Terms

These are key terms related to data sharing, governance, and management, as used in the NCDHHS Data Sharing Guidebook, ensuring a common understanding of terminology and facilitating effective communication and compliance with data policies and regulations.

Aggregation
Combining data about individuals while protecting individual privacy by using groups of individuals or whole populations rather than isolating one individual at a time.

Audit Request Pathway
Request by an oversight or regulatory entity for a systematic review and analysis of an organization's data for compliance, financial, or quality purposes.

Breach
An incident wherein information is taken from a system without the knowledge or authorization of the system's owner. This could be inadvertent, accidental, or malicious. A data breach can occur within a small company or a large organization, and it may involve sensitive, proprietary, or confidential information, such as credit card or bank details, personal health information (PHI), personally identifiable information (PII), trade secrets of corporations, or intellectual property. Also called Cyber Breach or Data Breach.

Business Associate Agreement (BAA)
Outlines each party's responsibilities of safeguarding protected health information (PHI). A BAA is a critical document that ensures both parties understand their roles in protecting PHI. It includes the permissible uses and disclosures of PHI, the appropriate safeguards to be implemented, and the responsibilities in case of a breach of PHI.

Business Intelligence
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 DHHS' programmatic or business needs.

Business Users
Individuals within an organization who utilize various resources, tools, and systems to perform tasks related to their specific roles and responsibilities in achieving the organization's objectives. They often interact with technology platforms, applications, and data to facilitate decision-making, manage operations, and drive business growth.

Chief Data Officer (CDO)
Individual responsible for overseeing Data Office activities, including facilitating Data Governance-related committees, developing partnerships, overseeing staff and technical activities, consulting with Data Recipients, monitoring requests, and managing document inventory.

Confidential Data
Data with restricted access, use, or disclosure according to state or federal law, regulation, or policy.

Confidential Disclosure Agreement
Outlines permissible disclosures of confidential data and information between a third-party and NCDHHS, usually generated by and at the request of the third party.

Data Asset Inventory
An inventory that is updated annually by Divisions and Offices and includes information about high-value data assets across NCDHHS.

Data Classification
The classes determine the level of security that must be placed around the data.

Data Custodian
Oversees the safe transport, storage, and disposition of data, including infrastructure, activities, and safeguards required to maintain the confidentiality, integrity, and availability of the data. Collaborates with the Data Stewards to ensure data availability. Communicates with Data Owner and Data Steward regarding any data management issues that pose a risk to data security and/or access.

Data Dictionary
A centralized repository of information about data (e.g., meaning, origin, usage, format, relationship to other data elements). A file that defines the organization of a database.

Data Element
A basic unit of data that has a unique meaning and distinct values or attributes.

Data Governance
The people, processes, and technology required for data quality, integrity, availability, usability, and security throughout its lifecycle. Can also be referred to as a set of processes that ensures that data assets are formally managed throughout the enterprise.

Data Integration
Combining data sets through record linkage to understand multi-program and multi-service relationships, involving personal identifiers or a unique ID for linking records.

Data Integration Staff
Individuals handling and securing data for approved uses, responsible for consulting with Party staff, cleaning data, linking data, and preparing it for use.

Data Management and Strategic Use Purposes
Encompasses Data Management, Data Quality, Data Improvement Activities, and Operational and Business Intelligence Activities. Individuals within the NCDHHS Data Office and ITD responsible for handling and securing Confidential Data for approved uses. They consult with Party staff, clean data, link data, and prepare data for approved use.

Data Minimization
The idea that one should only collect or share the personal data that is necessary to achieve a specific goal.

Data Office
An office within the North Carolina Department of Health and Human Services responsible for overseeing the management and governance of the organization's data assets. This team ensures that data is accurately collected, maintained, and used in a manner that supports NCDHHS's mission while adhering to legal, ethical, and policy standards, including compliance with HIPAA and other relevant regulations.

Data Owner
Individuals with the authority to legally bind a Party and authorize data release for specific projects. They are responsible for provisions of Data Sharing Agreements and have signatory authority for access and use of these data for permissible purposes.

Data Receiver
An individual or entity that is granted access to and receives data from another source or party within the department. This role typically comes into play after a data request is approved, and the data is transferred to the receiver for a specific, authorized use.

Data Recipient
Individual or entity requesting data for NCDHHS operational, business intelligence purposes, research, or approved use.

Data Request Reviewer Worksheet
A tool used to guide the review of data requests, ensuring they align with legal, ethical, and strategic priorities.

Data Requestor
An individual or entity that formally requests access to a specific data set or information resource within the department. This role initiates the data access process by submitting a structured request that outlines the purpose, scope, and intended use of the requested data.

Data Reviewer
Supports strong review practices to ensure data access and use are legal, ethical, and align with the department's priorities.

Data Sharing
The collaborative and secure exchange of data information among various entities within the department and its affiliated organizations. This can include sharing data for research, policymaking, and improving public health outcomes while adhering to privacy and security regulations.

Data Sharing Agreement (DSA)
Documents terms and conditions for intradepartmental data sharing of Confidential Data, including data transfer and security for Data Recipients.

Data Source
A discrete data set or system owned by a Party, each having its own Data Owner.

Data Steward
Includes the processes involved with acquiring, storing, using data, as well as the data's security and quality. Data stewards are staff with assigned or designated responsibility who have direct operational-level responsibility for information management.

Data Stewards Group
Committee of representatives with expertise on respective Data Sources, reviewing data requests and proposed projects for methodological and analytical soundness.

Data Storage
The process of storing, managing, and preserving digital data in a structured and organized manner for future use. The method for storing data will depend upon whether data are open (publicly available) or restricted (confidential).

Data Transfer
The process of moving data from one location to another, which must be secure if the data are confidential or restricted.

Data Use Agreement (DUA)
Agreement outlining terms for Data Owner(s) providing Data Recipient with data access, including objectives, methodology, permitted uses, security plans, completion dates, and terms for data destruction.

Data Use Priorities
The Department of Health and Human Services works to advance the health, safety, and well-being of all North Carolinians in collaboration with a wide array of partners and stakeholders.

Data User
An individual or entity that actively engages with, analyzes, or processes data as part of their operational, research, or administrative responsibilities within the department.

De-identification Standards under FERPA
Refers to the protocols and procedures used to remove or obscure personal identifiers from education records, ensuring that the information cannot be used to identify individual students.

De-identified Data
Data modified by removing personally identifiable information to reduce the identification likelihood of the individuals concerned.

Equity
Refers to the principle of fairness and justice in the way people are treated and provided access to opportunities and resources.

Exploratory Data Classification
Refers to data that is initially being analyzed or reviewed to determine its potential for further use, sharing, or in-depth analysis.

Family Educational Rights and Privacy Act (FERPA)
Sets out requirements for the protection of students' education records and provides parents and eligible students certain rights with respect to the student's education records.

Health Insurance Portability and Accountability Act (HIPAA)
A federal law with specific requirements to maintain the privacy and security of "protected health information."

High Value Data Assets
Critical data assets identified by Divisions or Offices, supporting NCDHHS operations, strategic goals, public knowledge, frequently requested by the public, satisfying legislative/reporting requirements, or identified through public consultation.

Identifiable Data
Data that includes personal identifiers that can link the information to specific individuals.

Informed Consent
Involves providing an individual with sufficient information to determine if they consent to an action.

Institutional Review Board (IRB)
A group that reviews and monitors research involving human subjects to ensure ethical standards are met.

Institutional Review Board (IRB) Approval
Process by which a committee formally reviews and approves research involving human subjects to ensure that it is conducted ethically and in accordance with regulatory standards.

Integrated Data
Data combined from different sources to provide a comprehensive view, enhancing analysis and decision-making.

Intra-Departmental Memorandum of Understanding (IMOU)
Documents the purpose and governance process. The IMOU will be signed by all data partners as they enter the collaboration.

Legal Counsel
Defined by the NCDHHS Office of General Counsel, it refers to the legal advisors or representatives for NCDHHS.

Legal Request Pathway
Request related to a subpoena, court order, discovery, litigation, investigation, and/or as instructed by a NCDHHS attorney or the NC Department of Justice.

Legislative Data Request Pathway
Request from or on behalf of a legislative member, committee, or Division.

Limited Data Set (LDS)
A data set that excludes many identifiers but not all, allowing for some geographic details and dates, as defined under 45 CFR §164.514(e).

NCDHHS Priorities
Strategic focuses or goals set by NCDHHS to guide operations and decision-making.

Open (Public) Data
Data that can be shared openly, either at the aggregate or individual level, based on state and federal law.

Operational and Business Intelligence Activities
Activities involving data integration or exploratory analysis to answer policy and business questions and meet other needs.

Operational Data Request Form
Form used to submit requests related to ongoing work of NCDHHS and supports business intelligence with a Division, Office, strategic partner (under a current agreement with NCDHHS), including local offices.

Operational Data Request Pathway
Requests related to ongoing work of NCDHHS and supports business intelligence with a Division, Office, strategic partner (under a current agreement with NCDHHS), including local offices.

Privacy
Data released to the requestor must be kept secure and cannot be shared with unauthorized users.

Public Request Pathway
A process governed by NC state law allowing individuals to request public records without needing to disclose their identity or request purpose.

Quality Improvement
An ongoing process to identify, analyze, and implement changes aimed at improvement by assessing strengths and weaknesses.

Reporting
Collecting and formatting raw data and translating it into a digestible format to fulfill business requirements, compliance activities, or assess performance.

Research Request Form
Form used to submit requests related to Research conducted in partnership with NCDHHS.

Research Request Pathway
Request that will be used for "a systematic investigation designed to contribute to generalizable knowledge." Institutional Review Board (IRB) review and approval may be required.

Restricted Data
Data that can be shared, but only under specific circumstances with appropriate safeguards in place.

Row Level Data
Data provided at the most granular level, where each row represents a single record.

Strategic Partner
An individual, agency, organization, company, local office, or other entity that is under current agreement with NCDHHS, and conducting ongoing work of NCDHHS that supports operational and business intelligence.

The Privacy and Security Officer (PSO)
Provides security policy, advisory service, and disposal for data access and use. Ensures that all data handling and usage comply with relevant security and privacy standards.

Unavailable Data
Data that cannot or should not be shared, either because of state or federal law, lack of digital format, or due to data quality or other concerns.

Waiver of HIPAA Authorization
Approval from an Institutional Review Board (IRB) to use or disclose protected health information (PHI) without the patient's explicit consent under specific conditions, typically for research purposes, when obtaining consent is impracticable and the research poses minimal risk to privacy.

Waiver of Informed Consent
Approval from an Institutional Review Board (IRB) to conduct research without obtaining informed consent from participants under specific circumstances, such as when the research involves minimal risk to participants and the waiver will not adversely affect their rights and welfare.

Updated 5/24/24

This glossary is intended to be a living document, updated regularly to reflect new terms and evolving definitions in the field of data management.