GENERAL ASSEMBLY OF NORTH CAROLINA
SESSION 2025

H.B. 819
Apr 7, 2025
HOUSE PRINCIPAL CLERK

H D

HOUSE BILL DRH10370-MQa-98

Short Title:	DIT Agency Bill.	(Public)
Sponsors:	Representative Johnson.	
Referred to:		

A BILL TO BE ENTITLED

AN ACT TO MAKE VARIOUS CHANGES TO THE GENERAL STATUTES RELATED TO THE DEPARTMENT OF INFORMATION TECHNOLOGY, COMMUNICATIONS SERVICES, AND TELECOMMUNICATIONS.

The General Assembly of North Carolina enacts:

PART I. NC LONGITUDINAL DATA SYSTEM

SECTION 1.1. Chapter 116E of the General Statutes reads as rewritten:

"**Chapter 116E.**

"**~~Education~~ North Carolina Longitudinal Data System.**

"**§ 116E-1. Definitions.**

(1) ~~"Center" means the~~ Center. – The Governmental Data Analytics Center as established in Part 8 of Article 15 of Chapter 143B of the General Statutes.

(1a) CJIS. – The federal Criminal Justice Information Systems in 28 C.F.R. Part 20.

(2) ~~"De-identified data" means a~~ De-identified data. – A data set in which parent and student identity information, including the unique student identifier and student social security number, has been removed.

(3) ~~"FERPA" means the~~ FERPA. – The federal Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.

(3a) HIPAA. – The federal Health Insurance Portability and Accountability Act of 1996.

(3b) IDEA. – The federal Individuals with Disabilities Education Act, 20 U.S.C. §§ 1400, et seq.

(3c) Public school. – As defined in G.S. 115C-5(7a).

(4) ~~"Student data" means data~~ Student data. – Data relating to student performance. Student data includes State and national assessments, course enrollment and completion, grade point average, remediation, retention, degree, diploma or credential attainment, enrollment, discipline records, and demographic data. Student data does not include juvenile delinquency records, criminal records, and medical and health records.

(5) ~~"System" means the~~ System. – The North Carolina Longitudinal Data ~~System.~~System, including components referred to as the North Carolina Longitudinal Data Service.

(6) ~~"Unique Student Identifier" or "UID" means the~~ Unique Student Identifier or UID. – The identifier assigned to each student by one of the following:

a. A ~~local school administrative unit~~ public school based on the identifier system developed by the Department of Public Instruction.
b. An institution of higher education, nonpublic school, or other State agency operating or overseeing an educational program, if the student has not been assigned an identifier by a ~~local school administrative unit.~~public school.

(7) ~~"Workforce data" means data~~ Workforce data. – Data relating to employment status, wage information, geographic location of employment, and employer information.

"**§ 116E-2. Purpose of the North Carolina Longitudinal Data System.**

~~(a)~~ The North Carolina Longitudinal Data System is a statewide data system that contains individual-level student data and workforce data from all levels of education and the State's workforce. The purpose of the System is to do the following:

(1) Facilitate and enable the exchange of student data among agencies and institutions within the State.
(2) 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.
(3) Facilitate and enable the linkage of student data and workforce data.

~~(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.~~

…

"**§ 116E-4. Powers and duties of the Center.**

(a) The Center shall have the following powers and duties with respect to the System:

…

(4) Before the use of any individual data in the System, the Center shall do the following:
a. Create and publish an inventory of the ~~individual student~~ data proposed to be accessible in the ~~System and required to be reported by State and federal education mandates.~~System.
b. Develop and implement policies to comply with ~~FERPA~~ FERPA, IDEA, HIPAA, CJIS, the Internal Revenue Code, and any other privacy ~~measures,~~ measures relevant to data available to the System, as required by law or the Center.
c. Develop a detailed data security and safeguarding plan that includes the following:
1. Authorized access and authentication for authorized access.
2. Privacy compliance standards.
3. Privacy and security audits.
4. Breach notification and procedures.
5. Data retention and disposition policies.

(5) Oversee routine and ongoing compliance with ~~FERPA~~ FERPA, IDEA, HIPAA, CJIS, the Internal Revenue Code, and other relevant privacy laws and policies.
(6) Ensure that any contracts that govern databases that are outsourced to private vendors include express provisions that safeguard privacy and security and include penalties for noncompliance.
~~(7) Designate a standard and compliance time line for electronic transcripts that includes the use of UID to ensure the uniform and efficient transfer of student~~

~~data between local school administrative units and institutions of higher education.~~

(8) Review research requirements and set policies for the approval of data requests from State and local agencies, the General Assembly, and the public.

(9) Establish an advisory committee on data quality to advise the Center on issues related to data auditing and tracking to ensure data validity.

(b) The Center shall adopt rules according to Chapter 150B of the General Statutes as provided in G.S. 116E-6 to implement the provisions of this Article.

(c) The Center shall report annually to the Joint Legislative Education Oversight Committee, the Joint Legislative Commission on Governmental Operations, and the Joint Legislative Oversight Committee on Information Technology beginning July 1, 2019. The report shall include the following:

(1) An update on the implementation of the System's activities.

(2) Any proposed or planned expansion of System data.

(3) Any other recommendations made by the Center, including the most effective and efficient configuration for the System.

"**§ 116E-5. North Carolina Longitudinal Data System.**

(a) There is created the North Carolina Longitudinal Data System. The System shall be located administratively within the Department of ~~Public Instruction but shall exercise its powers and duties independently of the Department of Public Instruction and the State Board of Education.~~Information Technology.

(b) The System shall allow users to do the following:

(1) Effectively organize, manage, disaggregate, and analyze individual student and workforce data.

(2) Examine student progress and outcomes over time, including preparation for postsecondary education and the workforce.

(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,~~ public schools, 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.~~Commerce.

h. The Department of Revenue.

i. The Department of Health and Human Services.

j. The Department of Labor.

(2) Ensure routine and ongoing compliance with FERPA, IDEA, HIPAA, CJIS, the Internal Revenue Code, and other relevant privacy laws and policies, including the following:

a. The required use of de-identified data in data research and reporting.

b. The required disposition of information that is no longer needed.
c. Providing data security, including the capacity for audit trails.
d. Providing for performance of regular audits for compliance with data privacy and security standards.
e. Implementing guidelines and policies that prevent the reporting of other potentially identifying data.

(3) Facilitate information and data requests for State and federal education reporting with existing State agencies as appropriate.
(4) Facilitate approved public information requests.
(5) Develop a process for obtaining information and data requested by the General Assembly and Governor of current de-identified data and research.

(e) Use of data accessible through the System shall be regulated in the following ways:
(1) Direct access to data shall be restricted to authorized staff of the System.
(2) Only de-identified data shall be used in the analysis, research, and reporting conducted by the System.
(3) The System and recipients of data in fulfillment of approved data requests shall only use ~~aggregate~~ aggregated data in ~~the release of data in reports and in response to data requests.~~public reports.
(4) Data that may be identifiable based on the size or uniqueness of the population under consideration shall not be reported in any form by the System.
(5) The System shall not release information that may not be disclosed under FERPA, IDEA, HIPAA, CJIS, the Internal Revenue Code, and other relevant privacy laws and policies.
(6) Individual or personally identifiable data accessed through the System shall not be a public record under G.S. 132-1.

(f) The System may receive funding from the following sources:
(1) State appropriations.
(2) Grants or other assistance from ~~local school administrative units,~~ public schools, community colleges, constituent institutions of The University of North Carolina, or private colleges and universities.
(3) Federal grants.
(4) Any other grants or contributions from public or private entities received by the System.

(g) Ownership of all data collected and maintained by the System remains with the contributors to the System. Management and disclosure of data by the System does not change ownership of the data."

"**§ 116E-6. Data sharing.**

(a) ~~Local school administrative units,~~ Public schools, charter schools, community colleges, constituent institutions of The University of North Carolina, and State agencies shall do all of the following:
(1) Comply with the data requirements and implementation schedule for the System as set forth by the Center.
(2) Transfer student data and workforce data to the System in accordance with the data security and safeguarding plan developed by the Center under G.S. 116E-5.

(b) Private colleges and universities, the North Carolina Independent Colleges and Universities, Inc., and nonpublic schools may transfer student data and workforce data to the System in accordance with the data security and safeguarding plan developed under G.S. 116E-5.

(c) All data sharing supported by the System shall comply with all applicable federal and State data and data privacy laws and regulations."

PART II. CYBERSECURITY/DEPARTMENT ADMINISTRATION

SECTION 2.1.(a) Findings. – The General Assembly finds that it is in the best interest of the State for the Department of Information Technology to lead the State's cybersecurity efforts comprehensively rather than having State agencies handle cybersecurity individually in a fragmentary way.

SECTION 2.1.(b) Funding. – For the 2025-2027 fiscal biennium, of the funds available in the Information Technology Reserve, the Department of Information Technology may use up to the sum of twenty-five million dollars ($25,000,000) each fiscal year to enhance Department capabilities with respect to each of the following areas, and the funds are hereby appropriated for that purpose:

(1) Continuation of cybersecurity projects funded in S.L. 2023-134.

(2) State agency adherence to plans and policies related to cybersecurity incident, security alert, advisory response, security awareness, and agency cybersecurity training protocols.

(3) Monitoring and ensuring State agency adherence to risk assessment policy for identification and remediation of critical security vulnerabilities, including, but not limited to, significant cybersecurity incidents.

(4) Review of State agency incident response plans to ensure security standards are met with respect to cybersecurity incidents.

SECTION 2.2. For the 2025-2027 fiscal biennium, of the funds available in the Information Technology Reserve, the sum of three million eight hundred thousand dollars ($3,800,000) in each fiscal year may be used by the Department of Information Technology to support the further development and integration of the NC HealthConnex system, and the funds are hereby appropriated for that purpose. Funds shall be used to develop new technical integrations and reconnections between health care provider electronic health record systems and NC HealthConnex.

SECTION 2.3. G.S. 143B-1378 reads as rewritten:

"**§ 143B-1378. Assessment of agency compliance with cybersecurity ~~standards.~~plans and standards; reporting requirements.**

At a minimum, the State CIO shall annually assess the ability of each State agency, and each agency's contracted vendors, to comply with the current cybersecurity enterprise-wide set of standards established pursuant to this section. The assessment shall include, at a minimum, the rate of compliance with the enterprise-wide security standards and an assessment of security organization, security practices, security information standards, network security architecture, and current expenditures of State funds for information technology security. The assessment of a State agency shall also estimate the initial cost to implement the security measures needed for agencies to fully comply with the standards as well as the costs over the lifecycle of the State agency information system. Each State agency shall submit information required by the State CIO for purposes of this assessment. The State CIO shall include the information obtained from the assessment in the State Information Technology Plan. The State CIO shall consider an agency's noncompliance with cybersecurity plans and standards when reviewing agency requests under Parts 3 and 4 of this Article."

SECTION 2.4.(a) The General Assembly finds that it is in the best interests of the State for the Department of Information Technology (Department) to assess duplication in enterprise information technology spending across State agencies to identify opportunities for cost-savings and increased efficiency in information technology resource allocation. Reducing redundancy in information technology spending will enhance fiscal responsibility and improve coordination of information technology functions across State government.

SECTION 2.4.(b) During the 2025-2026 fiscal year, the Department shall select a third-party vendor to assist in a comprehensive assessment of enterprise information technology

spending across all State agencies to determine areas of duplication and inefficiency. The assessment shall include at least all of the following:

(1) Cybersecurity tools and licenses.
(2) Enterprise software licenses.
(3) Information technology staffing allocations and roles.
(4) Cloud computing services.
(5) Other information technology services and contracts deemed necessary for evaluation.

State agencies shall provide all data, reports, and assistance requested by the Department to facilitate the assessment described in this subsection. The Department may issue requests for information and proposals as needed to evaluate potential consolidation strategies, cost-saving measures, and improved information technology coordination.

SECTION 2.4.(c) On or before October 1, 2026, the Department shall submit a report to the Office of State Auditor, the Joint Legislative Oversight Committee on Information Technology, and the Fiscal Research Division detailing the following:

(1) Any findings on duplicative information technology spending.
(2) Recommendations for eliminating redundancies and optimizing information technology spending.
(3) An analysis of potential cost-savings and strategies for implementation.
(4) Any legislative or administrative actions necessary to support consolidation efforts.

SECTION 2.5. To assist in the Department's responsibility to monitor budgeting and accounting of expenditures for information technology, operations, services, projects, infrastructure, and assets for State agencies pursuant to G.S. 143B-1335, the Office of State Budget and Management and the Office of the State Controller shall establish information technology-specific fund codes within each State agency's existing budget codes no later than December 1, 2025. The State CIO shall work with the Office of State Controller and the Office of State Budget and Management to develop an implementation plan and shall submit the plan to the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division on or before September 1, 2026.

SECTION 2.6. G.S. 143B-1330 reads as rewritten:

"**§ 143B-1330. Planning and financing State information technology resources.**

(a) The State CIO shall develop policies for agency information technology planning and financing. Agencies shall prepare and submit such plans as required in this section, as follows:

…

(2) The State CIO shall develop a biennial State Information Technology Plan ~~(Plan), including, but not limited to, the use of cloud-based utility computing for use by State agencies.~~(Plan).
(3) The State CIO shall develop one or more strategic plans for information technology. The State CIO shall determine whether strategic plans are needed for any agency and shall consider an agency's operational needs, functions, and capabilities when making such determinations.

(b) Based on requirements identified during the strategic planning process, the Department shall develop and transmit to the General Assembly the biennial State Information Technology Plan in conjunction with the Governor's budget of each regular session. The Plan shall include the following elements:

…

~~(6) As part of the plan, the State CIO shall develop and periodically update a long-range State Information Technology Plan that forecasts, at a minimum, the needs of State agencies for the next 10 years.~~

(c) Each participating agency shall actively participate in preparing, testing, and implementing an information technology plan required under subsection (b) of this section. Separate agencies shall prepare biennial information technology plans, including the requirements listed in subsection (b) of this section, and transmit these plans to the Department by a date determined by the State CIO in each even-numbered year. Agencies shall provide all financial information to the State CIO necessary to determine full costs and expenditures for information technology assets and resources provided by the agencies or through contracts or grants. The Department shall consult with and assist State agencies in the preparation of these plans; shall provide appropriate personnel or other resources to the participating agencies and to separate agencies upon request. Plans shall be submitted to the Department by a date determined by the State CIO in each even-numbered year."

SECTION 2.7.(a) G.S. 115C-150.11(c), as enacted by Section 3J.1(a) of S.L. 2024-57, reads as rewritten:

"(c) Administrative Support. – The Department of Administration shall provide support to each school in matters related to finance, human resources, and procurement, ~~including~~ excluding for information technology. Each school shall enter into a memorandum of understanding with the Department of Administration with regard to this support. No civil liability shall attach to the Department of Administration, or to any of its employees, individually or collectively, for any acts or omissions of a school."

SECTION 2.7.(b) This section becomes effective July 1, 2025.

PART III. EFFECTIVE DATE

SECTION 3.1. Except as otherwise provided, this act becomes effective July 1, 2025.