell displaying less than XX 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 XX observations cannot be identified by manipulating data in adjacent rows, columns or other manipulations of any combination of dissemination materials

generated through LINC Projects. Examples of such data elements include, but are not limited to, geography, age groupings, sex, or birth or death dates.

Provider Responsibilities for Meeting Legal Requirements

Provider has collected the Confidential Data from individuals. Accordingly, Provider is solely responsible for ensuring that all legal requirements have been met to collect data on individuals whose Confidential Data are being provided to LINC.

6. Confidentiality and Breach Notification

a. Confidentiality. All LINC Data Integration Staff shall be informed of the confidentiality obligations imposed by this Agreement and must agree to be bound by such obligations prior to disclosure of Confidential Data to LINC Data Integration Staff, as evidenced by their signature on the Confidentiality Agreement in Attachment A. OIT shall protect the Confidential Data by using the same degree of care as OIT uses to protect its own confidential information, and no less than a reasonable degree of care.

b. Breach Notification. OIT is responsible and liable for any breach of this Agreement by any of its LINC Data Integration Staff. OIT shall report to the Provider all breaches that threaten the security of the State's databases resulting in exposure of Confidential Data protected by federal or state laws, or other incidents compromising the security of the State's information technology systems. Such reports shall be made to the Provider within 24 hours from when OIT discovered or should have discovered the occurrence. OIT shall also comply with any Applicable Law regarding data breaches.

7. Modification; Assignment; Entire Agreement

This Agreement may not be modified except by written agreement of the Provider and OIT. This Agreement may not be assigned or transferred without the Provider and OIT's prior written consent. Subject to the foregoing, this Agreement will be binding upon and inure to the benefit of, and be enforceable by, the Provider and OIT and its successors and assigns. Notwithstanding anything to the contrary, each party has the right to disclose the terms and conditions of this Agreement to the extent necessary to establish rights or enforce obligations under this Agreement. This Agreement supersedes all previous LINC Data Sharing Agreements, whether oral or in writing.

8. No Further Obligations

The Provider and OIT do not intend that any agency or partnership relationship be created by this Agreement. No party has any obligation to provide any services using or incorporating the Confidential Data unless the Provider agrees and approves of this obligation under the terms of the LINC EMOU. Nothing in this Agreement obligates the Provider to enter into any further agreement or arrangements relating to disclosure of information or data.

9. Compliance with Law, Applicable Law

The Provider and OIT agree to comply with all applicable laws and regulations in connection with this Agreement. The Provider and OIT agree that this Agreement shall be governed by the laws of the State of Colorado, without application of conflicts of laws principles.

10. Term of Agreement

The Provider and OIT may terminate this Agreement upon sixty (60) days' written notice to the other party. The terms of this Agreement that by their nature are intended to survive termination will survive any such termination as to Confidential Data provided, and performance of this Agreement, prior to the date of termination, including Sections 2, 3, 4, 5, 6, 7, 8, 9, and 10.

11. Use of Name

Neither the Provider nor OIT will use the name of the other party or its employees in any advertisement or press release without the prior written consent of the other party.

12. Definitions

a. Anonymized Data: Data where appropriate personal identifiers have been removed for a LINC Data Recipient such that the likelihood of being able to re-identify individuals is extremely low. The criteria for Anonymized Data are outlined in section 5a.
b. Confidential Data: Data submitted by the Provider that have not been Anonymized.
c. Data Use License (DUL): Agreement between OIT and the LINC Data Recipient that outlines the role and responsibilities of the LINC Data Recipient. The DUL shall include the LINC Project objectives, methodology, data description, data security plan, completion date, reporting requirements, data privacy requirements, and terms for data destruction.
d. LINC Data Integration Staff: The individuals within the Linking Hub who will have the approved responsibility of handling and securing relevant Confidential Data from Parties for approved LINC Projects. The LINC Data Integration Staff will consult with Party staff, clean Confidential Data, link Confidential Data, and prepare Anonymized Data for LINC Projects.
e. LINC Data Recipient: The individual or organization that has received approval for a LINC Project to use integrated Anonymized Data for analysis, research, or evaluation purposes. The LINC Data Recipient may be an employee from a LINC Data Provider or an external researcher.
f. LINC Project: A project approved under the terms of the LINC EMOU. A LINC Project must be analytic, research, or evaluative in nature. A LINC Project must require Confidential Data from two or more Data Providers and must be achievable by LINC Data Recipients with Anonymized Data.

[*Remainder of page left intentionally blank, continue on subsequent page*]

13. Representatives

The contacts for purposes of this Agreement are:

For Provider:

For OIT:

Jon Gottsegen
Chief Data Officer

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

OIT

By: _____
Name: Laura Calder
Title: Chief Financial Officer

Date: _____

PROVIDER

By: _____
Name:
Title:

Date: _____

Attachment A: [LINC EMOU]

Attachment B:

COLORADO GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY
CONFIDENTIALITY AGREEMENT

I, _____, hereby acknowledge that, with regard to a request for information through the Linked Information Network of Colorado (LINC) and the associated Data Sharing Agreement ("Agreement") between the Colorado Governor's Office of Information Technology (OIT) and _____ (Provider), I may acquire or have access to confidential information or personally identifiable information associated with Colorado residents.

I agree to comply with all the terms of the Agreement regarding the access, use, and disclosure of any information submitted by Provider to OIT.

At all times I will maintain the confidentiality of the information. I will not inspect or "browse" the information for any purpose not identified in the Agreement. I will not access, or attempt to access, my own information, or information relating to an individual or entity with which I have a personal or financial interest, for any reason not necessary to the performance of the work assigned to me under the Agreement. This includes, but is not limited to, information relating to family members, neighbors, relatives, friends, ex-spouses, their employers, and/or anyone not necessary for the work assigned.

At no time will I either directly or indirectly, disclose, or otherwise make the information available to any unauthorized person.

I agree to comply with all applicable state and federal laws and regulations with regard to confidentiality and security of the information, including but not limited to, the following.

Colorado Rules Volume 6 - Section 6.210
Colorado Information Security Act (C.R.S. 24-37.5)
Colorado Revised Statutes Title 26, Article 1, section 26-1-114
Governor's Office of Information Technology, System Applications Statement of Compliance (as revised)
Social Security Act (Title 42 U.S.C)
Privacy Act of 1974
Federal Information Security Management Act of 2002 (FISMA)
Internal Revenue Code Section 6103
Health Insurance Portability and Accountability Act (45 CFR Part 160 and Part 164)
42 Code of Federal Regulations ("CFR") Part 2
The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g and 34 CFR Part 99)

Civil and criminal penalties for willful misuse of information can be found in the aforementioned citations.

Executed:

_____ _____

Signature Date

Printed Name:

_____

Organization Name:

_____

Telephone: _____ Email: _____