Data Sharing Agreement

This Data Sharing and License Agreement ("Agreement") is entered into by and between [LINC DATA PARTNER NAME] ("Transferring Agency"), having an address at [LINC DATA PARTNER ADDRESS] and The Governor's Office of Information Technology ("Recipient"), whose principal office is located at 601 East 18th Avenue, Denver, CO, 80203. Transferring Agency and Recipient are each individually a "Party" and together the "Parties." All activities in this Agreement must be accomplished 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 7/26/19 and the Provider's Joinder Agreement executed by Provider on [DATE], the validity of which are acknowledged and incorporated herein as Attachment A.

Whereas, Transferring Agency is charged with sharing data with Recipient.

Whereas, Recipient will act as the data linking hub of The Linked Information Network of Colorado (LINC).

Now, therefore, in consideration of the mutual promises contained herein, the sufficiency of which each Party hereby acknowledges as adequate, the Parties agree as follows:

1. Defined Terms.

a) "Anonymized Data" means Data that has been properly De-identified. Only Anonymized Data may be released to LINC Project Teams for approved LINC Projects. The Transferring Agency has determined that Anonymized Data shall remove all personal identifiers which can be used to distinguish or trace an individual's identity. These include name, social security number, date of birth, residential address smaller than town or city, telephone and fax numbers, email address, data provider unique identifiers.

b) "CORA" means the Colorado Open Records Act, § 24-72-200.1, *et seq.*, C.R.S.

c) "CJI" means all FBI CJIS-provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including, but not limited to: biometric, identity history, person, organization property (when accompanied by any PII), and case/incident history data. In addition, CJI refers to FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to, data used to make hiring decisions. The following type of data is exempt from the protection levels required for CJI: transaction control type number (e.g. ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or PII.

d) "CJIS Addendum" means the addendum attached to this Agreement as Addendum 1.

e) "Confidential Data" means Data submitted by the Provider that have not been Anonymized and contains PII.

f) "Data" means the information described in Appendix A.

g) "Data Breach" means an event resulting in an unauthorized access, use, exposure, disclosure, exfiltration, or loss of Data.

h) “Data Use License (DUL)” means the Agreement signed by the LINC Project Team that outlines the role and responsibilities of the LINC Project Team allowing receipt of the Anonymized LINC Project Data. 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.

i) “De-identified” means the removal of all PII from the Data so that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. If the Data is subject to HIPAA, “De-Identified” means the removal of PII from the Data in accordance with HIPAA.

j) “Destroy" means to remove Data from Recipient’s systems, paper files, records, databases, and any other media regardless of format, in accordance with the standard detailed in the OIT Security Policy.

k) “Enterprise Memorandum of Understanding (EMOU)” means the partnership agreement that defines the governance model, roles, and responsibilities of participating organizations in LINC.

l) "HIPAA” means the Health Insurance Portability and Accountability Act of 1996 and subsequent Amendments.

m) “Incident” means an event that results in or constitutes an imminent threat of the unauthorized access, use, loss, disclosure, modification, disruption, or destruction of communication and information resources of the State.

n) “Linked Information Network of Colorado (LINC)” means the data sharing collaborative in Colorado that allows for approved research and analytic projects requiring de-identified linked administrative data sets.

o) “LINC Data Integration Team” means the Recipient individuals who will have the approved responsibility of handling and securing relevant Confidential Data from Transferring Agency for approved LINC Projects. The LINC Data Integration Team will consult with Transferring Agency Team, clean Confidential Data, link Confidential Data, and prepare Anonymized Data for LINC Projects.

p) “LINC Project” means a data 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 sources and must be achievable by LINC Project Teams with Anonymized Data.

q) “LINC Project Team” means 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 Project Team may be an employee from a Transferring Agency or an external researcher.

r) “OIT” means the Governor’s Office of Information Technology.

s) “OIT Security Policies” means the security policies established by OIT to secure information held by State Agencies, which are available at: https://oit.colorado.gov/standards-policies-guides/technical-standards-policies.

t) "Protected Health Information" has the same meaning as such term is defined in HIPAA.

u) "PII" means information which can reasonably be used to identify, contact or locate an individual, either alone or in combination with other information.

2. **Sharing of Data.** Transferring Agency will submit to Recipient, or otherwise permit the LINC Integration Team 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 Recipient's data security standards and the State of Colorado's cybersecurity policies (http://www.oit.state.co.us/ois/policies).

3. **Data Use and Restrictions.** Transferring Agency hereby grants Recipient a limited, revocable right to use the Data solely for purposes of LINC Projects approved through the governance processes defined in the LINC EMOU. (the "Purpose"). Specifically, Recipient may perform data cleaning, linkage, and preparation of the LINC Project Data to meet the goals of the approved LINC Project. If Appendix A indicates the Data includes CJI, then Recipient must treat the Data in accordance with the terms of the CJIS Addendum. If the CJIS Addendum applies to the Data, then the terms of that Addendum are hereby incorporated by reference to this Agreement. In the event of a conflict between the CJIS Addendum and the terms of this Agreement, the terms of the CJIS Addendum shall apply.

a) **Disclosure to Third Parties.** Recipient will only provide approved Anonymized LINC Project Data to LINC Project Teams who have signed the LINC Data Use License in Attachment C. Recipient shall not sell, lease, rent, loan, transfer, distribute, alter, mine or disclose the Data, including but not limited to, metadata and Anonymized Data, with any third party without the prior written consent from Transferring Agency. Recipient has not and will not use or disclose any Personal Identifying Information, as defined by § 24-74-102(1), C.R.S., for the purpose of investigating for, participating in, cooperating with, or assisting Federal Immigration Enforcement, including the enforcement of civil immigration laws, and the Illegal Immigration and Immigrant Responsibility Act, which is codified at 8 U.S.C. §§ 1325 and 1326, unless required to do so to comply with Federal or State law, or to comply with a court-issued subpoena, warrant or order.

b) **Restrictions on Access to Confidential Data.** Recipient shall not disclose the Confidential Data to anyone other than Recipient's Data Integration Team who have signed the Confidentiality Agreement in Attachment B and are working on a specific LINC Project under the terms of the LINC EMOU.

c) **Data Security Requirements.** Recipient agrees to secure and protect the Data against any unauthorized use or access in accordance with the most recent version of the OIT Security Policies. Recipient agrees to proceed according to requirements, contained in (FISM) NIST SP800-39, Managing Information Risk. Furthermore, Recipient 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. Recipient 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. Upon request and in accordance with conditions to be mutually agreed upon by Recipient and Transferring Agency, Transferring Agency may audit, assess, or pen test the efficacy of the applied NIST controls.

d) **Accuracy.** If either Party becomes aware that the Data is inaccurate or outdated, it agrees to inform the other Party within a reasonable time period.

e) **Storage of Data.** Recipient agrees to: (i) use, hold, and maintain the Data in compliance with any and all applicable laws and regulations, (ii) store the Data only in facilities located within the United States, and (iii) maintain the Data in a secure environment in accordance with the OIT Security Policies.

f) **Destruction of Data.** For approved LINC Projects that require data matching once, Recipient shall retain the Transferring Agency's Confidential Data for LINC projects for a period of three months after providing the Anonymized Data to the LINC Project Team. After this three-month period, all Confidential Data will be deleted by Recipient, unless otherwise directed by the Transferring Agency 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, Recipient shall retain an encrypted file that contains only the data necessary for matching and the unique LINC random identifier. This encrypted identity file will be destroyed three months after the last required data match for the approved LINC Project. Recipient shall retain the Anonymized Data related to the approved LINC project for the life of the project period as identified in the LINC Data Use License. Upon Transferring Agency's request, or upon any termination or expiration of the Agreement, Recipient shall Destroy or return any Data in its possession, pursuant to Transferring Agency's instructions, in accordance with OIT Security Policies. Upon Transferring Agency's request, Recipient shall certify in writing that it has Destroyed the Data within thirty (30) days of Recipient's receipt of Transferring Agency's request.

g) **Reservation of Rights.** Except for the rights explicitly granted under this Agreement, Recipient is not granted any rights in and to the Data, including, but not limited to any Anonymized Data.

h) **Research, Analytics and Published Materials.** Recipient and LINC Project Teams may use the Data to run internal analytics and investigational protocols, and create reports and public materials including data dashboards only to the extent such activities align with the Purpose approved by the Transferring Agency through the processes outlined in the LINC EMOU.

i) **Linking Data to other Datasets.** Transferring Agency agrees that Recipient may include the Data with data from other sources in carrying out the Purpose approved through the processes outlined in the LINC EMOU. Recipient agrees that such combined datasets will treat and safeguard the data in accordance with all applicable laws.

j) **Right to Audit.** The Transferring Agency has the right to perform an audit on the LINC computing environment to ensure that all data security and access conforms with the terms of this agreement.

4. **Security Incident and Data Breach.**

a) **Incident Response.** If Recipient becomes aware of an Incident, Recipient shall use commercially reasonable practices to fully investigate and resolve the Incident and take steps to prevent developments that may result in the Incident becoming a Data Breach in accordance with all applicable privacy and security laws.

b) **Data Breach Response.** Immediately upon becoming aware of a suspected or actual Data Breach, Recipient shall: (i) notify Transferring Agency of the Data Breach in writing, (ii) start a full investigation into the Data Breach, (iii) cooperate fully with Transferring Agency's investigation of and response to the Data Breach, and (iv) use commercially reasonable efforts to prevent any further Data Breach in accordance with applicable privacy and security laws. If notification of the Data Breach is required pursuant to applicable law, Recipient shall coordinate with Transferring Agency in delivering such notifications and shall be responsible for all costs associated with such notification. In the event the Parties determine that Recipient should deliver the necessary notifications, Recipient shall obtain Transferring Agency's prior written approval of the notifications prior to distributing such notifications.

c) **Data Breach Report.** If Transferring Agency reasonably determines that a Data Breach has occurred, then Transferring Agency may request that Recipient submit a written report, and any supporting documentation, identifying (i) the nature of the Data Breach including the dates of the Data Breach, when Recipient discovered the Data Breach, and number of impacted individuals, (ii) the steps Recipient has executed to investigate the Data Breach, (iii) what Data or PII was used or disclosed, (iv) who or what was the cause of the Data Breach, (v) what Recipient has done or shall do to remediate any deleterious effect of the Data Breach, and (vi) what corrective action Recipient has taken or shall take to prevent a future Incident or Data Breach. Recipient shall deliver the report within seven (7) days of Transferring Agency's request of the report. If the Recipient learns of more information necessary for understanding the nature of the Data Breach, risk to the Data, remediation efforts, or notification requirements after submitting the report, Recipient shall update Transferring Agency without delay.

d) **Effect of Data Breach.** Transferring Agency may terminate this Agreement immediately, at its sole discretion, upon the occurrence of a Data Breach. In addition, Transferring Agency may restrict Recipient's access to the Data and require Recipient to suspend all work involving the Data, pending the investigation and successful resolution of any Data Breach.

e) **Liability for Data Breach.** Without limiting any other remedies Transferring Agency may have under law or equity, Recipient shall reimburse Transferring Agency in full for all costs, including but not limited to, payment of legal fees, audit costs, fines, and other imposed fees arising out of or relating to a Data Breach that Transferring Agency actually incurs. All responsibilities of Recipient under this Section 4 shall be completed by Recipient at Recipient's sole cost, without any right of reimbursement, set-off, payment, or remuneration of any kind from Transferring Agency.

5. **Term and Termination.**

a) The "Term" of this Agreement shall be one (1) year from the last date of execution set forth on the signature page unless terminated sooner pursuant to the terms herein. At the end of the Term, this Agreement shall automatically renew for additional one (1) year periods for up to five(5) years unless either Party provides the other Party with written notice of its intent to terminate this Agreement sixty (60) days prior to expiration of the then-current Term.

b) Transferring Agency may suspend its performance or terminate this Agreement immediately upon written notice to Recipient in the event of Recipient's breach of any of its obligations under Sections 3 or 4.

6. **Dispute Resolution.** In the event of a dispute related to this Agreement, the Parties' Executive Directors shall have ten (10) business days to resolve the dispute. If this fails, both Parties shall submit the matter in writing to the Executive Director of the Department of Personnel and Administration, or their delegate for final resolution.

7. **General Provisions.**

a) **Amendment.** The Parties may only amend this Agreement in a writing signed by both Parties.

b) **Assignment.** Recipient's rights and obligations under this Agreement are personal and Recipient may not transfer or assign its rights without Transferring Agency's prior, written consent. Any of Recipient's attempts at assignment or transfer without such consent shall be void. If Transferring Agency approves any assignment or transfer of Recipient's rights and obligations, this Agreement will continue to govern such rights and obligations.

c) **Counterparts.** The Parties may execute this Agreement in multiple, identical, or original counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement.

d) **Entire Understanding.** This Agreement, including, but not limited to, the recitals, which are incorporated into this Agreement by reference, represents the complete integration of all understandings between the Parties related to the data sharing. All prior representations and understandings related to the data sharing, oral or written, are merged into this Agreement. Prior or contemporaneous additions, deletions, or other changes to this Agreement shall not have any force or effect whatsoever, unless embodied herein.

e) **Severability.** The invalidity or unenforceability of any provision of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement, which shall remain in full force and effect, provided that the Parties can continue to perform their obligations under this Agreement in accordance with the intent of this Agreement.

f) **Survival.** Sections 1, 3, 4, 6 and 7 of this Agreement, as well as any other provisions that by their nature should survive, shall survive any termination of this Agreement.

g) **Waiver.** A Party's failure or delay in exercising any right, power, or privilege under this Agreement, whether explicit or by lack of enforcement, shall not operate as a waiver, nor shall any single or partial exercise of any right, power, or privilege preclude any other or further exercise of such right, power, or privilege.

h) **Legal Requests.** Transferring Agency acknowledges and agrees that Recipient, or its contractors, may be required to share the Data to respond to a subpoena, court order, open records request or valid legal request (each a "Legal Request"). To the extent permitted by law, Recipient will refer the Legal Request to Transferring Agency of any disclosure of the Data so that Transferring Agency may seek a protective order at its own cost.

i) **CORA.** The Parties agree to coordinate if either agency receives a CORA request for data that is subject to this Agreement. CORA requests are time sensitive and must be referred to the Parties within one (1) business day to meet statutory open records requirements. To the extent not prohibited by applicable law, this Agreement may be subject to public release through CORA.

j) **Third-Party Beneficiaries.** No third party shall be able to enforce or have the benefit of any of the provisions of this Agreement.

k) **Consents and Compliance with Law.** Each Party shall comply with (i) all applicable federal and State laws, rules, and regulations, that apply to their obligations under the Agreement, including, but not limited to, Privacy Act of 1974, Federal Information Security Management Act of 2002 (FISMA), C.R.S. § 24-73-102 (Protection of Personal Identifying Information), C.R.S. 24-37.5 Part 4 (Colorado Information Security Act), Governor's Office of Information Technology, System Applications Statement of Compliance (as revised), C.R.S. § 24-72-201, et seq. (Colorado Open Records Act or CORA), C.R.S. § 24-30-2101 (Colorado Address Confidentiality Program Act, ACP) (collectively, "Laws"); and (ii) shall obtain all necessary consents to transfer and use the Data for the Purpose in accordance with such Laws. In the event a consent is revoked by an individual in accordance with applicable Laws, the Party that receives the revocation of consent will immediately notify the other Party of the revocation of consent. Upon receipt of a revocation of consent, Recipient shall Destroy and cease using the Data associated with that consent from the date Recipient receives the notice of revocation.

8. Signatures.

Transferring Agency

Signature: _____ Date: _____

[Signatory Name]

[Title]

[Organization]

Recipient

Signature: _____ Date: _____

Amy Bhikha

Chief Data Officer

The Governor's Office of Information Technology

Appendix A

DATA TO BE SHARED

Data to be Shared

The specific data to be shared for a LINC Project will be reviewed and approved by the Transferring Agency according to the processes in the LINC EMOU. The Data Use License signed by the LINC Project Team will include the specific data shared for the LINC Project.

[*Insert if Transferring Agency is a Covered Entity and is sharing Protected Health Information:* Recipient acknowledges and agrees that the Data is Protected Health Information that is protected pursuant to HIPAA, and is subject to the additional terms in the Agreement that apply to Protected Health Information.]

Recipient acknowledges and agrees that the Data is CJI, and is subject to the terms contained in the CJIS Addendum in Attachment D which will be signed by members of the LINC Data Integration Team.

Authorized Personnel and Contractors

Cell Suppression Policy

Without limiting the generality of the definition if De-identified in the Agreement, the Parties agree the Data Use License signed by the LINC Project Team will include a required cell suppression level. Parties agree that LINC Projects including data from the Transferring Agency 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 **5 or fewer** observations may be displayed. Also, no use of percentages or other mathematical formulas may be used if they result in a cell displaying **5 or fewer** 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 **5 or fewer** 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.

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 the _____ (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 federal, state, and local laws and regulations with regard to confidentiality and security of the information identified here.

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:

Attachment C

The Linked Information Network of Colorado

Data Use License

1. Preamble

This Data Use License ("DUL") is entered as of _____ (the "Effective Date") by _____ ("LINC Data Recipient").

This DUL addresses the conditions under which the Colorado Governor's Office of Information Technology (" OIT") will disclose, and the LINC Data Recipient may use, the Anonymized Data for LINC Projects specified in this DUL and/or any derivative file(s) (collectively, the "LINC Project Data"). The terms of this DUL are consistent with those in the LINC Enterprise Memorandum of Understanding (EMOU) and can be changed only by a written and signed amendment to this DUL or by terminating this DUL and entering a new DUL, after approval by the LINC Review Committee.

2. Definitions

a. Anonymized Data. Integrated data that do not include Personal Identifiers. The specific set of Personal Identifiers that must be removed from Anonymized Data are established by each LINC Data Provider in a separate legal agreement with OIT. LINC will use the most restrictive definition of Anonymized Data among all LINC Data Providers contributing data to the LINC Project in this DUL.
b. Authorized Personnel: The members of the LINC Data Recipient team who have been listed in this DUL as having approved access to the LINC Project data and agree to abide by the terms of this DUL.
c. LINC Data Provider: An organization that has direct responsibility for a source of data contributed to the approved LINC Project. This may be an Office or Division of a larger organization, in other cases it may be the organization itself.
d. LINC Data Recipient: The individual or organization that made the approved LINC request for data analysis, research, or evaluation purposes. The LINC Data Recipient will be an employee from a LINC Party or an external researcher.
e. LINC Director: The individual who is responsible for facilitating LINC committees, developing and managing partnerships with Party organizations, overseeing LINC staff,

consulting with data requestors, monitoring LINC Projects, and managing the inventory of documents associated with LINC operations and LINC Projects.

f. LINC Project: A project approved by the LINC Review Committee that is analytic, research or evaluative in nature. A LINC Project requires data from two or more Data Providers and must be achievable by LINC Data Recipients with Anonymized Data.
g. LINC Project Data: Anonymized Data for use by the LINC Data Recipient. These data are only to be used for the approved purposes outlined in the approved LINC Request Form.
h. LINC Request Form: The document that is reviewed by the LINC Review Committee for approval, revision or rejection decisions. The approved LINC Request Form is attached to this DUL as Exhibit 1.
i. LINC Review Committee: The committee composed of representatives from each LINC Data Provider with program or policy expertise and data expertise. At least one of these representatives must have decision-making authority over the use of their data.
j. Personal Identifiers: Any information about an individual that can directly or indirectly distinguish or trace an individual's identity, associate or link an individual to private information, distinguish one person from another, or be used to re-identify individuals.

3. Financial Understanding

The LINC Data Recipient agrees to pay a fee of _____ for the project to the Colorado Evaluation and Action Lab that serves as the fiscal agent for LINC. Half will be invoiced upon project approval and half will be invoiced upon secure transfer of the LINC Project Data. Payment is expected to be executed within 30 days of receipt of invoice.

4. Permitted LINC Project: Approved Use and Data Elements

This DUL pertains to the LINC Project _____ This LINC Project was approved by the LINC Review Committee on _____ and the approved LINC Request Form is attached and incorporated into this DUL as Exhibit 1. The approved LINC Request Form details the permitted use of the LINC Project Data as well as the approved data elements to be included in the LINC Project Data.

The LINC Data Recipient shall not use the LINC Project Data for any purpose independent of, separate from or not directly connected to the purpose(s) specifically approved by the LINC Review Committee. The LINC Data Recipient shall only receive Anonymized Data and will not be permitted to receive any Personal Identifiers.

5. Data Ownership and Accuracy

LINC Data Recipient acknowledges that LINC Data Recipient has no ownership rights with respect to the LINC Project Data, and that the LINC Data Recipient may only receive and use the LINC Project Data for the purposes approved by the LINC Review Committee.

The LINC Project Data is current as of the date and time compiled and can change. The LINC Data Providers do not ensure 100% accuracy of all records and fields. Some data fields may

contain incorrect or incomplete data. OIT and LINC Data Providers cannot commit resources to explain or validate complex matching and cross-referencing programs. LINC Data Recipient accepts the quality of the data they receive. Questions related to LINC Project Data completeness (i.e., approved data elements in the attached Exhibit 1 were received) or matching accuracy shall be sent to the LINC Director within sixty (60) days of receipt. Data that has been manipulated or reprocessed by the LINC Data Recipient is the responsibility of the LINC Data Recipient. OIT cannot commit resources to assist LINC Data Recipient with converting data to another format or answering questions about data that has been converted to another format. Additional issues with the LINC Project Data shall be noted in the Regular Project Report(s) (described in Section 9 below).

6. Data Transfer

LINC Project Data will be transferred to the LINC Data Recipient through a Secure File Transfer Protocol (SFTP) provided or approved by OIT. The LINC Data Recipient will be provided secure access to the SFTP and will be allowed to download the LINC Project Data file(s) for a limited period of time after which access to the SFTP will be removed.

7. Safeguarding Data

Security Controls. The LINC Data Recipient shall implement and maintain the data security controls specified in the LINC Request Form (attached as Exhibit 1) that has been approved by the LINC Review Committee.

Re-Disclosure of Data. LINC Data Recipient shall not use the LINC Project Data for any purpose beyond that specified in Exhibit 1, attached hereto. Furthermore, LINC Data Recipient shall not use the LINC Project Data in an attempt to track individuals, link to an individual's data from other data sources, determine real or likely identities, gain information about an individual or contact any individual (or next-of-kin) who is the subject of the LINC Project. Re-disclosure of data shall result in the immediate suspension of the LINC Project and possible termination of the LINC Project by the LINC Review Committee. Furthermore, individuals engaging in re-disclosure of data will not be approved Authorized Personnel on future LINC Projects.

Cell Suppression Policy. The LINC Data Recipient agrees that any use of LINC Project Data in the creation of any dissemination materials (manuscript, table, chart, study, report, presentation, etc.) concerning the specified purpose 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 _____ observations may be displayed. This is the most stringent cell size allowable among the LINC Data Providers for the LINC Project specified in the approved LINC data request in Exhibit 1. Also, 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 LINC Project. Examples of such data elements include, but are not limited to, geography, age groupings, sex, or birth or death dates.

8. LINC Project Authorized Personnel

Any person or entity that processes or receives the LINC Project Data and its agents must be obligated, by contract, to adhere to the terms of this DUL and agree to follow the data security controls approved in the attached Exhibit 1, prior to being granted access to LINC Project Data. The following named individuals, and only these individuals, will have access to the LINC Project Data. The LINC Data Recipient will submit a LINC Project Change Request to the LINC Director when an individual leaves the project. The LINC Data Recipient will obtain written approval from the LINC Director for additions to this list prior to granting access to LINC Project Data.

Name	Role	Organization

9. Accountability: Unauthorized Access, Use, or Disclosure

LINC Data Recipient shall take all steps necessary to identify any use or disclosure of LINC Project Data not authorized by this DUL. The LINC Data Recipient will report any unauthorized access, use or disclosure of the Data to OIT via the LINC Director within two business days from learning or should have learned of the unauthorized access, use, or disclosure. In the event that OIT determines or has a reasonable belief that the LINC Data Recipient has made or may have made use or disclosure of the LINC Project Data that is not authorized by this DUL, OIT may, at its sole discretion, require the LINC Data Recipient to perform one or more of the following, or such other actions as OIT, in its sole discretion, deems appropriate:

a. promptly investigate and report to OIT the LINC Data Recipient's determinations regarding any alleged or actual unauthorized access, use, or disclosure;
b. promptly resolve any issues or problems identified by the investigation;
c. submit a formal response to an allegation of unauthorized access, use, or disclosure;

d. submit a corrective action plan with steps designed to prevent any future unauthorized access, use, or disclosures; and
e. return all LINC Project Data or destroy LINC Project Data it has received under this DUL.

The LINC Data Recipient understands that as a result of OIT's determination or reasonable belief that unauthorized access, use, or disclosures have taken place, OIT may refuse to release further LINC Project Data to the LINC Data Recipient for a period of time to be determined by OIT, in its sole discretion.

10. LINC Project Reporting Requirements

Regular Project Reports. LINC Data Recipients must submit Regular Project Reports to the LINC Review Committee, annually or at the midterm point of the project cycle, whichever comes first. The report shall be a standard form automatically distributed by the LINC Director or support staff and shall require:

a. IRB approval documentation
b. Summary of progress to date
    - How project is informing policy or practice
    - Description of anticipated and unanticipated findings
    - Description of challenges encountered and how they are being resolved
c. Dissemination materials and key findings to date
d. Project funding source (if applicable)

Change Requests. LINC Data Recipients will initiate, when necessary, a LINC Project change request. Minor requests (e.g., change in key personnel, a first-time extension of up to six months) will be reviewed by the LINC Director. Major requests (e.g., additional research questions; change in organization using data) will be reviewed by the LINC Review Committee.

Key Findings and Interpretations Release Request. LINC Data Recipients are required to share LINC Project findings to the LINC Review Committee prior to any public release. LINC Review Committee members have the right to request that their organization be anonymized in any publications. LINC Data Recipients shall submit key findings and interpretations in a standard format provided by the LINC Director or support staff. LINC Review Committee members shall confirm in writing, via a standard form provided by the LINC Director, that key findings have been reviewed and are ready for release. The LINC Review Committee members can request review of specific dissemination materials (e.g., presentations, publications).

LINC Acknowledgement. All publicly-released materials resulting from the LINC Project referenced in this DUL shall include the following acknowledgement: "This work would not be possible without anonymized data provided by the Linked Information Network of Colorado (LINC). The findings do not necessarily reflect the opinions of the Colorado Governor's Office of

Information Technology, the Colorado Evaluation and Action Lab, or the organizations contributing data."

Final Publication(s). The LINC Data Recipient shall provide the LINC Director with an electronic copy of all published work resulting from the LINC Project associated with this DUL within 30 days of publication.

11. Data Retention and Destruction

The LINC Data Recipient agrees to destroy all LINC Project Data by the approved LINC Project end date, in accordance with the "Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals," as established by the U.S. Department of Health and Human Services (HHS). The LINC Data Recipient may request an extension of the Data Retention Period by submitting a written request that includes justification to the LINC Review Committee via the LINC Director. This extension request must be submitted 30 days prior to the LINC Project end date.

When retention of the LINC Project Data is no longer justified, the LINC Data Recipient agrees to destroy the Data and send a completed "Certification of Project Completion & Destruction of Data" form (Attachment 1 to this Agreement) to OIT via the LINC Director by the approved LINC Project end date. The LINC Data Recipient agrees not to retain any LINC Project Data, or any parts thereof, or any derivative files that can be used in concert with other information after the aforementioned file(s) and LINC Project Data are destroyed unless the LINC Review Committee grants written authorization. The LINC Data Recipient acknowledges that such date for retention of LINC Project Data is not contingent upon action by OIT.

12. Term and Termination

By signing this DUL, the LINC Data Recipient agrees to abide by all provisions set out in this DUL. This DUL will become effective upon the last date of execution by OIT and the LINC Data Recipient to this DUL. Unless terminated sooner pursuant to Sections 6 and 8 above, this DUL will remain effective in its entirety until the completed "Certification of Project Completion & Destruction or Retention of Data" has been received by the OIT.

[*Remainder of this page left intentionally blank*]

13. Signature

The effective date of the DUL shall be _____. The DUL will remain in effect until _____.

IN WITNESS WHEREOF, the Party hereto have caused this Agreement to be executed by their duly authorized representative.

[NAME]

_____ Dated: _____

[TITLE]

[ORGANIZATION]

Attachment 1:

Linked Information Network of Colorado (LINC)

Certification of Project Completion and Data Destruction

The LINC Data Use License (DUL) signed by _____ ("Data Recipient") on _____ date for LINC Project #_____ allowed for the receipt of anonymized LINC Project data during the project period. The Principal Investigator (PI) and/or Co-Principal Investigator (Co-PI) identified in the LINC DUL is required to destroy all data provided for the approved LINC Project by the end date of the project specified in the LINC DUL. In the DUL, the LINC Data Recipient agreed not to retain any LINC Project Data, or any parts thereof, or any derivative files that can be used in concert with other information after the aforementioned file(s) and LINC Project Data.

By signing below, the PI or Co-PI assures that all data elements loaned to the authorized personnel listed in the DUL for LINC Project #19-01 have been destroyed in accordance with the "Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals," as established by the U.S. Department of Health and Human Services (HHS). The details of data destruction are as follows:

1. Data destruction date:
2. Data destruction personnel:
3. Data destruction method:

Signature: _____ Date: _____

LINC Project #_____

PI/Co-PI Name: _____

Organization: _____

Phone Number: _____ Email address: _____

Address: _____

Please send the signed and completed form to:
Val Henderson, Project Specialist (val@coloradolab.org)