Charlotte Regional Data Trust Governance Documents Overview

TO REVIEW PRIOR TO SIGNATURE:

Enterprise Memorandum of Understanding (EMOU): Represents the agreement between UNC Charlotte and the Data Trust. The EMOU documents the shared Data Trust mission, purpose, and governance process. The EMOU references and appends the Security Policy, references the Data Sharing Agreement and the Data Use License, and it defines key governance terms. Data Partners sign a Joinder to the EMOU upon entering the Data Trust collaboration.

Data Sharing Agreement: The Data Sharing Agreement (DSA) describes the terms of data sharing with each Data Partner and is signed by both the Data Trust and the Data Partner. DSAs may include additional negotiated language specific to the organization and partnership. DSAs may also be project-specific without ongoing data storage.

OTHER DOCUMENTS REFERENCED:

Security Policy: Describes the Data Trust security and privacy agreements and procedures, including the incorporation of the latest data security advancements (use of cloud technology, for example). The Policy is referenced and appended in both the EMOU and the DSA. Any future changes in the Policy will be reviewed by DAROC and approved by the Board of Directors, if acceptable. All data sharing partners will be notified in writing of any approved changes to the Policy.

Confidentiality Agreement: References and appended in the DSA. Documents the responsibility of Data Trust staff to maintain confidentiality. Signed by Data Trust staff

Data Use License (DUL): Outlines the legal terms of data use by approved data recipients and researchers. It describes researcher roles and responsibilities including the appended approved data license request specifying objectives, methods, data security plan, and timeline. The DUL is acknowledged by the research team for each approved project and is signed by the entity where the research team is employed. The DUL also requires a signed data destruction form that is appended to the DUL at the completion of the project.

Review Prior to Signature:

Enterprise Memorandum of Understanding

Charlotte Regional Data Trust

Enterprise Memorandum of Understanding

1. Preamble

The University of North Carolina at Charlotte Institute for Social Capital, Inc. d/b/a Charlotte Regional Data Trust ("Data Trust") was founded in 2004, and became a signature research initiative of the UNC Charlotte Urban Institute in March 2012. The Data Trust receives administrative data from multiple community data partners, securely integrates the data, and deidentifies it for approved research use by partner agencies, university researchers and other approved end-users. The Data Trust uses integrated administrative data to increase the community's capacity for data-informed decision-making and foster university research that impacts the community and deepens understanding of complex community issues. By linking data across agencies, sectors, and programs, the Data Trust integrated data system allows community stakeholders to understand challenges and opportunities beyond typical service silos.

The Data Trust was founded by a group of community stakeholders including UNC Charlotte, Charlotte-Mecklenburg Schools, the Foundation for the Carolinas, Mecklenburg County Department of Social Services, and the United Way of Central Carolinas. It was incorporated in 2005 as a 501(c)3 organization and a subsidiary of the UNC Charlotte Foundation. The Data Trust is governed by a board of community and university stakeholders and staffed by UNC Charlotte personnel. Through its affiliation with UNC Charlotte and the UNC Charlotte Urban Institute, The Data Trust also offers analytical support to assist organizations in their research and data analyses efforts and connects the community to the expertise of faculty researchers.

The fragmentation and diffusion of data is one of the most significant barriers community organizations and researchers must overcome to accurately understand community problems and tailor effective solutions. The Data Trust creates the capacity to integrate fragmented community data for citizen and community benefit. Benefits for the community include a deeper and more nuanced understanding of multifaceted issues that span organizational and institutional silos, the capacity to understand the impact of an intervention across organizations and institutions, the ability to identify areas where organizations can work better together to better intervene or prevent persistent community challenges, and the ability to track nuanced data and outcomes over time.

This Enterprise Memorandum of Understanding ("EMOU") documents the shared understanding of The Data Trust's purpose and facilitates data-driven, cross-system collaboration that shields against disclosure of protected data in compliance with all federal and state laws and regulations including, but not limited to, the Family Educational Rights and Privacy Act ("FERPA"), the Health Insurance Portability and Accountability Act ("HIPAA"), and the Federal Policy for the Protection of Human Subjects (the "Common Rule").

The EMOU is a part of a suite of documents that guide the use and protection of data at The Data Trust. Other documents include the Data Sharing Agreement that specifies the specific terms and conditions for sharing data, the Data Trust Security Policy that guides the protection and privacy of Data Trust data, the Data Use License that specifies the use of Data Trust data for approved projects, and Certification of Project Completion and Destruction of Data form that is required to complete the Data Use License. The governance framework ensures that Data Trust protects sensitive information and accomplishes its purpose, creating benefits for the community and the common good.

2. Parties

This EMOU is made among the Data Trust, UNC Charlotte, and entities executing a joinder in the form of Exhibit A hereto (each such entity, a "Data Partner"). The Data Trust, UNC Charlotte, and Data Partners may each be referenced herein individually as a "Party," or collectively as the "Parties." Execution of the joinder does not constitute an amendment to the EMOU; its sole effect is to add an additional entity as a Data Partner and bind such entity to the terms of the EMOU in their entirety.

3. Definitions

A. Confidential Data: Data submitted by a Data Partner that contains personal identifiers defined in an applicable Data Sharing Agreement.
B. Critically Evaluative: Research is deemed to be Critically Evaluative if a primary purpose or a reasonable consequence of that research is evaluation of the effectiveness of a Data Partner, rather than evaluation of the overall well-being of individuals or effectiveness of intervention strategies and approaches more broadly.
C. Data and Research Oversight Committee or "DAROC": A committee of the Data Trust Board consisting of one or more representatives from the Data Trust, UNC Charlotte, and Data Partners. The purpose of DAROC is to review Data License Requests and prevent the disclosure of Confidential Data. Each Data Partner has the right to participate in the DAROC review of any request for data or reports that include that Data Partner's data.
D. Data License Request or "DLR": A request to conduct a Data Trust Project utilizing data integrated by the Data Trust.
E. Data Sharing Agreement or "DSA": An agreement between each Data Partner and the Data Trust that documents the specific terms and conditions for sharing Confidential Data for integration in the Data Trust Database and/or for deidentified use in an approved Data Trust Project. A Business Associate Agreement ("BAA") is a type of DSA. The Party contributing Confidential Data will determine whether a BAA is the preferred type of DSA.
F. Data Use License or "DUL": An agreement between the Data Trust and a Data Trust Data Recipient that outlines the role and responsibilities of the Data Trust Data Recipient. The DUL shall include the Data Trust Project objectives, methodology, data description, data security plan, completion date (if applicable), reporting requirements, dissemination

plan, data privacy requirements, and terms for data destruction. The Data Trust will be responsible for transferring Deidentified Data for any Data Trust Project to the approved Data Trust Data Recipient under the terms of an applicable DUL. A standard DUL with terms will be approved by the Data Trust Board and updated as necessary.

G. Deidentified Data: Data that has been deidentified by removing elements 1-6 of Personally Identifiable Information, as such term is defined herein.
H. Data Trust Board: The Board of Directors of the Data Trust, which is composed of designated Party representatives charged with defining and protecting the mission of the Data Trust. Responsibilities of the Data Trust Board include appointing members of DAROC, setting priorities for Data Trust Projects, and reviewing/approving the fee structure used for Data Trust Projects when applicable.
I. Data Trust Data or Database: The data or database developed by the Data Trust through its processes of formatting, merging, or cleansing data received from Data Partners.
J. Data Trust Data Integration Staff: Data Trust or UNC Charlotte employees or contractors who will have the approved responsibility of handling and securing relevant Confidential Data from Data Partners for an approved Data Trust Project. The Data Trust Data Integration Staff will consult with Party staff, oversee data integration, and ensure data deidentification in accordance with the Data Trust Security Policy. All Data Trust Data Integration Staff, as with any other Data Trust staff or contractors with access to Confidential Data, will be required by Data Trust to execute non-disclosure agreements.
K. Data Trust Data Recipient: The individual or organization that makes a request to Data Trust for data analysis, research, or evaluation purposes. The Data Trust Data Recipient may be a Party employee or an external researcher. The Data Trust Data Recipient must have an executed Data Use License.
L. Data Trust Executive Director: The individual who is responsible for facilitating meetings of the Data Trust Board and its various committees, developing and managing partnerships with Parties, supporting Data Trust staff, consulting with Data Trust Data Recipients, monitoring Data Trust Projects, and managing the inventory of documents associated with Data Trust operations and Data Trust Projects.
M. Data Trust Project: A project approved by DAROC through a Data License Request. A Data Trust Project must be analytic, research, or evaluative in nature. A Data Trust Project must be achievable by Data Trust Data Recipients with Deidentified Data, unless informed consent is in place for all individuals included in the analysis or all parties whose data are involved have agreed to share data for the particular project as evidenced by legal agreement.
N. Data Trust Security Policy: The Data Trust Security Policy sets forth the information security controls implemented by Data Trust to maintain the confidentiality of Confidential Data and preserve the confidentiality, integrity, and availability of the Data Trust Database and ensure appropriate deidentification protocols and procedures. A copy of the current Data Trust Security Policy is attached as Exhibit B hereto. The Data Trust Security Policy is subject to revisions designed to enhance existing controls. Data Partners will be notified in advance of any revision to the Data Trust Security Policy.
O. Metadata: Information about the data deposited by Data Trust partners and managed by Data Trust staff. Metadata may be descriptive (to understand a variable),

administrative (to manage data), or structural (to understand relationships among data). Metadata may be submitted by data partners or developed Data Trust staff as part of its operational processes. Metadata that could be used to re-identify data will be considered sensitive and will be managed according to the Data Trust Security Policy.

P. Personally Identifiable Information or "PII": PII means data that include any of the following: (1) then name of an individual or that individual's parents or guardians, (2) social security number, (3) specific home address, (4) driver's license number, (5) student identification number, (6) client or other personal identification number, or (7) a list of personal characteristics or other information that would make the individual's identify easily traceable.

Q. UNC Charlotte: The University of North Carolina at Charlotte, an institution of higher education. Data Trust is not part of UNC Charlotte, but rather exists and operates independently as a supporting "associated entity." As an associated entity, Data Trust receives financial, administrative, and personnel support from UNC Charlotte.

4. Justification and Benefits of The Data Trust

The success of the Data Trust depends upon participation of the Parties in the governance framework described in this EMOU as well as usage of shared data integration infrastructure for Data Trust Projects.

The Data Trust uses both a data integration approach and a federated approach, depending upon what is specifically agreed upon in the DSA between the Data Partner and The Data Trust. Under the preferred data integration approach, Data Partners will transfer Confidential Data to the Data Trust for storage in the Data Trust Database. This approach allows data to be more quickly available for partner and community research and it also facilitates regular updates of approved reports and dashboards that are created from the Data Trust's integrated data. Under a federated approach, Data Partners will maintain their own Confidential Data and transfer such data to Data Trust for approved Data Trust Projects based on Data License Requests.

This EMOU does not obligate Data Partners to use the Data Trust in all cases if a different pathway for project approval and data linkage is preferred by Data Partners whose data are requested.

The Parties have concluded that Data Trust improves data sharing by:

- Establishing consistent data sharing and linking processes that adhere to all applicable state and federal laws, rules, and authoritative policies and guidelines
- Limiting the transfer of Confidential Data (as the Data Trust manages the data of several Parties) and transferring data to a single centralized data infrastructure that employs staff with the required expertise and authorization to handle such Confidential Data
- Reducing the burden on Parties' legal counsel and data management teams
- Building capacity for routine cross-system data-driven collaboration and reporting
- Increasing the efficiency of data sharing for cross-system analytic needs

- Reducing respondent burden for research and analytic needs
- Reducing the cost and time that may be required to collect new data
- Taking a person-, household, and/or family-centered approach to data use as opposed to an exclusively institution-centered approach.
- Enabling the long-term collection and use of administrative data to improve knowledge and guide decision-making.

5. Purpose of the EMOU

The purpose of this EMOU is to establish the governance framework necessary to operate the Data Trust, including processes for establishing Data Trust priorities, requesting data, reviewing and determining approval for Data Trust Project requests, monitoring Data Trust Projects, and disseminating Data Trust Project information as appropriate. The governance framework of this EMOU is accompanied by a DSA between each Data Partner and the Data Trust.

6. Financial Understanding

The services of Data Trust will be supported by UNC Charlotte, through a fee-for-use model, and when necessary, through the fundraising function and capacity of the Data Trust Board. The fee-for-use will only be charged to Data Trust Data Recipients. Parties to this EMOU will not be charged to participate in Data Trust unless they are Data Trust Data Recipients. Fees may include the costs incurred by Parties to this EMOU for their efforts to provide data. The fee structure will be developed, monitored, and modified by the Data Trust Executive Director and will be approved by the Data Trust Board prior to implementation. The Data Trust Director and the Data Trust Board will consider similar practices that other integrated data systems and data warehouses employ when developing fee structure, which may include reduced fees to encourage use of data by graduate students, partner research staff and individuals from underrepresented groups. The Data Trust Board retains the legal authority and capacity to engage in discrete or ongoing fundraising activities to support the services and infrastructure of Data Trust.

7. Data Trust Governance Framework

A. Data Trust Project Priorities

There are two ways that priorities will be established for the Data Trust. The first is for each Data Partner to establish criteria for a request of their data to be considered (e.g., federal requirements established for end uses, priority data uses of the Data Partner; restrictions based on project funding sources). The second is for the Data Trust Board to establish cross-system analytic, research, and evaluation topic areas that would benefit from using the shared data infrastructure of the Data Trust. This does not preclude approval of requests that address other project priorities, but the priorities establish the strategic optimization of both data architecture, functionality, and the cultivation of prospective data depositors.

B. Data Trust Project Request Process

The request process is intended to be transparent, efficient, and provide DAROC with the information needed to review a Data License Request. The process is structured to increase the value of Data Trust Project proposals to multiple stakeholders using the expertise of the DAROC to support Data Trust's mission. The request process will consist of two steps: (1) proposed project screening form and (2) submission of a Data License Request to DAROC.

1. Proposed Project Screening: Requestors will be required to complete a screening form on their proposed research project using Data Trust data. The form will help Data Trust staff screen out potential projects that are not appropriate for the Data Trust, including those requests that do not further the Data Trust's mission, cannot be answered through available data, are methodologically problematic, or do not meet ethical standards established by federal statute and the Data Trust board. If the screening form suggests concerns or potential improvements or modifications to the proposed project, requestors will be asked to participate in a phone or in-person consultation with the Data Trust Executive Director (or designee) to discuss their proposed project. At any point, a requestor can ask for a meeting with the Executive Director (or designee) to discuss their project or project development or to receive guidance on how to complete and submit a Data License Request. The Data Trust Executive Director (or designee) will provide the requestor with an estimated fee for the Data Trust Project before the Data License Request is submitted to DAROC.

2. Submission of a Data License Request. The Data License Request form is intended to capture the information DAROC needs to make a decision around appropriate Data Trust Database access and use. The Data License Request is reviewed first by Data Trust staff before final review and approval by DAROC. At minimum, the Data License Request will include:
    a. Purpose (general data analysis, research, or evaluation)
    b. Party sponsor(s) (name and contact information)
    c. Statement of Benefit (individual participants, the primary organizations, the community, and broader society)
    d. Population of study (e.g., age, demographics, geography, years)
    e. Data elements and rationale (specific variables requested and why they are necessary to answer research questions)
    f. Research methodology (background and significance, research questions/hypotheses, research design, sample, and analytic method)
    g. Risks and measures to minimize risks
    h. Dissemination plan
    i. Project start and end date (anticipated release of findings to partners)
    j. Funding source(s) and estimated fee for the project
    k. Key personnel and their credentials including confirmation of human subjects research training
    l. If applicable, IRB approval (or submission date)
    m. Data management and security plan that meets minimum requirements for Deidentified Data

C. Data License Request Review and Decision Process

The review process is intended to simultaneously review and strengthen Data Trust Project proposals. After the requestor has completed the initial screening process to ensure the appropriateness of the proposed project and submitted their Data License Request, Data Trust staff will perform an initial review of all submitted Data License Requests as described below.

1. Data Trust staff initial review. The purpose of the initial review is to ensure that only completed requests that have met initial screening criteria are forwarded to DAROC. The initial review will be limited to the following:

    a. Confirming that the Data License Request form is complete (i.e., no blank fields)
    b. Confirming the proposed research methodology is described clearly and comprehensively.
    c. Confirming the sufficiency of the data management and security plan

    Non-responsive requests will be returned with feedback to the requestor with the opportunity to revise and resubmit. Responsive requests will be forwarded to DAROC.

DAROC will make the final decision on the Data License Request (i.e., reject, revise, approve) according to the following guidelines.

2. DAROC review and decision. DAROC will convene at least quarterly, or more frequently as needed, in person or virtually, to review Data License Requests and conduct other DAROC business in a timely and responsive manner. All DAROC members are asked and encouraged to review DLRs, but a comprehensive review is assigned to DAROC members with subject matter or methodological expertise relevant to the particular Data License Request. Assigned reviewers complete the comprehensive review using the review checklist and make a recommendation to DAROC for vote. A DLR requires a 2/3 quorum vote for approval, revise and resubmit, or rejection.

    Each Data Partner will nominate at least one representative to DAROC who will be responsible for reviewing Data License Request proposals for ethical considerations (e.g., benefits versus risk of the Data Trust Project focus area) and methodological considerations (e.g., appropriate data elements and analytic approach).

    Data Partners have veto power over the use of their own data only. When invoking veto power, Data Partners must provide a clear rationale for why their data cannot be used for the request or may provide alternative data options to meet needs of the Data License Request. The Requestor will have the opportunity to resubmit the Data License Request with the alternative options. DAROC members will be given the opportunity to offer solutions to address the reason for the veto during the meeting and via virtual platforms. If there is no solution that addresses the reason for the veto to the satisfaction of the Data Partner, the veto will stand.

Data Trust staff will communicate DAROC schedules and require requestors to be available to answer questions during the meeting, either virtually or in person. The specific review procedures will be approved and monitored by DAROC and allow reasonable flexibility for virtual participation, proxy membership, and email voting. Key steps in the process include:

a. Upon receipt of a Data License Request assignment, assigned DAROC members will complete a standard Data License Request review rubric and will make an initial recommendation of reject, revise, or approve. The assigned DAROC members will submit the completed review rubric to Data Trust staff. The expectation is that DAROC members will have consulted, as appropriate, within their organization prior to the meetings or bring to the meeting organization representatives necessary to make a fully informed decision.

b. Once every assigned DAROC member has submitted the review rubric, Data Trust staff will synthesize the initial review information from DAROC members and send to the full DAROC membership and the Data Requestor.

c. All standing members of DAROC appointed by the Data Trust Board consistent with DAROC policy and Data Partners that have data being requested for a Data Trust Project proposal will have one vote each. Decisions on Data License Requests will be made by majority vote and result in one of the following determinations:

   Approve: Does not require substantive changes or clarification to the proposal. DAROC may require minor changes or offer suggestions to strengthen the project proposal. The proposal does not need to return to the full committee, and the Data Trust Executive Director (or designee) can oversee the required changes and update DAROC accordingly.

   Revise and Resubmit: Requires changes or clarification to the proposal that necessitate further consideration by DAROC. DAROC will typically consider revised proposals upon submission within a designated time period. Expedited reviews of revised proposals can occur at DAROC's discretion.

   Reject: The potential benefits of the Data Trust Project proposal do not outweigh identified concerns or flaws. A decision by DAROC to reject a Data License Request is final and there is no appeal process.

d. In addition to majority approval, approval must be given unanimously by Data Partners with data included in the Data License Request. Should one or more Data Partners reject a request of their data, the Data License Request can be revised to remove the data that was not approved and resubmitted.

e. The Data Trust Executive Director (or designee) will send DAROC and Data Trust Board members a summary of Data Trust Project decisions. The Data Trust Executive Director will consult as needed with the Data Trust Board to prioritize Data Trust Project timelines.

f. The Data Trust Executive Director (or designee) will send a written notice (email or letter) to the requestor conveying the decision, synthesizing reviewer comments, and outlining next steps (if applicable). A timeline and final cost estimate shall also be provided for approved Data Trust Projects.

D. Data Management Process

The following Data Management Process applies only to approved Data License Requests. All aspects of the Data Management Process are initiated by Data Trust staff, with specific roles referenced below when applicable.

1. The Data Trust will execute a DUL with the Data Trust Data Recipient. The DUL will specify data security requirements, the cell suppression policy for public dissemination (e.g., reports, presentations, publications), status reporting requirements, and will conform to any and all Party-specific requirements. Each investigator on the project will be required to acknowledge the their obligations under the DUL in writing.

2. Data Trust Data Integration Staff will follow the terms of the DSA(s) with Data Partners whose Confidential Data are included in the Data License Request. The process for electronically retrieving or transferring approved Confidential Data to the Data Trust Database may vary by Data Partner and is detailed in the DSA(s). The expectation is that if data is not already held within the Data Trust Database, approved Confidential Data will be provided to the Data Trust within 30 days of Data License Request approval. Parties will alert the Data Trust Executive Director during the DAROC meeting if the 30-day timeline is not feasible.

3. Data Trust Data Integration Staff will adhere to all applicable state and federal laws, rules, and authoritative policies and guidelines for training and authorization to handle the Confidential Data from participating Parties. The Data Trust Data Integration Staff will be responsible for securely receiving and storing Confidential Data from each Party as outlined in the DSA(s) and the Data Trust Security Policy. Metadata received by partners and developed by Data Trust staff will also be managed in accordance with the Data Trust Security Policy.

4. Deidentification processes will be developed by the Data Trust consistent with minimum requirements of the Data Trust Security Policy, reviewed by DAROC, and approved by the Board. The Data Trust Executive Director will confirm that the deidentification approach is consistent with DAROC's approved deidentification approach for Data Trust Projects as well as relevant DSAs. In all cases, Data Trust Projects will use the minimum required Confidential Data to achieve the approved goals.

5. Data Trust Data Integration Staff will securely transfer the Deidentified Data to the Data Trust Data Recipients under the agreed upon terms of the DUL.

6. Through the duration of active research projects, the Data Trust Data Recipient will submit progress reports to DAROC annually or at the midterm point of the project cycle, whichever comes first to Data Trust staff , who will communicate progress to DAROC and the Data Trust Board.

7. After completion of the project, the Data Trust Data Recipient will complete a final report, destroy data as required by the terms of the DUL, and acknowledge destruction of the data by signing and returning the Data Destruction Form appended to the DUL.

8. The Data Trust will always comply with federal and state laws and will default to sharing Deidentified Data only with approved Data Trust Data Recipients.

E. Oversight of Data Trust Projects

Oversight processes for Data Trust Projects are intended to facilitate transparency and mutualism. Transparency ensures that all stakeholders have information about compliance with legal and ethical requirements as well as the outcome of projects. Mutualism refers to all Data Partners, Data Trust staff and Data Trust Data Recipients having consistent and timely communication to ensure that Data Trust Projects further the Data Trust's mission.

Should a Data Trust Data Recipient use data for purposes that were not approved, the Data Trust will take steps to immediately terminate access to such data. It is the responsibility of the Data Trust Executive Director to communicate and confirm this terminated access.

The Data Trust Executive Director (or designee) will monitor timely completion of progress reports, final reports, and data destruction forms. Data Trust Data Recipients shall initiate on an as-needed basis change reports and project updates.

1. Progress Reports: Data Trust Data Recipient must provide progress reports as required by DAROC policy or as otherwise requested by DAROC.

2. Data License Request Amendments : Data Trust Data Recipients will initiate, when necessary, amendments to Data License Requests. Minor requests (e.g., change in key personnel, a first-time extension of up to six months) will be reviewed by the Data Trust Executive Director or staff designee. Major requests (e.g., additional research questions; change in organization conducting analyses) will be reviewed by DAROC. Data Trust staff will maintain records of all approved Data License Request amendments.

3. Pre-Publication Reports: Data Trust Data Recipients will share a pre-publication report of Data Trust Project findings with DAROC prior to any public release as required by DAROC policy. Pre-publication reports will consist of the final draft of any presentation or manuscript to be submitted for publication and should be provided in electronic format. DAROC members who represent Data Partners will be provided an opportunity

to respond to a pre-publication report deemed Critically Evaluative of the Data Partner they represent in accordance with DAROC policy. Where inappropriate use and/or inaccurate data, data analyses, or conclusions are alleged by a Data Partner, the Data Partner can appeal to the Data Trust Board to review the request, analysis, and results. Inappropriate use of data by Data Trust Data Recipients may result in withdrawal of permission to use the Data and/or denial of future Data License Requests. All reports and presentations that use Data Trust data will be required to include a standard acknowledgement.

4. Project Updates and Announcements: During the study period, Data Trust Data Recipients will be required to notify staff of any newly released products, media coverage, or announcements pertaining to the use of Data Trust data. This information will be routinely collected as a part of annual progress reports, or more frequent reports if required by the DUL. After the study period, the Data Trust Data Recipient will be encouraged to initiate project updates or announcements and Data Trust staff will make efforts to track ongoing references to the use and impact of Data Trust data. Data Trust Data Recipients agree to this as a part of the DUL.

5. Data Destruction Forms: This is a standard form automatically distributed by the Data Trust to Data Trust Data Recipients that confirms data destruction consistent with the DUL following completion of an Data Trust Project.

8. Counterparts.

This EMOU may be executed in one or more counterparts, each of which shall be considered to be one and the same agreement, binding on all Parties hereto, notwithstanding that all Parties are not signatories to the same counterpart. Furthermore, duplicated signatures, signatures transmitted via facsimile, or signatures contained in a Portable Document Form (PDF) document shall be deemed original for all purposes.

9. EMOU Effective Date and Terms.

The effective date of the EMOU shall be July 23, 2021 . The EMOU will remain in effect until the Data Trust Board terminates the EMOU. An individual Party to the EMOU can end its involvement upon a termination request from an authorized representative. Termination halts all future Data License Requests for that Party's data, but Data Trust Projects approved prior to termination will continue.

10. Amendment.

The Data Trust may amend this EMOU by giving notice to all Parties, subject to the following conditions:

a. The amendment will take effect at the specified time after the effective date of the notice.

b. No amendment will retroactively amend any terms of the EMOU or affect the confidentiality of any Confidential Data.

c. Any Party, upon receipt of Data Trust's notice of amendment, may elect to terminate the EMOU pursuant to Section 9 above.

IN WITNESS WHEREOF, the Parties hereto have caused this EMOU to be executed by their duly authorized representatives.

The University of North Carolina Institute for Social Capital, Inc. d/b/a Charlotte Regional Data Trust

_____ Date: 8/9/2021

Dr. M. Lori Thomas, Executive Director

The University of North Carolina at Charlotte

_____ Date: 8/9/2021

Dr. Joan F. Lorden, Provost and Vice Chancellor for Academic Affairs

EXHIBIT A

Joinder Agreement

Pursuant to, and in accordance with The University of North Carolina at Charlotte Institute for Social Capital, Inc. d/b/a Charlotte Regional Data Trust Enterprise Memorandum of Understanding (EMOU), effective July, 23, 2021 as may be amended from time to time, the entity signing this Joinder Agreement (the "New Party") hereby acknowledges that it has received and reviewed a complete copy of the EMOU. The New Party agrees that upon execution of this Joinder, it will become a Data Partner and Party as such terms are defined in the EMOU and will be fully bound by and subject to all of the terms and conditions of the EMOU.

In witness thereof, the New Party has caused its duly authorized representative to execute this Joinder Agreement, as follows:

[New Party's Name]

By: _____
[Name of Signing Official, Title]

Date: _____

Charlotte Regional Data Trust

Data Sharing Agreement

1. Preamble

This Data Sharing Agreement ("DSA") is made among The University of North Carolina at Charlotte Institute for Social Capital, Inc. d/b/a Charlotte Regional Data Trust ("Data Trust"), the University of North Carolina at Charlotte ("UNC Charlotte"), and _____ ("Data Partner"), and is effective as of the last date of signature shown below (the "Effective Date"). Data Trust, UNC Charlotte, and Data Partner may each be referenced herein individually as a "Party," or collectively as the "Parties." Unless otherwise defined in this DSA, capitalized terms herein without definition will have the same meanings as those defined in the Enterprise Memorandum of Understanding ("EMOU") signed by the Parties, a copy of which is attached as Exhibit A and incorporated herein by reference.

As provided in the EMOU, this DSA describes the specific terms and conditions for sharing Confidential Data for integration in the Data Trust Database and/or for deidentified use in an approved Data Trust Project. In the event of a conflict between this DSA and the EMOU, the EMOU will control.

2. Transfer of Data from Data Partner to the Data Trust

Data Partner will submit to the Data Trust, or otherwise permit Data Trust Data Integration Staff to electronically access, Confidential Data for integration into the Data Trust Database or as required for approved Data Trust Projects in accordance with the EMOU. If Data Partner is transmitting Confidential Data to Data Trust (as opposed to providing access for downloading), Confidential Data must be transmitted electronically only via encrypted files.

3. The Data Trust's Rights to Share/Redistribute the Data

Except as expressly provided in this DSA and the EMOU (including any Data Use License issued under the EMOU), any data submitted to Data Trust by the Data Partner will not be further distributed without Data Partner's written approval.

4. Data Storage, Access, Use, and Destruction

Data Trust will comply with the following data storage, access, use, and destruction requirements:

a. Storage and Access. The Data Trust will store and limit access to Confidential Data as provided in the Data Trust Security Policy.

b. Use. The Data Trust shall use the Confidential Data solely for purposes approved through the EMOU. Data Trust shall only disclose Confidential Data to Data Trust Data Integration Staff who have the authority to handle the data in furtherance of such purposes, and will only provide approved Data Trust Project Data to Data Trust Data Recipients who have signed Data Use Licenses in accordance with the EMOU.

c. Data Destruction. The Data Trust will return or destroy Data Partner's Confidential Data within ninety (90) days of termination of the EMOU; provided, however, that termination will not affect any Data Trust Projects approved prior to the date of termination. Confidential Data provided by Data Partner specifically for an approved Data Trust Project will be retained for a period of twelve months after providing Deidentified Data to the Data Trust Data Recipient, unless otherwise agreed by Data Partner and the Data Trust. After this twelve-month period unless otherwise extended via a Data License Request Amendment, all Confidential Data and Deidentified Data related to the Data Trust Project will be deleted.

5. Deidentification of Data Trust Project Data

a. Criteria for Deidentified Data. Only Deidentified Data may be released to Data Trust Data Recipients for approved Data Trust Projects.

b. Cell Suppression Policy. The Data Trust agrees that Data Trust Projects including data from the Data Partner in the creation of any dissemination materials (manuscript, table, chart, study, report, presentation, etc.) must adhere to the following cell suppression policy unless otherwise agreed by Data Partner and the Data Trust for an approved Data Trust Project. This policy stipulates that no cell (e.g., grouping of individuals, patients, clients) with less than 10 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 10 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 10 observations cannot be identified by manipulating data in adjacent rows, columns or other manipulations of any combination of dissemination materials generated through Data Trust Projects. Examples of such data elements include, but are not limited to, geography, age groupings, sex, or birth or death dates.

6. Data Partner Responsibilities for Meeting Legal Requirements

Data Partner has collected the Confidential Data from individuals. Accordingly, Data Partner 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 Trust.

7. Confidentiality and Breach Notification

a. Confidentiality. All Data Trust Data Integration Staff shall be informed of the confidentiality obligations imposed by this DSA, the EMOU, and the Data Trust Security Policy, and must agree to be bound by such obligations prior to disclosure of Confidential Data to Data Trust Data Integration Staff, as evidenced by their signature on an Data Trust Confidentiality Agreement substantially in the form set forth on Exhibit B hereto.

b. Breach Notification. Data Trust is responsible and liable for any breach of this DSA by any of its Data Trust Data Integration Staff. The Data Trust will report to the Data Partner all breaches that result in the exposure of Confidential Data protected by federal or state laws. Such reports shall be made to the Data Partner within 24 hours

from when the Data Trust discovered or should have discovered the occurrence. Data Trust shall also comply with any applicable law regarding data breaches, including but not limited to the North Carolina Identity Theft Protection Act (N.C. Gen. Stat. § 75-60 *et seq*.).

8. 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, each of 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. This DSA supersedes all previous data sharing agreements among the Parties, whether oral or in writing.

9. 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 Confidential Data unless the Data Partner agrees and approves of this obligation under the terms of the EMOU. Nothing in this DSA obligates the Data Partner to enter into any further agreement or arrangements, or furnish any Confidential Data, other information, or materials.

10. Compliance with Law, Applicable Law

The Parties agree to comply with all applicable laws and regulations in connection with this DSA. The Data Partner and the Data Trust agree that this DSA shall be governed by the laws of the State of North Carolina, without application of conflicts of laws principles.

11. Counterparts.

This DSA may be executed in one or more counterparts, each of which shall be considered to be one and the same agreement, binding on all Parties hereto, notwithstanding that all Parties are not signatories to the same counterpart. Furthermore, duplicated signatures, signatures transmitted via facsimile, or signatures contained in a Portable Document Form (PDF) document shall be deemed original for all purposes.

12. Term of DSA

Any 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 Confidential Data provided, and performance of this DSA, prior to the date of termination, including Sections 2, 3, 4, 5, 6, 7, 8, 9, and 10.

13. Use of Name

Neither the Data Partner nor Data Trust 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.

14. Party Representatives

The Parties' contacts for purposes of this Agreement are:

For Data Partner:

[Executive Name]
[Title]
[Address]
[Phone]
[Fax]
[Email]

For UNC Charlotte and the Data Trust:

M. Lori Thomas, PhD, MSW, MDiv
Executive Director
Institute for Social Capital
d/b/a Charlotte Regional Data Trust
9201 University City Boulevard
Charlotte, NC 28223
Phone: 704.687.7037
Fax: 704.687.5327
Email: LoriThomas@uncc.edu

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

The University of North Carolina at Charlotte Institute for Social Capital, Inc.
d/b/a Charlotte Regional Data Trust

_____ Date: _____
Dr. M. Lori Thomas, Executive Director

The University of North Carolina at Charlotte

_____ Date: _____
Dr. Jennifer Troyer, Provost and Vice Chancellor for Academic Affairs

[Data Partner]

_____ Date: _____
[Name of Signing Official, Title]

Other Referenced Documents:

Security Policy

Charlotte Regional Data Trust Security Policy

1. Executive Summary and Definitions

Data and information are a critical resource for the operation of the Institute for Social Capital, Inc. d/b/a Charlotte Regional Data Trust("Data Trust"). As such, the Data Trust Security Policy (the "Data Trust Security Policy" or this "Policy") outlines the minimum protections for information within the Data Trust. Much of the data and information within Data Trust is confidential, personally identifiable, and sensitive healthcare and education information that may be subject to HIPAA regulations, FERPA regulations, or other privacy laws, rules, or regulations. Unless otherwise defined in Policy, capitalized terms herein without definition will have the same meanings as those defined in the Enterprise Memorandum of Understanding ("EMOU") signed by Charlotte Regional Data Trust, UNC Charlotte, and all Data Partners.

2. Purpose

The purpose of Policy is to ensure that all individuals and entities interacting and/or sharing data with Data Trust understand their responsibilities to preserve the security, reliability, integrity, and availability of information. This is accomplished by reducing the risk of compromise and taking appropriate security measures to protect Data Trust resources. Access to certain Data Trust information resources is a privilege, not a right, and implies user responsibilities. Such access is subject to the Data Trust, University of North Carolina System, and University of North Carolina at Charlotte policies, standards, guidelines, and procedures, as well as federal and state laws and regulations (collectively, "Applicable Law").

Data deposited into the Data Trust database are maintained and managed in various forms, including the data deposited, the integrated data that retain PII for ongoing linking and integration, and the data that are deidentified for approved data management and research purposes. This policy directs the security of Data Trust data in all forms. Once transferred to an end-user, the security of the Deidentified Data is specified in the specific Data Use License (DUL) and monitored by Data Trust staff.

3. Scope

This Policy applies to individuals, using, accessing, storing, transmitting, or overseeing Data Trust Data or the Data Trust Database. This includes, but is not limited to:

- Faculty, staff, and students
- Affiliates, associates, contractors, and volunteers
- Third-party vendors and third-party researchers

4. Responsibilities

A. The Data Trust Executive Director will have primary responsibility for:

- Oversight of information security
- Implementation and enforcement of this Policy
- Educating the Data Trust community, researchers, and data contributors about information security responsibilities

B. The Data and Research Oversight Committee ("DAROC") may make recommendations on the policies and guidelines regarding the protection of confidentiality of data.
C. The Data Trust Board has responsibility for reviewing and approving this policy and any subsequent changes suggested by the Data Trust Executive Director or DAROC.

5. Security Policies

A. Limited Access. The Data Trust will limit access to Confidential Data to Data Trust Data Integration Staff who have signed a non-disclosure agreement and who are working on an Data Trust Project or an authorized purpose under the terms of the EMOU. Researchers and end-users of Data Trust Data must have an executed Data Use License ("DUL") to access Deidentified Data as described in the EMOU.

B. Secure Storage. Partner data deposited in the Data Trust integrated data system and integrated data that retain PII are Confidential Data and considered Level 3 (Highly Restricted) Data pursuant to UNC Charlotte's Standard for Information Classification (the "Standard"). Deidentified Data sets created for research purposes are considered Level 2 sensitive data pursuant to UNC Charlotte's guidelines. Confidential Data, and Deidentified Data will be stored consistent with the Standard and its accompanying guidelines, including the Guideline for Data Handling, the Guideline for Data Security in Cloud Services, Guideline for the Security of Endpoints, and the Guideline for Research Data Security as appropriate. UNC Charlotte adopted the ISO/IEC 27002 cybersecurity framework in 2012, and the Standard and all accompanying guidelines are rooted in this code of practice for information security management. Consistent with the Standard, Data Trust commits to:

- Isolating servers and workstations that store and access any Data Trust integrated data that retain PII to a HIPAA VLAN or storing such data only in cloud storage locations that are HIPAA compliant.
- Encrypting and password-protecting any device used to access or transfer Confidential Data or Deidentified Data.
- Encrypting Confidential Data and Deidentified Data transferred to or from external networks.
- Regularly auditing account ownership and permissions to ensure appropriate access.
- Following UNC Charlotte's Standard for Account Passwords for all accounts.
- Using UNC Charlotte-approved antivirus software on computers storing or accessing Confidential Data or Deidentified Data.

- Enabling screensavers after 15 minutes of inactivity and prompting for login when the screensaver has been activated.
- Providing all users with the lowest necessary level of access to Confidential and Deidentified Data.
- Storing Confidential Data only on UNC Charlotte managed servers or using appropriate UNC Charlotte cloud storage providers and never storing on local hard drives.

C. Use. Data Trust will use Confidential Data solely for purposes authorized by the EMOU. The Data Trust will disclose Confidential Data only to Data Trust Data Integration Staff who have the authority to handle the data in furtherance of such purposes. Data Trust will provide Deidentified Data only to designated Data Trust and UNC Charlotte staff for data management purposes and to those Data Trust Data Recipients who have signed an approved DUL.

D. Access Controls. Confidential Data (Partner Data and Personally Identifiable Data) will only be accessible to designated Data Trust Data Integration Staff. Deidentified Data for data management purposes and for approved data license requests will be accessible by only approved Data Trust staff and end-users who have a fully executed DUL. Access controls are pursuant to UNC Charlotte's Standard for User Access Management and the Guideline for User Access Management

E. Data Destruction. Data destruction will be defined by individual Data Sharing Agreements and Data Use Licenses with approved investigators. All data subject to destruction will be disposed of consistent with UNC Charlotte's Standard for Hardware and Media Disposal and associated guideline.

6. Exceptions

Exceptions to this Policy require approval of the Data Trust Executive Director, DAROC, and the Data Trust Board.

7. Policy Improvements

A. The Data Trust Executive Director and DAROC may propose policy changes that improve the security of data, including Confidential Data, but may not decrease the protection of Confidential Data.

B. Changes in this policy must be approved by the Data Trust Board.

C. Data Partners will be notified in writing of policy or guidelines changes prior to the effective date of such changes.

Other Referenced Documents:

Confidentiality Agreement

Confidentiality Agreement

Name: _____

Job Title: _____

Email Address: _____

Supervisor: _____

I acknowledge that through my normal duties with the UNC Charlotte Urban Institute (Institute), including, but not limited to, my participation in externally funded projects as well as in the day-to-day operations of the department, I may have either direct or indirect access to data derived from confidential files supplied by clients and colleagues as well as other sensitive information from many sources including the UNC Charlotte Urban Institute, University administration, and associated entities of the University including the Charlotte Regional Data Trust.

I am aware of restrictions on the use and disclosure of project related data as regulated by data sharing agreements, memoranda of understanding and data security plans executed on behalf of a particular project and/or client. I understand that all information related to projects should be treated as "Confidential Information" unless I am otherwise informed by my supervisor or Institute program manager(s).

With regard to research project data:

- I will use data only for the research purposes set forth in the proposal.
- I will not attempt to identify individuals, families or households within data that has been de-identified.
- In the event that the identity of any individual, family or household is discovered inadvertently, I will:
    - Make no use of this information.
    - Inform the Lead Principal Investigator of this discovery immediately.
- I will never release data to anyone who has not been authorized to receive the data.
- I will never report results in a way that could permit inadvertent disclosure of an individual.
- I will make best efforts to follow outlined and approved protocol, executed data security plans and all other contracts and agreements associated with a project and/or client.

"Confidential Information" also includes any and all business and technical information including information relating to the design, creation, building, revising, and maintaining of the Charlotte Regional Data Trust database. Data contained in the Charlotte Regional Data Trust database are

trade secret information as defined by N.C. Gen. Stat. § 66-152, and unauthorized access, storage, or disclosure of such data may result in addition legal and contractual penalties.

I understand that any violation of this Agreement may result in disciplinary action from the University of North Carolina at Charlotte and/or the UNC Charlotte Urban Institute.

Signed	Date
Print Name	

Other Referenced Documents:

Data Use License

Charlotte Regional Data Trust

Data Use License

1. Preamble

This Data Use License ("DUL") is made by and between The University of North Carolina at Charlotte Institute for Social Capital, Inc. d/b/a Charlotte Regional Data Trust (the "Data Trust") and _____ ("Data Trust Data Recipient"), and is effective as of the last date of signature shown below (the "Effective Date"). The Data Trust and the Data Trust Data Recipient may each be referenced herein individually as a "Party," or collectively as the "Parties."

This DUL addresses the conditions under which the Data Trust will disclose, and the Data Trust Data Recipient may use, Deidentified Data for Data Trust Projects specified in this DUL and/or any derivative file(s) (collectively, the "Data Trust Project Data"). The terms of this DUL are consistent with terms in the Enterprise Memorandum of Understanding ("EMOU") executed by and between the Data Trust, UNC Charlotte, and Data Partners, and can be changed only by a written and signed amendment to this DUL or by the Parties terminating this DUL and entering a new DUL, after approval by DAROC. The Parties agree further that instructions or interpretations issued to the Data Trust Data Recipient concerning this DUL, or the Data Trust Project Data specified herein, may be issued to the Data Recipient in writing by the Data Trust.

2. Definitions

a. Authorized Personnel: The members of the Data Trust Data Recipient team who have been listed in this DUL as having approved access to the Data Trust Project data and have agreed to abide by the terms of this DUL through their signature below.
b. Confidential Data: Data submitted to the Data Trust by a Data Partner that contains personal identifiers or other information identified as sensitive pursuant to an applicable Data Sharing Agreement.
c. Critically Evaluative: Research is deemed to be Critically Evaluative if a primary purpose or a reasonable consequence of that research is evaluation of the effectiveness of a Data Partner, rather than evaluation of the overall well-being of individuals or effectiveness of intervention strategies and approaches more broadly.
d. Data and Research Oversight Committee or "DAROC": A committee of the Data Trust Board responsible for reviewing Data License Requests and preventing the disclosure of Confidential Data. Each Data Partner has the right to participate in the DAROC review of any request for data or reports that include that Data Partner's data.
e. Data Sharing Agreement or "DSA": An agreement between each Data Partner and the Data Trust that documents the specific terms and conditions for sharing Confidential Data for integration in the Data Trust Database and/or for deidentified use in an approved Data Trust Project.

f. Data License Request or "DLR": A request to conduct a Data Trust Project utilizing data integrated by the Data Trust. The DAROC-approved Data License Request is attached and incorporated into this DUL as Exhibit A.
g. Data Partner: An organization that has an active Data Sharing Agreement with Data Trust and has direct responsibility for a source of data contributed to the Data Trust Database and utilized for approved Data Trust Projects.
h. Data Trust Board: The Board of Directors of the Data Trust, which is composed of designated representatives of the Data Trust, Data Partners, and UNC Charlotte, and is charged with defining and protecting the mission of the Data Trust. Responsibilities of the Data Trust Board include appointing members of DAROC, setting priorities for Data Trust Projects, and reviewing/approving the fee structure used for Data Trust Projects when applicable.
i. Data Trust Data or Database: The data or database developed by the Data Trust through its processes of formatting, merging, or cleansing data received from Data Partners.
j. Data Trust Executive Director: The individual who is responsible for facilitating meetings of the Data Trust Board and its various committees, developing and managing partnerships with Parties, supporting Data Trust staff, consulting with Data Trust Data Recipients, monitoring Data Trust Projects, and managing the inventory of documents associated with Data Trust operations and Data Trust Projects.
k. Data Trust Project: A project described in a Data License Request and approved by DAROC that is analytic, research or evaluative in nature. A Data Trust Project requires data from one or more Data Partners and must be achievable by Data Trust Data Recipients with Deidentified Data, unless informed consent is in place for all individuals included in the analysis or all parties whose data are involved have agreed to share data for the project as evidenced by legal agreement.
l. Data Trust Project Data: Data for use by the Data Trust Data Recipient for an approved Data Trust Project. Data Trust Project Data are only to be used for the approved purposes outlined in the approved Data License Request. Data Trust Project Data includes both data from Data Partners and any external data that is merged with Data Partner data for an approved Data Trust Project.
m. Deidentified Data: Data that has been deidentified by removing elements 1-6 of Personally Identifiable Information, as such term is defined herein. Data Partners may establish more restrictive definitions of Deidentified Data in Data Sharing Agreements; the most restrictive definition of Deidentified Data among all Data Partners contributing data to the Data Trust Project related to this DUL will control.
n. Personally Identifiable Information or "PII": PII means data that include any of the following: (1) then name of an individual or that individual's parents or guardians, (2) social security number, (3) specific home address, (4) driver's license number, (5) student identification number, (6) client or other personal identification number, or (7) a list of personal characteristics or other information that would make the individual's identify easily traceable.
o. UNC Charlotte: The University of North Carolina at Charlotte, an institution of higher education. The Data Trust is not part of UNC Charlotte, but rather exists and operates

independently as a supporting "associated entity." As an associated entity, the Data Trust receives financial, administrative, and personnel support from UNC Charlotte.

3. Financial Understanding

If applicable, the Data Trust Data Recipient agrees to pay a fee of $_____ to be invoiced upon secure transfer of the Data Trust Project Data. Payment is expected to be executed within 30 days of receipt of invoice.

4. Permitted Data Trust Project: Approved Use and Data Elements

This DUL pertains to the Data Trust Project entitled: _____. This Data Trust Project was approved by DAROC on _____ (Date) and the approved Data License Request is attached as Exhibit A.

The approved Data License Request details the permitted use of the Data Trust Project Data as well as the approved data elements to be included in the Data Trust Project Data. This DUL pertains only to the use and data elements identified in the approved Data License Request.

The Data Trust Data Recipient will not use the Data Trust Project Data for any purpose independent of, separate from or not directly connected to the purpose(s) specifically approved by DAROC in the attached Data License Request. The Data Trust Data Recipient will only receive Deidentified Data and will not be permitted to receive any Personally Identifiable Information, unless allowable due to informed consent or other permissible use of PII.

5. Data Ownership and Accuracy

The Data Trust Data Recipient acknowledges that it has no ownership rights with respect to the Data Trust Project Data, and that the Data Trust Data Recipient may only receive and use the Data Trust Project Data for the purposes approved by DAROC.

The Data Trust Project Data is current as of the date and time compiled and can change. Although the Data Trust works with Data Partners to continuously improve the quality of Data Trust Data and to document what is known about such data through its ongoing metadata documentation, neither Data Partners nor the Data Trust can ensure 100% accuracy of all records and fields. Some data fields may contain incorrect or incomplete data. Data Partners cannot commit resources to explain or validate complex matching and cross-referencing programs. The Data Trust Data Recipient accepts the quality of the Data Trust Project Data it receives. Questions related to Data Trust Project Data completeness or matching accuracy must be sent to the Data Trust within sixty (60) days of receipt. Data Trust Project Data that has been manipulated or reprocessed by the Data Trust Data Recipient is the responsibility of the Data Trust Data Recipient. The Data Trust cannot commit resources to assist the Data Trust Data Recipient with converting data to another format or answering questions about data that has

been converted to another format. Additional issues with the Data Trust Project Data should be noted in the progress report(s) described in Section 10 below.

6. Data Transfer

Data Trust Project Data will be transferred to the Data Trust Data Recipient through a Secure File Transfer Protocol (SFTP), secure web portal or other secure methods provided or approved by the Data Trust. The Data Trust Data Recipient will be provided secure access to the method of transfer and will be allowed to download the Data Trust Project Data file(s) for a limited period of time after which access will be removed.

7. Safeguarding Data

a. Security Controls. The Data Trust Data Recipient will implement and maintain the data security controls specified in the approved Data License Request (attached as Exhibit A) that has been approved by DAROC.

b. Re-Disclosure of Data. The Data Trust Data Recipient will not use the Data Trust Project Data for any purpose beyond that specified in the approved Data License Request. Furthermore, the Data Trust Data Recipient will not use the Data Trust 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 Data Trust Project. Re-disclosure of Data Trust Project Data will result in the immediate suspension of the Data Trust Project and possible termination of the Data Trust Project by DAROC. Furthermore, individuals engaging in re-disclosure of Data Trust Project Data will not be approved as Authorized Personnel on future Data Trust Projects. UNC Charlotte employees and students are additionally subject to disciplinary action.

c. Cell Suppression Policy. The Data Trust Data Recipient agrees that any use of Data Trust 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 10 observations may be displayed. This is the most stringent cell size allowable among the Data Partners for the Data Trust Project specified in this DUL. Also, no use of percentages or other mathematical formulas may be used if they result in a cell displaying less than 10 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 10 observations cannot be identified by manipulating Data Trust Project Data in adjacent rows, columns or other manipulations of any combination of dissemination materials generated through this Data Trust Project. Examples of such data elements

include, but are not limited to, geography, age groupings, racial identity groups, sex, or birth or death dates.

8. Data Trust Project Authorized Personnel

Any person or entity that processes or receives the Data Trust Project Data must be obligated to adhere to the terms of this DUL and agree to follow the data security controls approved in the attached Data License Request prior to being granted access to Data Trust Project Data. The following named individuals, and only these individuals, will have access to the Data Trust Project Data. The Data Trust Data Recipient will notify the Data Trust in writing when an individual leaves a Data Trust Project. The Data Trust Data Recipient will obtain written approval from the Data Trust for additions to this list prior to granting access to Data Trust Project Data by submitting a Data License Request amendment as described in Section 10 below. By signing this DUL where indicated in the signature page, Authorized Personnel are acknowledging that they understand and will adhere to the terms of this DUL to the same extent as the Data Trust Data Recipient.

Name	Role on project	Organization

Add rows as necessary to include all personnel named in the approved DLR

9. Accountability: Unauthorized Access, Use, or Disclosure

The Data Trust Data Recipient will take all steps necessary to identify any use or disclosure of Data Trust Project Data not authorized by this DUL. The Data Trust Data Recipient will report any unauthorized access, use or disclosure of the Data Trust Project Data to the Data Trust within two (2) days of the date it learned or should have learned of the unauthorized access, use, or disclosure. In the event that the Data Trust determines or has a reasonable belief that the Data Trust Data Recipient has allowed unauthorized access, use, or disclosure of the Data Trust Project Data, the Data Trust may, at its sole discretion, require the Data Trust Data Recipient to perform one or more of the following, or such other actions as the Data Trust, in its sole discretion, deems appropriate:

a. promptly investigate and report to the Data Trust the Data Trust 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 or destroy all Data Trust Project Data it has received under this DUL.

The Data Trust Data Recipient understands that as a result of the Data Trust's determination or reasonable belief that unauthorized access, use, or disclosures have taken place, the Data Trust may refuse to release further Data Trust Project Data to the Data Trust Data Recipient for a period of time to be determined by Data Trust, in its sole discretion, and that the Data Trust Data Recipient will not be entitled to a refund of any fees paid hereunder.

10. Data Trust Project Reporting Requirements

a. Progress Reports. Data Trust Data Recipients must submit progress reports to DAROC annually or at the midterm point of the project cycle, whichever comes first. The report will be a standard form automatically distributed by the Data Trust and will require:
    i. IRB approval documentation, if applicable
    ii. 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
    iii. Dissemination materials and key findings to date
    iv. Newly released products, media coverage, or announcements pertaining to the use of Data Trust Project Data
    v. Project funding source (if applicable)

b. Data License Request Amendments. Data Trust Data Recipients will initiate, when necessary, amendments to Data License Requests. Minor requests (e.g., change in key personnel, a first-time extension of up to six months) will be reviewed by the Data Trust Executive Director or staff designee. Major requests (e.g., additional research questions; change in organization using data; request for additional years of data; change in dissemination plan) will be reviewed by DAROC.

c. Pre-Publication Reports. Data Trust Data Recipients are required to share a pre-publication report of Data Trust Project findings with DAROC at least fourteen (14) business days prior to any public release. Pre-publication reports will consist of the final draft of any presentation or manuscript to be submitted for publication and should be provided in electronic format. DAROC members who represent Data Partners will be provided an opportunity to respond to a pre-publication report deemed Critically Evaluative of the Data Partner they represent in accordance with DAROC policy. Where inappropriate use and/or inaccurate data, data analyses, or conclusions are alleged by a Data Partner, the Data Partner can appeal to the Data Trust Board to review the

request, analysis, and results. Inappropriate use of data by Data Trust Data Recipients may result in withdrawal of permission to use the Data Trust Project Data and/or denial of future Data License Requests.

d. Data Trust Acknowledgement. All publicly-released materials resulting from the Data Trust Project referenced in this DUL must include the following acknowledgement: "This work uses deidentified data provided by the Charlotte Regional Data Trust, in partnership with The University of North Carolina at Charlotte. The findings do not necessarily reflect the opinions of the Charlotte Regional Data Trust, UNC Charlotte, or any of the organizations contributing data."

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

11. Data Retention and Destruction

The Data Trust Data Recipient agrees to destroy all Data Trust Project Data by the approved Data Trust Project end date, 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 U.S. Department of Health and Human Services (HHS). The Data Trust Data Recipient may request an extension of the Data Trust Project end date by submitting a written change request that includes justification to DAROC in accordance with Section 10 above. This extension request must be submitted 30 days prior to the Data Trust Project end date indicated on the approved DLR.

Following destruction of the Data Trust Project Data, but in no event later than the approved Data Trust Project end date, the Data Trust Data Recipient agrees to send a completed "Certification of Project Completion & Destruction of Data" form (Exhibit B to this DUL). The Data Trust Data Recipient agrees not to retain any Data Trust 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 Data Trust Project Data are destroyed unless DAROC grants written authorization. The Data Trust Data Recipient acknowledges that its obligations under this Section 11 are not contingent upon any affirmative action by the Data Trust.

12. Term and Termination

By signing this DUL, the Data Trust Data Recipient agrees to abide by all provisions set out in this DUL. This DUL will become effective upon the Effective Date. Unless terminated sooner pursuant to this DUL, this DUL will remain effective in its entirety until the completed "Certification of Project Completion & Destruction of Data" has been received by the Data Trust.

IN WITNESS WHEREOF, the Parties hereto have caused this DUL to be executed by their duly authorized representatives.

The University of North Carolina Institute for Social Capital, Inc.
d/b/a Charlotte Regional Data Trust

_____ Date: _____
Dr. M. Lori Thomas, Executive Director

[Data Trust Data Recipient]

By: _____ Date: _____

Title: _____

Acknowledged by Authorized Personnel:

Signature: _____ Date: _____

Signature: _____ Date: _____

Signature: _____ Date: _____
Add rows as necessary to include all personnel named in the approved DLR

EXHIBIT A

Approved Data License Request

EXHIBIT B

Certification of Project Completion & Destruction of Data

Data Trust Project title: _____

Data Trust Data Recipient: _____

The Data Use License ("DUL") entered into by the Data Trust Data Recipient identified above allowed for the receipt of deidentified Data Trust Project Data (as such term is defined in the DUL) during the project period. The Data Trust Data Recipient is required to destroy all Data Trust Project Data provided for the approved Data Trust Project by the end date of the project specified in the approved Data License Request for the Data Trust Project. In the DUL, the Data Trust Data Recipient agreed not to retain any Data Trust 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 Data Trust Project Data.

By signing below, an authorized representative of the Data Trust Data Recipient assures that all Data Trust Data loaned to the authorized personnel listed in the DUL for the Data Trust Project 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: _____

[Data Trust Data Recipient]

By: _____ Date: _____

Title: _____

Acknowledged by Authorized Personnel:

Signature: _____ Date: _____

Signature: _____ Date: _____

Signature: _____ Date: _____

Add rows as necessary to include all personnel named in the approved DLR