North Carolina Longitudinal Data Service

Privacy Threshold Analysis (PTA) and Security Form

Preamble

The NCDIT Privacy Threshold Analysis (PTA) for NCLDS is used to gather information about each NCLDS Data Request involving exposure of Personal Identifiable Information (PII) and/or Protected Health Information (PHI) to determine if any information privacy concerns exist, and to document that the Data Request meets the requirements for the transfer of data.

The PTA process maps Data Request information to NCDIT's requirements for the movement of sensitive data and identifies required information and documentation that should be submitted with the PTA for review by the NCLDS Team and NCDIT Privacy Team.

A Data Request must meet privacy safeguarding requirements before data sets containing PII/PHI can be transferred to a Requester. The data usage must be legal and must align with the Fair Information Practice Principles (FIPPs) (see https://www.fpc.gov/resources/fipps), and there must be a written and signed Data Use Agreement in place prior to the transfer of data.

If you have questions about this template or process, please contact the NCLDS Team and the NCDIT Privacy Team.

NCDIT Privacy Team: DITPrivacy@nc.gov

NCLDS Team: NCLDShelp@nc.gov

A. Data Request Information	
Data Request ID	
Project Title	
Date Data Request Initiated	

NCDIT Lead/POC	
Title	NCLDS Executive Director
Email	ncldshelp@nc.gov

Description of Use/Overview:
Provide a comprehensive overview of the use case data request in plain language, excluding abbreviations, that includes identification of the type(s) of data (personal, employment, financial, medical, etc.); whose PII/PHI it is (employee, student, patient data, etc.); the purpose of the use, and the limitations on the use.
Overview

Project Purpose/Objectives

Federal and/or State Privacy Standards/Statutes/ Policies to which the Data in the Request may be Subject

IDEA Part C (DHHS, NCDPI)	□
FERPA (DHHS, NCDPI, NCCCS, UNCSO, NCICU)	□
HIPAA (DHHS)	□
NCGS §§ 9S-4(x), 143B-7, & 143B-10 (Commerce)	□
20 CFR Part 603, subpart B (Commerce)	□
Internal Revenue Code (Commerce)	□
CJIS	□
Other	□
If Other, please list:	

Data Requested

To view/open the Data Requested extract, please see the associated link provided in the NCLDS Data Selector Application.

Summary of PII/PHI Usage (Select one)	
Data Request made by NCLDS Contributors: Per the NCLDS Contributor Memorandum of Understanding (7.b): "Reports requested by and disclosed to a [Contributor] shall contain UIDs unless prohibited by Applicable Law or by a restriction put in place by the relevant Contributor. If the Contributors responding to a Request determine that other PII or identified Data should or must be shared to fulfill the Request, other identified Data may be shared upon mutual agreement by the relevant Contributors. The receiving Party must comply with privacy and security protections included in this Agreement and all Applicable Law."	□
All other Data Requests: Per NCLDS Contributor MOU (8.a): "GDAC, with assistance from the relevant Contributors, shall i. De-identify Data, including the removal of UIDs, before generating Reports for Requestors who are not Parties to this Agreement. The Parties shall assign random unique identifiers to De-Identified Data in the Reports to replace the UIDs; ii. Provide Requestors with relevant Metadata; iii. Perform small cell suppression to the most restrictive level based on the Data disclosed by the relevant Contributors; and iv. Screen for Secondary Disclosures."	□

Data Request ID	
Does the contract Data Use Agreement include PII/PHI handling language?	
Yes; see Sections 1, 4, 5, and 6 of the Data Use Agreement	●
No	○
To view/open the Data Use Agreement (DUA), please see the associated link provided in the NCLDS Data Selector Application.	

Primary Contact	
Full Name	
Do Project Personnel require access to PII/PHI?	
Yes	●
No	○

First and Last Name	NCID	Role on Project	Added by	Status	Status Date

B. Purpose	
Data requests need to fit within one of the following purposes. (Select ALL that apply)	
A. To improve data quality, data automation, and data linking of common enterprise data across the State.	☑
B. To implement shared internal compliance controls for data governance including enhanced auditing capabilities across the enterprise.	□
C. To provide a platform for shared service and business system optimization analytics across the enterprise, to include predictive models used to estimate program or policy reach, effectiveness, and/or impact.	☑
D. To make data more easily accessible, standardized, efficiently processed, and useful across the State.	☑

C. Data Subjects	
Identify the categories of individuals present in the data request data. (*Select ALL categories that apply*)	
Employees	□
Children (0-5)	□
Students (K-12)	□
Students (postsecondary & continuing education)	□
Patients	□
Incarcerated Individuals	□
Other	□
If Other, describe	

D. Types of Information and Risk Impact

I. Types of Information

Identify the types of information that will be accessed as part of this Data Request.
(*Select each category required*.)

Personal Information		Employment Information		Personal Financial Information		Medical Information	
Name	□	Employment status	□	Pay, wage, earnings information	□	Inpatient and outpatient medical records	□
ID Number (e.g., eScholar UID, CNDS, etc.)	□	Duty Position	□	Separation information	□	Pharmacy records	□
Social Security Number (SSN)	□	Leave balances and history	□	Financial benefit records	□	Immunization records	□
Full or Partial Address (including ZIP code only)	□	Work Schedules	□	Income tax withholding records	□	Medical and physical board records	□
Email Address(es)	□	Individual Personnel Records	□	Accounting Records	□	Neuropsychological functioning and cognitive testing data	□
Date of Birth (even if year of birth only)	□	Retirement Records	□			Health assessments	□
Gender	□	Sponsor Duty Location	□				
Branch of Service	□	Unit of Assignment (UIC)	□				
Citizenship	□	Occupation	□				
Defense Enrollment Eligibility Reporting System benefit number(DEERS Beneficiary ID)	□	Rank	□				
Sponsorship and beneficiary information	□	Skill specialty	□				
Race and ethnic origin	□	Security Clearance Information	□				

List any additional sensitive data you plan to use that is not identified above:

II. Risk Impact of Data

What is the impact of the collected information on identifying a specific individual?

	Low	Moderate	High
Identifiability	Data elements are not directly identifiable alone but may indirectly identify individuals or significantly narrow large datasets.	Combined data elements uniquely and directly identify individuals. (e.g., driver's license + financial information)	Individual data elements directly identify specific individuals. (e.g., SSN, EDIPI)
	○	○	○

What is the impact of the potential loss, compromise, or disclosure of PII?

	Low	Moderate	High
Quantity of PII	A limited number of individuals affected by a loss, theft, or compromise. Limited collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach.	A serious or substantial number of individuals affected by loss, theft, or compromise. Serious collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach. Aggregation of a serious or substantial amount of data.	A severe or catastrophic number of individuals affected by loss, theft, or compromise. Severe or catastrophic collective harm to individuals, harm to the organization's reputation, or cost to the organization in addressing a breach. Aggregation of a significantly large amount of data, e.g., "Big Data."
	○	○	○

What is the sensitivity level of the data elements?

	Low	Moderate	High
Data Element Sensitivity	Data fields, alone or in combination, have little relevance outside the context.	Data fields, alone or in combination, may be relevant in some other contexts and may, in those contexts, make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.	Data fields, alone or in combination, are directly usable in other contexts and make the individual or organization vulnerable to harms, such as identity theft, embarrassment, loss of trust, or costs.
	○	○	○

What is the impact of the disclosure of the information collected?			
	Low	Moderate	High
Context of Use	Disclosure of the act of collecting and using the PII, or the PII itself, is unlikely to result in harm to the individual or organization. (E.g.: name, address, and phone numbers of a list of people who subscribe to a general-interest newsletter.)	Disclosure of the act of collecting and using the PII, or the PII itself, may result in harm to the individual or organization. (E.g.: name, address, and phone numbers of a list of people who have filed for retirement benefits.)	Disclosure of the act of collecting and using the PII, or the PII itself, is likely to result in severe or catastrophic harm to the individual or organization. (E.g.: name, address, and phone numbers of a list of people who work undercover in law enforcement.)
	○	○	○

What is the impact of the location and access to the data?			
	Low	Moderate	High
Access to and Location of PII	Located on computers and other devices on an internal network. Access limited to a small population of the organization’s workforce, such as a program or office that owns the information on behalf of the organization. Access only allowed at physical locations owned by the organization (e.g., official offices). Backups are stored at government-owned facilities. Employees or contractors do not store or transport PII off-site.	Located on computers and other devices on a network controlled by the organization. Access limited to multiple populations of the organization’s workforce beyond the direct program or office that owns the information on behalf of the organization. Access only allowed by organization-owned equipment outside of the physical locations owned by the organization only with a secured connection (e.g., virtual private network (VPN)). Backups are stored at contractor-owned facilities.	Located on computers and other devices on a network not controlled by the organization or on mobile devices or storage media. Access open to the organization’s entire workforce. Remote access allowed by equipment owned by others (e.g., personal mobile devices). Information can be stored on equipment owned by others (e.g., personal USB drive).
	●	○	○

E. Source System Information	
Agency and Source System Names	
Early Childhood Integrated Data System (ECIDS), Department of Health and Human Services (DHHS)	□
NC SchoolWorks (NCSW), Department of Public Instruction (NCDPI)	□
NC Community College System (NCCCS)	□
UNC System Office (UNCSO)	□
NC Independent Colleges and Universities (NCICU)	□
Common Follow-Up System (CFS), Department of Commerce	□

Agency System Owners		
ECIDS/DHHS	Name	
	Office Phone	
	Email	
NCSW/NCDPI	Name	
	Office Phone	
	Email	
NCCCS	Name	
	Office Phone	
	Email	
UNCSO	Name	
	Office Phone	
	Email	
NCICU	Name	
	Office Phone	
	Email	
CFS/Commerce	Name	
	Office Phone	
	Email	

Agency Privacy Office(s)		
ECIDS/DHHS	POC Name	
	Office Phone	
	Email	
NCSW/NCDPI	POC Name	
	Office Phone	
	Email	
NCCCS	POC Name	
	Office Phone	
	Email	
UNCSO	POC Name	
	Office Phone	
	Email	
NCICU	POC Name	
	Office Phone	
	Email	
CFS/Commerce	POC Name	
	Office Phone	
	Email	

Authority

Cite the authority for the agency to collect, use, maintain and/or disseminate and cite the specific provision(s) that authorizes the operation of the system, collection of PII/PHI, and use as intended PII

§ 143B-1321. Powers and duties of the Department [NCDIT]; cost-sharing with exempt entities.
(a) The Department shall have the following powers and duties:
(1) Provide information technology support and services to State agencies.
(2) Provide such information technology support to local government entities and others, as may be required.
. . .
(4) Assist State agencies in meeting their business objectives.
(5) Plan and coordinate information technology efforts with State agencies, nonprofits, and private organizations, as required.
(6) Establish a consistent process for planning, maintaining, and acquiring the State's information technology resources. This includes responsibility for developing and administering a comprehensive long-range plan to ensure the proper management of the State's information technology resources.
(7) Develop standards and accountability measures for information technology projects, including criteria for effective project management.
(8) Set technical standards for information technology, review and approve information technology projects and budgets, establish and enforce information technology security standards, establish and enforce standards for the procurement of information technology resources, and develop a schedule for the replacement or modification of information technology systems.
. . .
(12) Operate as the State enterprise organization for information technology governance.
(13) Advance the State's technology and data management capabilities.
. . .
(18) Prescribe the manner in which information technology assets, systems, and personnel shall be provided and distributed among agencies, to include changing the distribution when the State CIO determines that is necessary.
. . .
(21) Establish and operate, or delegate operations of, centers of expertise (COE) for specific information technologies and services to serve two or more agencies on a cost-sharing basis, if the State CIO, after consultation with the Office of State Budget and Management, decides it is advisable from the standpoint of efficiency and economy to establish these centers and services.
(22) Identify and develop projects to facilitate the consolidation of information technology equipment, support, and projects.
(30) Support the operation of the CGIA, GICC, GDAC [Government Data Analytics Center, home of NCLDS], and 911 Board.

§ 116E-4. Powers and duties of the Center [GDAC].

(a) The Center shall have the following powers and duties with respect to the System:
. . .
(2) Provide general oversight and direction to the System.

§ 116E-5. North Carolina Longitudinal Data System.
. . .
(c) The System shall be considered an authorized representative of the Department of Public Instruction, The University of North Carolina, and the North Carolina System of Community Colleges under applicable federal and State statutes for purposes of accessing and compiling student record data for research purposes.
(d) The System shall perform the following functions and duties:
(1) Serve as a data broker for the System, including data maintained by the following:

a. The Department of Public Instruction.
b. Local boards of education, local school administrative units, and charter schools.
c. The University of North Carolina and its constituent institutions.
d. The Community Colleges System Office and local community colleges.
e. The North Carolina Independent College and Universities, Inc., and private colleges or universities.
f. Nonpublic schools serving elementary and secondary students.
g. The Department of Commerce, Division of Employment Security.
h. The Department of Revenue.
i. The Department of Health and Human Services.
j. The Department of Labor.

Using Data Sets NCDIT/ NCLDS has ingested

Does the data request involve using one or more data sets already ingested in NCDIT/ NCLDS?

Yes	○
No	●

If yes, has a Restricted Data Access Request to obtain permission to use the data been completed?

Yes	○
No	○
N/A	●

Has the request been approved by the data owner?

Yes; the Data Use Agreement governing the request is attached	●
No	○

Source Agency Privacy Office Agreement:

Have the agency source system privacy offices agreed with the intended use of the data?

Yes	●
No	○
If No, please explain why	

Use Limitations and Required Safeguards

List all limitations on the use of the data and required safeguards by the privacy office or data owner

Limitations on the use of data exposed to NCLDS and approved Requesters, in addition to those prescribed by the attached Data Use Agreement and all relevant state and federal statutes pertinent to each data element (e.g., FERPA, HIPAA, etc.), include the following:

§ 116E-2. Purpose of the North Carolina Longitudinal Data System.
(b)The linkage of student data and workforce data for the purposes of the System shall be limited to no longer than five years from the later of the date of the student's completion of secondary education or the date of the student's latest attendance at an institution of higher education in the State. (2012-133, s. 1(a).)

Data Retention Limits

Cite the data retention limits relevant to the approved Data Request

The requested records will be used to perform longitudinal statistical analyses in accordance with the project description in Part A.

Records are retained over the course of the approved period of the project (as detailed in the Data Use Agreement) in a secure server vetted by NCDIT, NCLDS, and/or its Contributor partners, in accordance with requirements established by NCDIT ESRMO.

Data Use Agreement

To view/open the Data Use Agreement (DUA) documentation, please see the associated link provided in the NCLDS Data Selector Application

Source System Information

Source System IL Level (e.g., IL-4) Note: For Cloud based systems only	
Source System RMF Data Categorization (e.g., H-M-M)	

Will you be linking data across systems?

Yes. Unless otherwise noted here, data will be linked across all approved data sources.	●
No	○

If you answered “Yes” above, what System(s) will you be linking data from/to?

Data will be linked among all of the systems indicated at the top of this page in accordance with the linkage requests included in the approved Data Request form

Will you be using person-level/individual-level data?

Yes	○
No	○

Will PII be exposed to the end user directly?

Yes	○
No	○

If yes, what fields are being removed or modified? What fields are being retained for end use?

To view/open the Data Elements Selected extract, please see the associated link provided in the NCLDS Data Selector Application.

Will you be linking data using a personal identifier or identifiers? (SSN, EDIPI, Name, DEERS ID, etc.)	
Yes	○
No	○
Which personal identifier(s) will be used?	
How will you be using the personal identifier(s)?	
Raw	○
Hashed	○
Masked	○

F. Risk Assessment (Data Privacy and Protection)

PII is accessed by NCLDS to facilitate and enable the exchange of student data among agencies and institutions within the State, generate timely and accurate information about student performance that can be used to improve the State's education system and guide decision makers at all levels, and facilitate and enable the linkage of student data and workforce data, per NCGS 116E-2. Data is collected from source systems in a raw form that contains PII. The PII is used to join data sets together as a unique key. In a limited set of data requests, authorized users with a need to know may be able to view PII. PII will also be used as inputs to population analytics; the resultant population analytics data will be aggregated at the unit level, but all appropriate protections will be in place to mitigate risk to the individual.

How many unique individuals will be identified in the data?	*Data Summary sheet available in NCLDS Data Selector Application*

Will the complete data set be used or will segments of the data be used? If a segment, what fields?

The entirety of the data sets resulting from the linkages described on the previous page will be used by the approved Data Requester.

Is PII exposed to the end user directly or will it be removed?

Exposed	○
Removed	○

What PII fields are being retained for end use?

Which data elements are being hashed?

Will only authorized users with a need to know be able to view PII/PHI in data request data?	
Yes	●
No	○
How is this access decided and enforced?	
Per Data Contributor approval of the Data Requester's team members proposed for authorized use in the approved Data Request (Stage B, Item II.a), and as enforced via the terms of the Data Use Agreement	
Will the data be aggregated at the unit level?	
Yes	○
No	○
If you answered “No” please explain why and under what circumstances.	

How are data protected while in the custody of NCLDS during dataset preparation? What administrative, technical, and physical safeguards will be implemented to protect the data throughout the NCLDS data preparation lifecycle?

Administrative:
• Employee training and agreement to a Non-Disclosure Agreement (NDA) are a pre-requisite for access to Vendor-hosted NCLDS applications and data and are renewed annually. Training topics include: Acceptable use of system and customer materials, cybersecurity incident prevention measures, privacy training, specialized training to comply with laws applicable to all data types (e.g., HIPAA, FERPA, etc.).

Technical:
• The Vendor encrypts all data during transit and at rest.
• Access control to all Vendor-hosted NCLDS applications and data is controlled through NC SEAT (North Carolina SAS Enterprise Authentication Tool) security roles and governance requirements. Access is granted only to authorized individuals.
• All Vendor-hosted NCLDS applications are integrated with NCID and require Multi-Factor Authentication.
• Penetration testing is used to assess risk and vulnerability prior to all major releases of Vendor-hosted NCLDS applications. If risks are identified, Vendor will mitigate and remediate issues found per the contract terms.

Physical:
• NCLDS data resides within a dedicated managed and hosted customer environment. Data is kept and remains logically separate from other customer data, unless otherwise defined in applicable agreements, approved for transfer by appropriate Vendor and customer management, or customer solution requirements.

If this data request involves PHI, are there measures in place to ensure HIPAA compliance (i.e. no re-identification)?

Yes	●
No	○

Do these safeguards meet the data owner and privacy office requirements?

Yes	●
No	○

Do they meet the requirements specified in the legal agreements (typically MOAs) that allow NCLDS access to the data for the purposes of data preparation for fulfilling an approved Data Request?

Yes	●
No	○

G. Joining Data Sets	
Will the data request require the joining of data sets?	
Yes	◉
No	○
If “Yes”, please explain the need to be met through joining:	

Has the privacy office representative for each data set agreed to this use?	
Yes	●
No	○
Has the joining of data and agreement of parties to this type of use been made part of a DUA?	
Yes	●
No	○

H. Security Review (Required Security Office Information)

Receiving Agency Security Office (Information Security Officer [ISO] or delegated official):

Office Name	
POC Name	
Office Phone	
Email	

Receiving Agency Security Attestation

Has the source agency provided attestation of their hosting environment such as: ISO27001, HITRUST, FedRAMP, SOC II Type 2 or Vendor Readiness Assessment Report?

NOTE: To view/open the Security Attestation Supporting documentation, please see the associated link(s) provided in the NCLDS Data Selector Application.

Yes, ISO27001	□
Please provide documentation	
Yes, HITRUST	□
Please provide documentation	
Yes, FEDRAMP	□
Please provide documentation	
Yes, SOC II Type 2	□
Please provide documentation	
Yes, Vendor Readiness Assessment	□
Please provide documentation	
No	□

Receiving Agency Security Attestation	
If no, can the receiving system otherwise demonstrate NIST 800-53 compliance?	
Yes	○
Please provide documentation	
No	○
If no, is the receiving system NIST 800-171 compliant?	
Yes	○
Please provide documentation	
No	○
Can the data security authority for the receiving system attest via the HECVAT On-Prem to the security of the receiving system?	
Yes	○
Please provide documentation	
No	○

NOTE: To view/open the Security Attestation Supporting documentation, please see the associated link(s) provided in the NCLDS Data Selector Application.

Assessment of Receiving Agency Risk Impact

Has the impact of exposure been reviewed with the security office?

Yes	○
No	○

Has the impact and location of data been reviewed with the security office?

Yes	○
No	○

Has the overall project been reviewed with the agency security office?

Yes	○
No	○

*NCLDS will work in partnership with Data Contributors impacted by each Data Request to secure the necessary receiving system security attestation from the Data Requester.

I. Documentation

Data Request

To view/open the NCLDS Data Request please see the associated link provided in the NCLDS Data Selector Application.

Data Use Agreement (DUA) with embedded Information Security Agreement language

To view/open the NCLDS Data Use Agreement (DUA) please see the associated link provided in the NCLDS Data Selector Application.

Next Steps

Once the PTA is complete, the NCDIT Privacy Team will review the PTA and documentation to determine next steps. The Team will reach out to the Lead concerning questions or clarifications. The Team will provide a written recommendation for next steps. Data requests that require Department-level privacy review or higher will be identified.