North Carolina Department of Health and Human Services

Intradepartmental Data Sharing Agreement

1. Preamble

This Data Sharing Agreement ("Agreement"), is by and between Click here to enter text. ("Data Owner"), the North Carolina Department of Health and Human Services ("NCDHHS") Data Office ("Data Office"), and the NCDHHS Information Technology Division ("ITD")and is effective as of the last date of signature shown below (the "Effective Date"). The Data Owner, Data Office, and ITD shall hereinafter collectively be referred to as the "Parties."

WHEREAS, under the authority and direction of the Secretary of the North Carolina Department of Health and Human Services, NCDHHS senior leadership and Data Owners will access and use NCDHHS data assets to enable data driven decision making through a modernized data sharing and IT infrastructure, which is critical to NCDHHS's mission to improve the health, safety, and wellbeing of all North Carolinians;

WHEREAS, the Data Office and ITD ("Data Integration Staff") will act as the data governance, management, and integration agent for the Secretary, NC DHHS senior leadership, Data Owners, Divisions, and Offices across NCDHHS for operational and research data requests that are made to support business intelligence and the work of NCDHHS; and

WHEREAS, Data Owner agrees to share certain data identified within the High Value Data Asset Inventory, in accordance with the terms and conditions of this Agreement and approved under the terms and conditions of the NCDHHS Intradepartmental Memorandum of Understanding ("IMOU"), a copy of which is attached and incorporated herein, and as permitted under applicable State and federal law and regulations.

NOW, THEREFORE, the Parties agree as follows:

1. Definitions

a. De-identified Data: Data that has been modified by removing personally identifiable information to reduce the likelihood of identification of the individuals to whom the data pertain. Standards for data deidentification may vary based on the source of the data and the laws, regulations, and/or policies that may apply to the data.
b. Confidential Data: Data for which access, use, or disclosure of the data is restricted according to state or federal law, regulation, or policy.
c. Chief Data Officer (CDO): The individual who is responsible for oversight of Data Office activities, including but not limited to facilitating Data Governance-related committees, developing and managing partnerships with the Parties, overseeing Data Office staff, overseeing technical implementation activities, consulting with Data Recipients, monitoring requests, and managing the inventory of documents associated with operations and Projects.
d. Data Custodian: Staff and employees charged with overseeing the safe transport, storage, and disposition of data, including infrastructure, activities, and safeguards required to maintain the confidentiality, integrity, and availability of the data.

e. Data Governance Council: The group comprised of representatives from each Party that shall be responsible for establishing, reviewing, and implementing this IMOU. This committee will also be responsible for appointing members of relevant committees, identifying data access and use priorities, and general oversight of data governance activities. The Chief Data Officer or designee will chair the Data Governance Council.
f. Data Integration: The process of combining one set of data with another through record linkage, which refers to the joining or merging of data based on common data fields, in order to better understand multi-program and multi-service relationships and involvement. These data fields may include personal identifiers (e.g. name, birth date) or a "unique ID" that is used to link or join records. While data integration may involve more risk, and therefore requires more oversight, it is essential for understanding multi-service involvement and informing data-driven policy processes.
g. Data Integration Staff: The individuals within the NCDHHS Data Office and NCDHHS Information Technology Division ("ITD") who have responsibility for handling and securing Data from the Parties for approved uses. The Data Integration Staff will consult with Party staff, clean data, link data, and prepare data for approved use.
h. Data Owner: One or more individuals, or their designee, who has/have signatory authority to legally bind a Party and who is/are empowered to authorize the release of data owned by the Party for a specific Project.
i. Data Quality and Strategic Use Purposes: Data Quality Assessment and Improvement Activities and Operational and Business Intelligence Activities.
j. Data Quality Assessment and Improvement Activities: Actions that measure the condition of data or increase the performance of data in regard to the data's completeness, accuracy, consistency, reliability, or timeliness.
k. Data Recipient: The individual or entity that makes a request for data intended for NCDHHS operational and business intelligence purposes, research, or approved use.
l. Data Sharing Agreement (DSA): An agreement between each Party, the Data Office, and ITD that documents the specific terms and conditions for intradepartmental data sharing of Confidential Data. The DSA will include a description of the lawful purpose of the data sharing and will include how data is transferred and secured for Data Recipients and refer to the IMOU as needed.
m. Data Stewards Group: A committee composed of representatives from each Data Source who have programmatic experience with and data expertise on their respective Data Source. When the Data Stewards Group reviews data requests and proposed Projects, as applicable, the designated representative (Data Steward) from each Data Source will be tasked with making a recommendation about whether a request for the Data Source's data contemplates a use case that is methodologically and analytically sound. The designated representative for the Data Source shall be selected by the Data Owner. The Chief Data Officer or designee will facilitate the Data Stewards Group.
n. Data Source: A discrete data set or data system owned by a Party. Each Data Source shall have its own Data Owner.
o. Data Use Agreement (DUA): Where applicable, agreement between the Data Recipient and Data Owner(s) that outlines the terms and conditions under which the Data Owner(s) will provide the

Data Recipient with access to the data. The DUA may include the objectives of the request, methodology, data description, permitted uses, data security plan (including access), completion date, reporting requirements, data privacy requirements, and terms for data destruction. A standard DUA with terms will be developed and updated by the Data Office, and approved by the NCDHHS Data Governance Council, as needed. Parties, at the discretion of Data Owner with input from Legal Counsel, may use the standard DUA, or a different agreement at the Data Owner's discretion.

p. High Value Data Assets: Identified by each Division and Office, and includes any Data Source the Division or Office owns that:
    a. Is critical to the operations of NCDHHS
    b. Serves the strategic goals of NCDHHS
    c. Can improve public knowledge of NCDHHS and its operations
    d. Is frequently requested by the public
    e. Responds to a need and demand as identified by the Department through public consultation; or
    f. Is used to satisfy any legislative or other reporting requirements

    The High Value Data Asset inventory lists these assets and is updated annually.
q. HIPAA: The Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, as amended, and its implementing regulations.
r. Intradepartmental Memorandum of Understanding (IMOU): Agreement that documents that vision, mission, and governance processes of data sharing and integration across NCDHHS.
s. Legal Counsel: As defined by the NCDHHS Office of General Counsel.
t. Operational and Business Intelligence Activities: Data Integration and/or exploratory analysis of one or more sets of data so that Data Owners and DHHS leadership can better answer policy and business questions or meet programmatic or business needs.

2. Transfer of Data

The Data Owner will provide to Data Integration Staff, or otherwise permit Data Integration Staff to electronically access, the data associated with requests approved in accordance with the IMOU. Data Integration Staff are required to sign and abide by a confidentiality agreement (see Attachment B) prior to being provided with electronic access to a data system or data source managed by NCDHHS. If Data Owner is transmitting the data to the Data Integration Staff (as opposed to providing electronic access for downloading the data directly), then the Data Owner will transmit the data electronically via encrypted files and in accordance with the NCDHHS Information Security Manual.

3. Rights to Share/Redisclose the Data

No data that is collected, owned, or managed by the Data Owner will be distributed to another party, including other Divisions or offices within NCDHHS, without the Data Owner's prior written approval, except as expressly provided in this Agreement and the IMOU.

4. Data Access, Security, Use, and Deletion

Data Integration Staff shall comply with the following access and security requirements:

a. Limited Access. Access to the Data Owner's data shall be limited to data described in Attachment A and shall only be accessed by Data Integration Staff who are working on a specific request approved by the Data Owner under the terms of the IMOU, this DSA, or a fully executed DUA. In conducting their work, Data Integration Staff shall limit their view of and access to the data to that which is minimally necessary to accomplish the purpose for which the data is being accessed and viewed.

b. Secure Storage. Data Integration Staff agrees to proceed according to requirements, contained in (FISM) NIST SP800-39, Managing Information Risk. Furthermore, Data Integration Staff shall be responsible for maintaining a secure environment compliant with State policies, standards and guidelines, and other Applicable Law that supports the Transmission of Data in compliance with the Specifications. Data Integration Staff 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 IMOU, the (FISM) NIST SP800-47, and Applicable Law, including appropriate administrative, physical, and technical safeguards that protect the confidentiality, integrity, and availability of that Data. Appropriate safeguards shall be those required by Applicable Law related to Data security, specifically contained in (FISM) NIST SP800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

c. Use. Data Integration Staff shall use the data solely for a Project approved through the process outlined in the IMOU. Data Integration Staff will only provide data to Data Recipients who are permitted to receive the data according to Attachment C or who have signed the Data Use Agreement or another agreement governing data access and use that is approved by the Owner.

d. Data Deletion. Data Integration Staff shall retain the Data Owner's data for the period of the IMOU ("Data Retention Period"), unless otherwise agreed to by the Data Owner as stipulated within a DUA. After this period, the data will be deleted by Data Integration Staff or other authorized personnel will submit a Certificate of Data Destruction (Attachment D) to the Data Owner.

5. Release of Data

a. Criteria for Release of Data. Data Integration Staff will only disclose data that have been approved and memorialized, as applicable, by the execution of appropriate agreements, including the DUA for approved use and by referring to Attachment A.

6. NCDHHS Responsibilities

The Data Owner shall consult with Legal Counsel to determine whether the requested data may be provided according to State and federal law and regulations and Division or office policies.

7. Confidentiality and Breach Notification

a. Confidentiality. All Data Integration Staff shall be informed of the confidentiality obligations imposed by this Agreement and must agree to be bound by such obligations prior to disclosure of the Data Owner's data to Data Integration Staff, as evidenced by staff members' signatures on Attachment B or the Acceptable Use Policy.

b. Potential Breach Notification. The Data Office and ITD agree to be responsible for unauthorized disclosures of data or breach of this Agreement that arises out of the performance of Data Integration Staff under this Agreement. Data Integration Staff shall report to the Data Owner all breaches or suspected breaches that threaten the security of the data and/or data systems that result or may result in unauthorized disclosure of the data, including inadvertent disclosures or other incidents compromising the security of NCDHHS' information technology systems. Such reports shall be made to the Data Owner and to the NCDHHS Privacy and Security Office by filing a report online at https://security.ncdhhs.gov/ within 24 hours from when Data Integration Staff discover the breach or incident. If the privacy or security incident involves Social Security Administration (SSA) data or Centers for Medicare and Medicaid Services (CMS) data, the Recipient shall report the incident within one (1) hour after the incident is first discovered.

8. Term of Agreement

a. Except as otherwise set forth in this Agreement, the term of this Agreement shall be for a period of three (3) years unless otherwise terminated as set forth in Paragraph 9(b).
b. The Parties shall review this Agreement annually in conjunction with the annual completion of the Data Asset Inventory.
c. Any of the Parties may terminate this Agreement upon providing thirty (30) days' written notice to the other Parties.
d. Within thirty (30) days of the termination of this Agreement, Data Integration Staff shall return or destroy all of the Data Owner's data that is in the possession of Data Integration Staff. Data Integration Staff shall retain no copies of the data. Data Integration Staff shall provide the Owner with written confirmation of compliance with this requirement by completing the Certificate of Data Destruction in Attachment D. Terms of this Agreement related to data access, security, use, confidentiality, and breach notification shall survive until all of the Owner's data has been returned or destroyed.

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

9. Party Representatives

The Parties' contacts for purposes of this Agreement are:

For Data Owner:	For NCDHHS Data Office:
Click here to enter text.	Click here to enter text.
For Data Owner:	For NCDHHS ITD:
Click here to enter text.	Click here to enter text.

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

NCDHHS Data Office

By:	Name: Click here to enter text.
	Title: Click here to enter text.
	Date*:* Click here to enter text.

NCDHHS ITD

By:	Name: Click here to enter text.
	Title: Click here to enter text.
	Date*:* Click here to enter text.

DATA OWNER

By:	Name:
	Title:
	Date*:* Click here to enter text.

Attachment A: Shared Data Fields/Datasets

Attachment A is the Division / Office specific NCDHHS Data Asset Inventory. This is an inventory that is updated annually and includes information about Division / Office identified high value data assets, i.e., any data that:

- Is critical to the operations of NCDHHS
- Serves the strategic goals of NCDHHS
- Can improve public knowledge of NCDHHS and its operations
- Is frequently requested by the public
- Responds to a need and demand as identified by the Department through public consultation; or
- Is used to satisfy any legislative or other reporting requirements

The Data Asset Inventory Form includes the following fields:

Data Repository where asset is contained	PII data (Y/N)	Data Steward
Application/Dataset Name	Protected data (Y/N)	Data Custodian
Division/Office	PHI data (Y/N)	Data Owner
Description (Function/Utilization)		Data Owner Designee
Major Entities in Dataset		

Application / Datasets That Can Be Shared, as of [Insert Date]:

1	Application/Dataset Description:
	Incorporated within BIDP: Yes No
	Frequency of Update: Nightly
	Protected Data, including PHI / PII: Yes No
	If applicable, De-identification guidelines (Insert Applicable Methodology/Guidance):
	If applicable, Data destruction guidelines:
	If applicable, Legal restrictions of use:
	Notes:

2	Application/Dataset Description:
	Incorporated within BIDP: Yes No
	Frequency of Update: Nightly and monthly
	Protected Data, including PHI / PII: Yes No
	If applicable, De-identification guidelines (Insert Applicable Methodology/Guidance):
	If applicable, Data destruction guidelines:
	If applicable, Legal restrictions of use:
	Notes:

3	Application/Dataset Description:
	Incorporated within BIDP: Yes No
	Frequency of Update: Nightly
	Protected Data, including PHI / PII: Yes No

	If applicable, De-identification guidelines (Insert Applicable Methodology/Guidance):
	If applicable, Data destruction guidelines:
	If applicable, Legal restrictions of use:
	Notes:

4	Application/Dataset Description:
	Incorporated within BIDP: Yes No
	Frequency of Update: Ongoing
	Protected Data, including PHI / PII: Yes No
	If applicable, De-identification guidelines (Insert Applicable Methodology/Guidance):
	If applicable, Data destruction guidelines:
	If applicable, Legal restrictions of use:
	Notes:

5	Application/Dataset Description:
	Incorporated within BIDP: Yes No
	Frequency of Update: Ongoing
	Protected Data, including PHI / PII: Yes No
	If applicable, De-identification guidelines (Insert Applicable Methodology/Guidance):
	If applicable, Data destruction guidelines:
	If applicable, Legal restrictions of use:
	Notes:

6	Application/Dataset Description:
	Incorporated within BIDP: Yes No
	Frequency of Update: Ongoing
	Protected Data, including PHI / PII: Yes No
	If applicable, De-identification guidelines (Insert Applicable Methodology/Guidance):
	If applicable, Data destruction guidelines:
	If applicable, Legal restrictions of use:
	Notes:

[add tables as needed]

Application / Datasets / Variables That Cannot Be Shared.

1	Application/Dataset Description:
	Protected Data, including PHI / PII: Yes No
	Relevant statute / rule / reason for legal restrictions of use:
	Notes:

[add tables as needed]

Attachment B: Confidentiality Agreement

Ensuring the confidentiality of all health reports, records, and files containing patient names and other individually identifying or sensitive information is of critical importance to the North Carolina Department of Health and Human Services (NCDHHS). Breaches of confidentiality can undermine public trust in NCDHHS and thereby hinder efforts to improve the health, safety, and well-being of North Carolinians.

The NCDHHS Data Office and the Information Technology Division (ITD) shall designate individual staff members ("Designated Staff Members") who will be permitted to view, access, and/or use data belonging to other NCDHHS Divisions or offices ("Data Owner") consistent with the terms of the Inter-agency Memorandum of Understanding (IMOU) and this Agreement entered into by the Data Owner, the NCDHHS Data Office, and ITD ("the Purpose"). Before a designated staff member may be given access to the Data Owner's data, the designated staff member shall sign the Confidentiality Agreement included within the NCDHHS PSO Acceptable Use for DHHS Resources or the form below. Copies of signed Confidentiality Agreements shall be kept on file by the NCDHHS Data Office and/or ITD and shall be furnished to the Data Owner upon request.

The data to which the designated staff member will have access may include information that is confidential under State and federal law and regulations, including but not limited to the restrictions set forth in 45 C.F.R. parts 160 and 164, subparts A and E, ("the Privacy Rule"), 45 C.F.R. Parts 160, 162 and 164, subparts A and C ("the Security Rule"), the applicable provisions of the Health Information Technology for Economic and Clinical Health Act (HITECH), and N.C.G.S. §§ 75-65 and 75-66.

Confidentiality Agreement Acknowledgement:

- I understand that I may have access to Data Owner's data that is confidential under State or federal law. I will maintain the confidentiality of Data Owner's data in accordance with this agreement and applicable State and federal law as well as the requirements set forth in the NCDHHS Privacy and Security Policies and Manuals[1] and the NC Statewide Information Security Manual.[2] I understand that unauthorized access or disclosure may be a violation of State and/or federal law.
- I will limit my access and use of the Data Owner's data to that which is minimally necessary to accomplish the Purpose set forth in this agreement.
- I will keep any account credentials granted by the Data Owner private. I will not share my account credentials with other users or any unauthorized individual. I will neither request nor use another person's account credentials, other credentials, or other unauthorized means to access Data Owner's data.
- I will provide Data Owner with notice no later than twenty-four (24) hours from the termination of this agreement, my departure from employment with NCDHHS, or my assignment to different duties within NCDHHS that do not require access to Data Owner's data.

[1] Located at https://policies.ncdhhs.gov/departmental/policies-manuals/section-viii-privacy-and-security/manuals
[2] Located at https://it.nc.gov/statewide-information-security-policies

- I will provide Data Owner with notice of any violations of this confidentiality agreement, including suspected and confirmed privacy/security incidents or privacy/security breaches involving unauthorized access, use, disclosure, modification, or destruction of Data Owner's data, including a breach of any account credentials. Notice shall be provided directly to the Data Owner by email or phone and to the Privacy and Security Office by filing a report at https://security.ncdhhs.gov/ within twenty-four (24) hours of the incident first being discovered. If the privacy or security incident involves Social Security Administration (SSA) data or Centers for Medicare and Medicaid Services (CMS) data, the Recipient shall report the incident within one (1) hour after the incident is first discovered.
- I understand that my failure to abide by the terms set forth in this Confidentiality Agreement may result in consequences that include, but are not limited to, the immediate termination of my access, the termination of the NCDHHS Data Office or ITD's access to the Data Owner's data, and disciplinary action up to termination of my employment or contract.

By signing below, I affirm that I have read this Confidentiality Agreement and agree to be bound by the terms therein.

Print Name: _____

Signature: _____

Date: _____

Division/Office: _____

Supervisor: _____

Attachment C: Data Priorities and Approved Uses

Within the limitations set forth in Attachment A, DHHS staff approved to work on any of the following approved uses may access and use the data listed in Attachment A.

1) DHHS will advance its mission to improve the health, safety, and wellbeing of all North Carolinians by prioritizing data use to further the following goals:

a) Advance health equity by reducing disparities in opportunity and outcomes for historically marginalized populations within DHHS and across the state.
b) Help North Carolinians end the pandemic, control the spread of COVID-19, recover stronger, and be prepared for future public health crises with an emphasis on initiatives serving those communities most impacted.
c) Build an innovative, coordinated, and whole-person — physical, mental and social health — centered system that addresses both medical and non-medical drivers of health.
d) Turn the tide on North Carolina's opioid and substance use crisis.
e) Improve child and family well-being so all children have the opportunity to develop to their full potential and thrive.
f) Support individuals with disabilities and older adults in leading safe, healthy and fulfilling lives.
g) Achieve operational excellence by living our values — belonging, joy, people-focused, proactive communication, stewardship, teamwork, and transparency.

2) **Generally Approved Use for Data Quality and Strategic Use Purposes**

Unless otherwise specified by the Data Owner in "Attachment A: Shared Data Fields/Datasets" to this Agreement, the Data Owner agrees and authorizes Data Integration Staff and persons or entities performing activities on behalf of Data Integration Staff or Data Owners, to utilize the minimum necessary Data for both: 1) Data Quality Assessment and Improvement Activities; and 2) Operational and Business Intelligence Activities (collectively known as "Data Quality and Strategic Use Purposes").

Permission to access the Data for Data Quality and Strategic Use Purposes is limited to Data Integration Staff and persons or entities performing activities on behalf of Data Integration Staff or the Data Owners, and strictly for DHHS's Data Quality and Strategic Use Purposes, unless otherwise specified by the Data Owner under this Agreement in "Attachment A: Shared Data Fields/Datasets" to this Agreement.

Otherwise, access and use of the Data specified by the Data Owner in "Attachment A: Shared Data Fields/Datasets" to this Agreement is strictly limited to purposes directly connected with the administration of specific programs and specific purposes where required or as otherwise limited by law or policy.

Unless prohibited in "Attachment A: Shared Data Fields/Datasets", the following are examples of approved cross-divisional or cross-sector data use for Data Quality and Strategic Use Purposes:

a. Data linkage to identify cross-enrollment or gaps in services and DHHS programs.
b. Data linkage to enable data-informed policy and program decision-making
c. Leveraging demographic information from previously siloed sources to enable population stratification, e.g. using race collected through vaccine operations that was not collected upon enrollment in SNAP for the same person.

d. Build a "whole person health" view of an individual for access by authorized users, e.g. case workers
e. Building internal or public facing (with appropriate suppression) visualizations and reports to inform policy and decision-making
f. Leverage entity resolution services for deidentified linkage of individual records for the purpose of record linkage
g. Identify household and family relationships. For example, discerning multigenerational, household, multi-relationships to better evaluate outcomes related to individual and family well-being, and better target through outreach.

3) **Division-Specific / Office-Specific Approved Uses**

Unless otherwise specified by the Data Owner in "Attachment A: Shared Data Fields/Datasets" to this Agreement, the Data Owner agrees and authorizes Data Integration Staff and persons, or entities performing activities on behalf of Data Integration Staff or Data Owners, to utilize the minimum necessary Data for the following Data-Ownerapproved data uses:

- [**BRIEF DESCRIPTION OF USE/PROJECT (Example- "PDS")]**
  [Example: Program data are integrated in the Program Data System (PDS), a comprehensive, integrated data system for North Carolina to inform policies and practices that produce better outcomes for program participants.]
- **[Example- DATA VISUALIZATION (EXTERNAL AND INTERNAL FACING)]**
  [Example- Program currently has three public data dashboards built off of public data. They are:
  - Dashboard 1 (Insert link to dashboard) built from data in the Program Data System. Updated monthly from extracts pulled from vendor's data warehouse. Currently working on automating the process using BIDP so that additional data can be incorporated into the current dashboard, for example demographic data with appropriate suppression.}
- **PROGRAM RESEARCH**
  [Example- Program is currently working on a qualitative research project with Program Partner (PP). The project has a specific focus around data equity. It is a two year project that began in January 2022 so findings from this work will likely not be available until 2024.]

Attachment D: Certification of Removal of Data Access and/or Destruction of Data

Date of Project Completion: Click here to enter text.
Date of Removal of Data Access and/or Data Destruction: Click here to enter text.
Person Providing Oversight for Removal of Access/Destroying Data: Click here to enter text.
Title: Click here to enter text.
Agency: Click here to enter text.
Phone Number: Click here to enter text. **E-mail:** Click here to enter text.
Term of Data Use Agreement: Click here to enter text.
Data Use Agreement Number:

I confirm that, as applicable, all access to NCDHHS Data permitted pursuant the above referenced Data Use Agreement has been rescinded and all NCDHHS Data received under the above referenced Data Use Agreement has been destroyed, including data held and/or accessed by all Authorized Personnel, as defined under the Data Use Agreement.

By signing below, I confirm that NCDHHS Data was destroyed and access to NCDHHS Data was rescinded, as applicable, on Click here to enter text. This destruction was carried out as follows:

1. Information in electronic format was destroyed in compliance with the minimum standards set out in the Guidelines for Media Sanitization (NIST 800-88) guideline issued by the US Dept of Commerce (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf).

2. Information in hardcopy or printed format was destroyed using a cross-cut shredder or an equivalent destruction method.

Signature:

Name: Click here to enter text.

Title: Click here to enter text.

Attachment E: Internal BAA or BAQSOA (if applicable)