# North Carolina Department of Health and Human Services Intradepartmental Memorandum of Understanding

## Background

This Intradepartmental Memorandum of Understanding (“IMOU”) facilitates an efficient, enduring culture of robust, data-driven cross-department collaboration that shields against unauthorized disclosure and misuse of protected data.

This IMOU documents and memorializes the vision, mission, and governance process of data sharing and integration across the North Carolina Department of Health and Human Services (“NCDHHS”) for business intelligence and operational data needs.

This IMOU will be signed by the Office of the Secretary and Data Owners and will govern intradepartmental data access and use not otherwise covered under a current agreement.

This IMOU references the Data Sharing Agreement (“DSA”), an agreement signed by the Data Owner, the Data Office, and Information Technology Division (“ITD”); the Data Use Agreement (“DUA”), an agreement signed by the Data Recipient and Data Owner(s); and the NCDHHS Data Sharing Guidebook, which provides NCDHHS personnel guidance and resources for appropriately accessing and using data.

NCDHHS, in collaboration with a wide array of partners and stakeholders, provides essential services to improve the health, safety, and well-being of all North Carolinians Much of this work involves administering or supporting the delivery of services that are critical to North Carolina’s most vulnerable populations, including children, seniors, people with disabilities, and lower-income individuals and families. NCDHHS’ goals for strategic data access and use reflect the wide range of programs NCDHHS administers and supports and the populations NCDHHS serves.

Collaboration across divisions and programs is essential to achieving optimal and efficient services for the residents of North Carolina, and data sharing is an indispensable component of cross-collaboration. For this reason, the NCDHHS Data Office (“Data Office”) and the Data Governance Organization support intradepartmental data access and use through data sharing process that support efficient data sharing, which in turn facilitates analyses and cross-department insights that improve service delivery and outcomes, while maintaining and strengthening privacy safeguards and legal requirements.

This IMOU supports the NCDHHS Data Office and Data Governance Organization’s ability to strategize, prioritize, and have visibility into activities across NCDHHS that relate to data governance.

This IMOU aligns with NCDHHS values and data strategy principles, including:

*Teamwork:* Democratize data to help more people across NCDHHS access data they need to do their work, and the analyses/insights derived from it, with fewer gatekeepers and bottlenecks.

*Transparency:* Give business users the ability to more easily access and work with data they need to carry out their jobs, no matter where the data are located, or which application created the data.

*Stewardship:* Just as it is important to be good stewards of financial resources and time, it is important to be good stewards of NCDHHS data, managing and overseeing data assets in a way that provides high-quality, accessible data that can have a positive impact on those we serve. Good stewardship also involves maintaining the public’s trust by ensuring the security, protection, and use of NCDHHS data is in accordance with applicable State and federal law and regulations.

*People-focused:* The well-being of the people we serve is paramount, including safeguarding the privacy and security of their personal information.

In short, this IMOU supports the Office of the Secretary and the NCDHHS Data Office in its vision to enable NCDHHS and its partners to efficiently make data-driven strategic and operational decisions by providing access to integrated, trustworthy, well-governed, well managed, and legally permissible use and exchange of data.

## Definitions

1. Access Request: procedure by which an individual or entity may request data.
2. Applicable Law: The rules of action or conduct prescribed by controlling authority, including State and federal law, statutes, regulations, policies, standards, rules, and guidelines.
3. De-identified Data: Data that has been modified by removing personally identifiable information to prevent the 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.
4. Confidential Data: Data for which access, use, or disclosure of the data is restricted according to state or federal law, regulation, or policy.
5. Chief Data Officer (CDO): The individual who is responsible for oversight of Data Office activities, including but not limited to facilitating Data Governance 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.
6. Controlled Unclassified Information: Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. CUI includes information the Federal government creates or possesses, or that an entity creates or possesses for or on behalf of the Federal government, that a law, regulation, or Federal government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, a federal executive branch agency or an entity acting for a federal executive branch agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways: Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify.
7. Data Access List: List of individuals or entities that have been approved to access data.
8. 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.
9. Data Governance Organization (DGO): The mission of the DGO shall be to strategize, prioritize, and oversee activities across NCDHHS related to data governance (DG). DG encompasses the people, processes, and information technology required to ensure data quality, integrity, availability, usability, and security throughout its lifecycle. The DGO will be staffed by the Data Office and will be comprised of two standing bodies: the Data Governance Executive Board and Data Governance Council. Additional *ad hoc* topic-specific working groups may be formed as needed.
10. Data Governance Executive Board (DGEB): The DGEB will provide guidance and oversight for data governance across the organization. The Executive Board is composed of executive-level leaders of participating Divisions and Offices. Representatives shall include each participating Division’s or Office’s Director or Assistant Secretary or equivalent, the Chief Information Officer (CIO), Chief Technology Officer (CTO), and Chief Data Officer (CDO). Many, though not all, DGEB members are also Data Owners as defined by the DHHS Data Sharing Guidebook. The DGEB will serve as the voting body for the DGO and will be responsible for establishing, reviewing, and implementing this IMOU. Key duties of the DGEB include approving data policies and major data-related decisions; voting on decisions about data priorities, projects, and resources; and holding Divisions and Offices accountable for adhering to Data Governance policies. The Chief Data Officer or designee will chair the Data Governance Executive Board.
11. Data Governance Council (DGC): The DGC will focus on implementing the vision and priorities of the DGEB, as well as establishing and maintaining processes for management and use of DHHS data and making recommendations to the DGEB regarding data-related Departmental policies and initiatives. The DGC is comprised of data-knowledgeable staff from each Division. DGEB members from each Division or Office may appoint one or more staff members to the DGC. These appointees should have both knowledge of business priorities and operations, and a basic level of data fluency, i.e., the ability to use and communicate ideas about data with others. The Chief Data Officer or designee will chair the Data Governance Council. The Data Office Data Governance Lead or another appropriate staff member as determined by the Chief Data Officer will chair the Data Governance Council.
12. Data Integration Staff: The individuals within the NCDHHS Data Office and NCDHHS Information Technology Division (“ITD”) who have responsibility for the 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.
13. Data Owner: One or more individuals, or their designee, with signatory authority to legally bind a Party and who is empowered to authorize the release of data owned by the Party for a specific Project.
14. Data Sharing Agreement (DSA): An agreement between each Party, the Data Office, and ITD that documents the specific data, 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 this IMOU as needed.
15. Data Recipient: The individual or entity that makes a request for data intended for NCDHHS operational and business intelligence purposes, research, or approved use. (Also referred to as Requestor)
16. Data Steward: A representative for a Data Source with programmatic experience and data expertise on their respective Data Source. The designated representative for the Data Source shall be selected by the Data Owner and will be responsible for the governance of their Data Source (such as data transfer, alteration, storage, retention, disposition, classification, etc.). This includes: documenting metadata, limitations, and sources of bias for the data; supporting established processes and policies for access and use; collaborating with the Data Owner to ensure strategic use; and collaborating with Data Custodian(s) to ensure data availability. When a request for data is made, the Data Steward will be tasked with making a recommendation about whether a request for the Data Source’s data contemplated a use case that is methodologically and analytically sound. When applicable, the Data Steward is responsible for cell suppression methodology and other statistical, data-based safeguards. The Data Steward is often the subject matter expert that works with data regularly for business purposes. The Data Steward may also participate in intradepartmental data governance coordination, such as efforts coordinated by the Data Stewards Community.
17. Data Source: A discrete data set or data system owned by a Party. Each Data Source shall have its own Data Owner.
18. Data Use Agreement (DUA): 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 Executive Board, 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.
19. High Value Data Assets: Identified by each Division and Office, and includes any Data Source the Division or Office owns that:
	1. Is critical to the operations of NCDHHS;
	2. Serves the strategic goals of NCDHHS;
	3. Can improve public knowledge of NCDHHS and its operations;
	4. Is frequently requested;
	5. Responds to a need and demand as identified by the Department through public consultation; or
	6. Is used to satisfy any legislative or other reporting requirements

The High Value Data Asset inventory lists these assets and is updated annually.

1. HIPAA: “HIPAA” means the Administrative Simplification Provisions, Sections 261 through 264, of the Federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, as modified and amended by the Health Information Technology for Economic and Clinical Health (“HITECH”) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Public Law 111-5, as amended.
2. IRB: institutional review board.
3. Legal Counsel: As defined by the NCDHHS Office of General Counsel.
4. Operational Data Request: A data request related to ongoing work of NCDHHS that supports business intelligence with a NCDHHS division or office, department, and/or strategic partner (under current agreement with NCDHHS), including local offices.

## Parties

This IMOU is entered into by the undersigned entities, each hereinafter referred to individually as a “Party” and collectively as the “Parties.” In order for any entity to be added as a Party to this IMOU, a joinder in the form of Exhibit A must be executed. Such joinder does not constitute an amendment to the terms of this IMOU. The sole effect of a joinder to this IMOU is to add an additional entity as a Party and bind such entity to the terms of this IMOU.

## Intent and Purpose

The Parties share a mutual vision of enabling effective and responsive policies and programs for North Carolina residents that are supported by timely and cost-efficient data analysis, public health surveillance, research, and evaluation using integrated data. The Parties have concluded that this IMOU is a necessary component of the data governance required to achieve this mutual vision. This collaboration between the Parties, facilitated by the Data Office, includes participation in the data governance framework described in this IMOU**.**

The Data Office may use a hybrid approach to data management to facilitate data access, storage, and integration, with data either being physically federated (where each Party maintains their own data and data are only transferred to an independent or third-party platform for data integration) or unfederated (where data is managed and stored by the Data Integration Staff as needed for linking and integration).

This IMOU does not require Parties to use the Data Office to coordinate data sharing when a different pathway for project approval and data linkage is preferred by the Parties whose data is requested.

The Parties agree that this IMOU and the Data Office’s facilitation of data governance processes can help support data sharing by:

* 1. Creating a data sharing governance framework and establishing consistent data sharing processes that adhere to all applicable state and federal laws, rules, policies, and guidelines
	2. Reducing the repetitive or redundant burdens on Parties’ legal counsel and data management teams
	3. Taking a person- or family-centered approach to data use as opposed to an exclusively division-centered or isolated service approach to data use
	4. Building capacity for routine cross-department and cross system data-driven collaboration
	5. Increasing the efficiency of data sharing for cross-department analytic needs.
	6. Enhancing privacy, security, and compliance with Applicable Law, including but not limited to HIPAA and requirements for handling other CUI, through standard processes, agreements, and structured communication

## Financial Understanding

Services provided by Data Integration Staff to fulfill data requests made by parties external to NCDHHS may be supported through a cost-based model, to the extent permitted by law and policy. When a fee is applicable, the fee will only be charged to Data Recipients who are not staff, employees, or contractors of NCDHHS. This fee may include the actual costs incurred by Parties to this agreement for their efforts to provide data. The detailed fee structure will be developed by the Chief Data Officer and approved by the Data Governance Executive Board and the NCDHHS Office of General Counsel prior to implementation.

## Guidelines for Data Access and Use

The NCDHHS Data Sharing Guidebook provides an overview of guidelines and key considerations for the data request process. Continuous improvements to data sharing processes are expected and encouraged. Regular updates to the Guidebook will be facilitated by the Data Office, with oversight by the Data Governance Organization and Legal Counsel, along with amendments and other **written** updates to this IMOU**.**

##

## Data Request Process

The data request process provides NCDHHS personnel with the information needed to utilize data as a strategic asset while ensuring ethical and legal data access and use through comprehensive review,

The process for requesting data will consist of three steps: (1) reviewing the data request pathways (see Guidebook) and determining, in consultation with the Data Office, if necessary, the appropriate pathway for the request; (2) submitting the request via the appropriate channel outlined in the Guidebook or as directed by the Data Owner; and 3) seeking Data Owner approval.

A majority of data requests involving data held by two or more Data Owners will be Operational Data Requests or Research Requests that should be submitted via the Data Office request process through the operational data request pathway. This includes requests where data from two or more Data Owners will be linked or integrated. For Data Office requests, the Data Request will be submitted to the Data Office on the appropriate data request form based on whether it is an operational or research data request. If the Requestor is unsure of the classification, the Requestor should contact the Data Office for guidance.

Updates to the data request forms will be facilitated by the Data Office, with oversight by the Data Governance Organization and review by Legal Counsel.

When the request does not involve linking or integrating data or data held by two or more Data Owners, data requests may be made through this process or outside of this process and directly to the Party whose data are requested, at the preference of the Data Owner.

Regardless of the data request pathway, Data Owners retain ultimate control and authority over the data in their custody.

## Data Office Requests Procedure

## Initial Review. For requests submitted to the Data Office, including requests for amendments to existing agreements, the Data Office will perform an initial review of the request and then forward the request for Data Steward review.

## The purpose of the initial review is to ensure that only complete and responsive project submissions are forwarded to Data Steward(s). The Data Office’s initial review will include the following:

* 1. Confirming the request form is complete (i.e., no blank fields) and accurate.
	2. Confirming all required supporting documentation has been submitted, such as IRB protocols for Research Requests and other approvals, where applicable.
	3. Confirming the request addresses at least one established NCDHHS priority.
	4. Determining whether the request to access and use the data is permissible under the applicable DSAs and the data security plan meets requirements of the relevant Data Sharing Agreement(s). If not, confirming whether a DUA is needed, or an amended or new DSA should be executed. Determinations may include consultation with Legal Counsel and Privacy and Security Officers.
	5. Consulting with Legal Counsel to determine whether the proposed use case for the requested data is permitted under state and federal laws and regulations.

The Data Office will provide feedback and return non-conforming, incomplete, or inaccurate requests to the Requestor. Conforming requests will be forwarded to the Data Steward(s) whose data is being requested for review and a recommendation to approve, revise, or reject the request.

## Evaluation by the Data Stewards(s). Following their initial review, the Data Office will reach out to the appropriate Data Steward to review the proposed projects or requests.

Each Data Owner will assign at least one Data Steward to each Data Source who will be responsible for reviewing data requests for that Data Source. The Data Owner may assign different Data Stewards for different Data Sources.

A Data Steward’s review and recommendation is a precursor to the Data Owner making the final decision. The Data Steward’s review and recommendation is based on subject matter expertise and is limited to assessing whether the case is methodologically and analytically sound. The recommendation itself does not need to be reviewed by legal counsel or approved by the Data Owner.

Each Data Steward included in a request will make a recommendation to either reject, request modifications to, or approve a data request, which is then presented to the Data Owners.

With respect to their own Data Sources, Data Owners may establish an internal process whereby their Data Steward consults with the Data Owner prior to making a recommendation.

Data Stewards may make the following recommendations:

1. Approve. The request does not require substantive changes or clarification to the request proposal. The Data Steward(s) may require minor changes or offer suggestions to strengthen the request;
2. Revise. The request requires changes or clarification that necessitates further consideration. Applicable Data Steward(s) will typically consider revised proposals as needed; or
3. Reject. The potential benefits of fulfilling the request do not outweigh the concerns related to fulfilling the request.

Recommendations made by the Data Steward(s) should be documented in writing.

## Data Owner Permission. Following review by the applicable Data Steward(s), the request and Data Steward(s) recommendation will be considered by all impacted Data Owners for concurrence.

## Should one or more Data Owners reject a request for their data, the request can be revised to remove the unapproved data and be resubmitted. All data requests that are approved by the Data Owner will also be reviewed by Legal Counsel to determine whether the requested data can be released for the final proposed use case. Review by Legal Counsel and the approval of all Data Owners whose data is involved in the request will be a prerequisite to the execution of any agreements pertaining to the data sharing and to the release of the data.

## Except as required by law, there is no appeal process and a Data Owner’s decisions are final.

## CDO Responsibilities. The CDO or designee will send Data Governance Executive Board members a summary of data request decisions annually or as requested. The CDO will consult as needed with the Data Governance Executive Board and Data Governance Council to prioritize requests.

If applicable, the CDO or designee will communicate to the Requestor via email and convey the decision, summarize reviewer comments, and outline next steps. A timeline and applicable final cost estimate will also be provided for approved projects.

##  Procedure for Requests for User Access to NCDHHS Data.

Individual staff, employees, and contractors who do not already have personal, authorized access and require access to dashboards or self- service data sets, or who need to pull data directly from the Data Source tables for specific approved use(s) may request access to this data through the process outlined below (“User Access Requests”):

* 1. Contact the Data Owner. Requestor will contact the relevant Data Owner (e.g. project owner of a specific dashboard), who will initiate the approval process as described in the Requesting Data Access and Use section of the Guidebook or alternative procedures as determined by the Data Owner.

If the User Access Requestor does not know the relevant Data Owner, then the User Access Requestor will contact the Data Office. The Data Office will initiate the approval process by contacting the appropriate Data Owner or their designated representative and determine whether the Data Office will further facilitate the User Access Request.

In cases where the user access requestor will be working directly with the Data Owner, the Data Office will provide the user access requestor the Data Office’s contact information.

If the Data Office determines they will be facilitating the User Access Requests:

1. When a new User Access Request is received, the Data Office will review the request and contact the User Access Requestor to discuss and document user requirements to determine access.
2. As needed, Data Office Staff and the Requestor will meet with Data Owners, Data Stewards, and Legal Counsel to review the request, data elements, and data use collaboratively.
	1. Granting Access.
		1. Once a User Access Request is reviewed and approved by the Data Owners, access privileges will be assigned to the Requestor. The Requestor will be required to have signed and abide by a confidentiality agreement and may be required to sign and abide by additional agreements or other documents to gain access, at the discretion of the Data Owner.
		2. As needed, Data Custodian and appropriate staff will meet with the Data Recipient to provide credentialing information and an overview of the data table(s) or dashboard(s) to which the user has been granted access.
		3. The Data Owner for all Data Sources for which the user has been given access will be notified that access has been granted, according to the applicable access provisioning process that is used.
		4. Contact information for the Data Recipient will be added to the Data Access List, maintained by the Data Office, with the appropriate date to revisit or terminate access (e.g. due to end of contract).
		5. All access that is granted to a Data Recipient will be the minimum necessary based on needs of the request, and for a duration not to exceed 12 months, with the option to renew the request at that time, unless otherwise agreed in writing.
	2. Terminating Access. The Data Owner will be responsible for maintaining and reviewing Data Access Lists of individuals authorized to access their Data Sources with Data Custodians quarterly and ensuring that each individuals’ access has been appropriately terminated by the Information Technology Division, as necessary.

## Request and Data Documentation Process

The Request and Data Documentation Process outlined below applies only to Data Office- involved requests. All aspects of the Request and Data Documentation Process outlined below are initiated by Data Office staff.

1. The Data Office will retain a copy of the fully executed Data Use Agreement (DUA) between the Data Recipient and Data Owner.
2. Data Office staff will follow the terms of the Data Sharing Agreement(s) entered into with the Data Owners whose data are included in the request. The process for electronically retrieving or transferring data may vary by Data Owner and by data type and will be detailed in the DSA(s).
3. Data Office and Data Integration Staff will adhere to all applicable state and federal laws, regulations, and policies when accessing or using data. Data Integration Staff will be responsible for securely receiving and storing all data received from each Party as outlined in the DSA(s).
4. As needed and approved by applicable Data Owners, Data Integration Staff will use standardized and replicable identity resolution strategies to integrate the data as needed for projects. Data Owners and/or Data Recipients may consult with the Data Integration Staff about preferred approaches to data integration.
5. Data Integration Staff will securely transfer data to the Data Recipients in accordance with the terms of the DSA and any applicable DUA.

## Oversight of Intradepartmental Data Requests

Oversight processes for intradepartmental requests are intended to facilitate all stakeholders have information about compliance with legal and ethical requirements as well as the outcome of projects and to enable all Parties, the Data Office, and Data Recipients have consistent and timely communication so that strategic data use can benefit NCDHHS and the lives of North Carolinians.

Should a Data Recipient use the data for purposes that were not approved pursuant to Section 8 of this MOU, a Data Owner may take action consistent with the terms of the DUA or, if no DUA applies, immediately terminate the Data Recipient’s access to the data, notify the NCDHHS Privacy and Security Office of the termination, require destruction of applicable data, and take other actions, including but not limited to any action that is required or permitted by law. It is the responsibility of the Data Owner or their designee to communicate to the Data Office and confirm this terminated access or data destruction as necessary.

Data Office Staff will monitor timely completion of the following documents from Data Recipients: 1) Project Reports, 2) Change Requests, 3) Key Findings and Interpretations Release Request, 4) Data Request Updates and Announcements, and 5) Certification of Project Completion and Destruction of Data.

1. Project Reports (recommended). Strongly recommended for research requests, but dependent upon terms of the DUA, Data Recipients will submit project reports to the Data Steward Group annually. The report will include:
	1. Copies of any updated IRB documents, including annual letters of approval issued by the reviewing IRB
	2. Summary of progress to date
		1. How data request is informing policy or practice
		2. Description of unanticipated findings
		3. Description of challenges encountered and how they are being resolved
	3. Products and key findings publicly released to date
	4. Project funding source (if applicable)
2. Change Requests (as needed). Data Recipients will initiate, when necessary, a change request. Minor requests (e.g., change in key personnel, a first-time extension of up to six months) will be reviewed by the Data Office. Major requests (e.g., additional research questions, change in the individual or organization conducting analyses, a request for additional data fields) will be reviewed by Legal Counsel for the Data Owners and the Data Steward(s) and/or Data Steward Group. Changes may require an amendment to the DUA.
3. Key Findings and Interpretations Release Request (Required for Research Requests and any request related to COVID-19 or Substance Use Disorder). Consistent with the terms of the DUA or DSA, Data Recipients may be required to share publications, presentations, or publicly shared work product that contain or have been derived from NCDHHS data with the Data Steward Group prior to publication or other public release. Data Steward(s) for the data that has been used by the Data Recipient to produce the publication, presentation, or other publicly shared work will review the materials and consult with Legal Counsel and the Privacy Office as necessary to ensure that the privacy and confidentiality of the individuals whose data was used is maintained and to ensure that any required attribution or disclaimer language has been included in the materials. The Data Stewards may also provide feedback to the Data Recipient about findings, conclusions, and any data idiosyncrasies, which Data Recipients who are external to NCDHHS may implement at their discretion. The Data Stewards will document completion of their review using a standard form. The Data Stewards can request product specific reviews (e.g., presentations, publications).
4. Certification of Project Completion and Destruction of Data (Required). This is a standard form that is automatically distributed by the Data Office and will require confirmation of data destruction consistent with the terms of the DUA.

## Communication Around the Data Request Process

1. Communications with the Requestor regarding recommendations made by the Data Stewards, including the need for revisions to an application, should come from the CDO, or designee.
2. The CDO or designee will provide updates to the Data Governance Executive Board and Data Governance Council at regular intervals on (a) Data Requests, (b) Major Change Requests, (c) summary of Minor Change Requests, and (d) Destruction of Data.
3. At each meeting of the Data Governance Executive Board and Data Governance Council, the CDO or designee will provide an update on high interest data requests, review results, key findings, and opportunities to learn more about requests (particularly research requests).
4. If the Parties, members of the Data Governance Executive Board, or members of the Data Governance Council have concerns about the fulfillment of a data request, a specific Project, or the governance process outlined herein, then the concerned individual(s) will work together in good faith to resolve the concern. The CDO or designee will be responsible for working with the Parties to resolve any concerns.

## Counterparts.

This IMOU may be executed in one or more counterparts, each of which will 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 will be deemed original for all purposes.

1. **Conflicts.**

The terms and conditions of this IMOU shall override and control any conflicting terms or conditions of any prior instance of this IMOU unless otherwise provided for in this IMOU. Notwithstanding the above, nothing in this IMOU shall override or control any conflicting terms or conditions of any other intradepartmental memorandum of understanding or data agreement previously entered into by a Party.

## IMOU Effective Date and Terms.

The effective date of this IMOU will be Click here to enter text., 20 Click here to enter text.. This IMOU will remain in effect for a term of five (5) years from the effective date and reviewed annually unless otherwise terminated as provided for in this IMOU. A Party to this IMOU may terminate its participation in this IMOU by providing written notice signed by the Party to the CDO.

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

[NCDHHS SIGNATURE]

[NCDHHS Office of the Secretary]

[NCDHHS SIGNATURE]

[NCDHHS Data Office]

Dated: Click here to enter text.

Dated: Click here to enter text.

# EXHIBIT A

## (Sample Form) Joinder Agreement

Pursuant to, and in accordance with the NCDHHS Intradepartmental Memorandum of Understanding (IMOU), effective Click here to enter text., 20 Click here to enter text., the entity signing this Joinder Agreement (the “New Party”) hereby acknowledges that it has received and reviewed a complete copy of this IMOU. The New Party agrees that upon execution of this Joinder, it will become a Party to this IMOU and swill be fully bound by and subject to all of the terms and conditions of this IMOU. In witness thereof, the New Party has caused its duly authorized representative to execute this Joinder Agreement, as follows:

[New Party’s Name]

By: Click here to enter text.

[Name of Official, Title] Date: Click here to enter text.