GENERAL ASSEMBLY OF NORTH CAROLINA
SESSION 2023

H D

HOUSE BILL DRH40105-LR-54C

Short Title:	DIT/Omnibus Law Changes.-AB	(Public)
Sponsors:	Representative Johnson.	
Referred to:		

A BILL TO BE ENTITLED

AN ACT MAKING OMNIBUS MODIFICATIONS TO LAWS RELATING TO STATE INFORMATION TECHNOLOGY AND THE PRIVACY OF PERSONAL IDENTIFYING INFORMATION.

The General Assembly of North Carolina enacts:

COMMERCIAL MOBILE RADIO SERVICE CHANGES

SECTION 1.1.(a) G.S. 143B-1405(a)(4)b. is repealed.

SECTION 1.1.(b) Effective July 1, 2024, G.S. 143B-1405 is repealed.

SECTION 1.1.(c) Effective July 1, 2024, G.S. 143B-1403(d) reads as rewritten:

"(d) Adjustment of Charge. – The 911 Board must monitor the revenues generated by the service charges imposed by this section. If the 911 Board determines that the rates produce revenue that exceeds or is less than the amount needed, the 911 Board may adjust the rates. The 911 Board must set the service charge for prepaid wireless telecommunications service at the same rate as the monthly service charge for nonprepaid service. A change in the rate becomes effective only on July 1. The 911 Board must notify providers of a change in the rates at least 90 days before the change becomes effective. The 911 Board must notify the Department of Revenue of a change in the rate for prepaid wireless telecommunications service at least 90 days before the change becomes effective. The Department of Revenue must provide notice of a change in the rate for prepaid wireless telecommunications service at least 45 days before the change becomes effective only on the Department's Web site. The revenues ~~must:~~

~~(1) Ensure full cost recovery for communications service providers over a reasonable period of time; and~~

~~(2)~~ ~~Fund~~ shall fund allocations under G.S. 143B-1404 of this Part for monthly distributions to primary PSAPs and for the State ESInet."

SECTION 1.1.(d) Effective July 1, 2024, G.S. 143B-1407(a) reads as rewritten:

"(a) Account ~~and Fund~~ Established. – A ~~PSAP Grant and~~ Statewide 911 Projects Account is established within the 911 Fund for the purpose of ~~making grants to PSAPs in rural and other high cost areas and~~ funding projects that provide statewide benefits for 911 service. The ~~PSAP Grant and~~ Statewide 911 Projects Account consists of revenue allocated by the 911 Board under ~~G.S. 143B-1405(c) and~~ G.S. 143B-1406. The Next Generation 911 Reserve Fund is established as a special fund for the purpose of funding the implementation of the next generation 911 systems as approved by the 911 Board."

SECTION 1.1.(e) Effective July 1, 2024, G.S. 143B-1409(2) is repealed.

ESTABLISH PRIVACY OFFICE/PRIVACY AMENDMENTS

SECTION 2.1.(a) Article 15 of Chapter 143B of the General Statutes is amended by adding a new Part to read:

"Part 12. Office of Privacy and Data Protection.

"**§ 143B-1425. Office of Privacy and Data Protection established.**

(a) The Office of Privacy and Data Protection is created within the Department. The purpose of the Office is to serve as a central point of contact for State agencies on policy matters involving data privacy and data protection.

(b) The State CIO shall appoint the Chief Privacy Officer (CPO), who serves as the Director of the Office.

(c) The primary duties of the Office with respect to State agencies consist of the following:

(1) To conduct an annual privacy review.

(2) To conduct an annual privacy training for State agencies and employees.

(3) To articulate privacy principles and best practices.

(4) To coordinate data protection in cooperation with the agency.

(5) To participate with the Office of the State CIO in the review of major State agency projects involving personally identifiable information.

(d) The Office shall serve as a resource to local governments and the public on data privacy and protection concerns by:

(1) Developing and promoting the dissemination of best practices for the collection and storage of personally identifiable information, including establishing and conducting a training program or programs for local governments; and

(2) Educating consumers about the use of personally identifiable information on mobile and digital networks and measures that can help protect this information.

"**§ 143B-1426. Reporting.**

(a) By December 1, 2023, and every four years thereafter, the Office of Privacy and Data Protection shall prepare and submit to the Joint Legislative Oversight Committee on Information Technology a report evaluating its performance. The Office shall establish performance measures in its 2023 report to the legislature and, in each report thereafter, demonstrate the extent to which performance results have been achieved. These performance measures must include, but are not limited to, all of the following:

(1) The number of State agencies and employees who have participated in the annual privacy training.

(2) A report on the extent of the Office of Privacy and Data Protection's coordination with international and national experts in the fields of data privacy, data protection, and access equity.

(3) A report on the implementation of data protection measures by State agencies attributable in whole or in part to the Office of Privacy and Data Protection's coordination of efforts.

(4) A report on consumer education efforts, including, but not limited to, the number of consumers educated through public outreach efforts, as indicated by how frequently educational documents were accessed, the Office of Privacy and Data Protection's participation in outreach events, and inquiries received back from consumers via telephone or other media.

(b) By July 1, 2023, the Office shall submit to the Joint Legislative Oversight Committee on Information Technology for review and comment the performance measures developed under subsection (a) of this section and a data collection plan.

(c) By October 1, 2023, the Office shall report to the Joint Legislative Oversight Committee on Information Technology on the extent to which telecommunications providers in

the State are deploying advanced telecommunications capability and the existence of any inequality in access to advanced telecommunications infrastructure experienced by residents of rural areas, tribal lands, and economically distressed communities. This report may be submitted at a time within the discretion of the Office, at least once every four years, and only to the extent the Office is able to gather and present the information within existing resources."

SECTION 2.1.(b) G.S. 143B-1320(a) is amended by adding a new subdivision to read:

"(13a) Office. – The Office of Privacy and Data Protection in the Department of Information Technology."

SECTION 2.2. Part 7 of Article 15 of Chapter 143B of the General Statutes reads as rewritten:

"Part 7. Security of Information Technology.

"**§ 143B-1375. Security.**

Confidentiality. – No data of a confidential nature, as defined in the General Statutes or federal law, may be entered into or processed through any information technology system or network established under this Article until safeguards for the data's security and privacy satisfactory to the State CIO have been designed and installed and are fully operational. This section does not affect the provisions of G.S. 147-64.6 or G.S. 147-64.7.

"**§ 143B-1376. Statewide security and privacy standards.**

(a) The State CIO shall be responsible for the security and privacy of all State information technology systems and associated data. The State CIO shall manage all executive branch information technology security and privacy and shall establish a statewide standard for information technology security and privacy to maximize the functionality, privacy, security, and interoperability of the State's distributed information technology assets, including, but not limited to, data classification and management, communications, and encryption technologies. The State CIO shall review and revise the security and privacy standards annually. As part of this function, the State CIO shall review periodically existing security and privacy standards and practices in place among the various State agencies to determine whether those standards and practices meet statewide security, privacy, and encryption requirements. The State CIO shall ensure that State agencies are periodically testing and evaluating information security and privacy controls and techniques for effective implementation and that all agency and contracted personnel are held accountable for complying with the statewide information security ~~program.~~ and privacy programs. The State CIO may assume the direct responsibility of providing for the information technology security of any State agency that fails to adhere to security and privacy standards adopted under this Article.

(b) The State CIO shall establish standards for the management and safeguarding of all State data held by State agencies and private entities and shall develop and implement a process to monitor and ensure adherence to the established standards. The State CIO shall establish and enforce standards for the privacy and protection of State data. The State CIO shall develop and maintain an inventory of where State data is stored. For data maintained by non-State entities, the State CIO shall document the reasons for the use of the non-State entity and certify, in writing, that the use of the non-State entity is the best course of action. The State CIO shall ensure that State data held by non-State entities is properly protected and is held in facilities that meet State security standards. By October 1 each year, the State CIO shall certify in writing that data held in non-State facilities is being maintained in accordance with State information technology privacy and security standards and shall provide a copy of this certification to the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division.

(c) Before a State agency can contract for the storage, maintenance, or use of State data by a private vendor, the agency shall obtain the approval of the State CIO.

(d) With the approval of the State CIO, enterprise-level system owners may share data between their secure systems and other enterprise-level secure systems to maximize State

government's effectiveness and productivity, unless sharing the data is expressly prohibited by State or federal law. Sharing of data under this subsection shall include the transfer of PII or other potentially sensitive data only when appropriate safeguards are in place for both the transfer of the data and storage of the data in the receiving system and when consistent with ~~the~~ Statewide Information Security ~~Policy.~~ and Privacy Policies. For purposes of this subsection, the term "owner" means a State agency having both (i) possession or control of data with the ability to access, create, modify, transfer, or remove data and (ii) authority to assign access privileges to others.

"**§ 143B-1377. State CIO approval of security standards and risk assessments.**

(a) Notwithstanding G.S. 143-48.3, 143B-1320(b), or 143B-1320(c), or any other provision of law, and except as otherwise provided by this Article, all information technology security goods, software, or services purchased using State funds, or for use by a State agency or in a State facility, shall be subject to approval by the State CIO in accordance with security and privacy standards adopted under this Part.

(b) The State CIO shall conduct risk assessments to identify compliance, operational, and strategic risks to the enterprise network. These assessments may include methods such as penetration testing or similar assessment methodologies. The State CIO may contract with another party or parties to perform the assessments. Detailed reports of the risk and security issues identified shall be kept confidential as provided in G.S. 132-6.1(c).

(c) If the legislative branch or the judicial branch develop their own privacy and security standards, taking into consideration the mission and functions of that entity, that are comparable to or exceed those set by the State CIO under this section, then those entities may elect to be governed by their own respective privacy and security standards. In these instances, approval of the State CIO shall not be required before the purchase of information technology security devices and services. If requested, the State CIO shall consult with the legislative branch and the judicial branch in reviewing the privacy and security standards adopted by those entities.

(d) Before a State agency may enter into any contract with another party for an assessment of network vulnerability, the State agency shall notify the State CIO and obtain approval of the request. If the State agency enters into a contract with another party for assessment and testing, after approval of the State CIO, the State agency shall issue public reports on the general results of the reviews. The contractor shall provide the State agency with detailed reports of the security issues identified that shall not be disclosed as provided in G.S. 132-6.1(c). The State agency shall provide the State CIO with copies of the detailed reports that shall not be disclosed as provided in G.S. 132-6.1(c).

(e) Nothing in this section shall be construed to preclude the Office of the State Auditor from assessing the security practices of State information technology systems as part of its statutory duties and responsibilities.

"**§ 143B-1378. Assessment of agency compliance with cybersecurity and privacy standards.**

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 and privacy 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 and privacy standards and an assessment of security organization, security and privacy 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 and privacy 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.

"**§ 143B-1379. State agency cooperation and training; liaisons; county and municipal government reporting.**

(a) The head of each principal department and Council of State agency shall cooperate with the State CIO in the discharge of the State CIO's duties by providing the following information to the Department:

(1) The full details of the State agency's information technology and operational requirements and of all the agency's significant cybersecurity incidents within 24 hours of confirmation.

(2) Comprehensive information concerning the information technology security employed to protect the agency's data, including documentation and reporting of remedial or corrective action plans to address any deficiencies in the information security and privacy policies, procedures, and practices of the State agency.

(3) A forecast of the parameters of the agency's projected future cybersecurity and privacy needs and capabilities.

(4) Designating ~~an~~ privacy and security agency ~~liaison~~ liaisons in the information technology area to coordinate with the State CIO. ~~The~~ Each liaison shall be subject to a criminal background report from the State Repository of Criminal Histories, which shall be provided by the State Bureau of Investigation upon its receiving fingerprints from the liaison. Military personnel with a valid secret security clearance or a favorable Tier 3 security clearance investigation are exempt from this requirement. If ~~the~~ a liaison has been a resident of this State for less than five years, the background report shall include a review of criminal information from both the State and National Repositories of Criminal Histories. The criminal background report shall be provided to the State CIO and the head of the agency. In addition, all personnel in the Office of the State Auditor who are responsible for information technology security reviews shall be subject to a criminal background report from the State Repository of Criminal Histories, which shall be provided by the State Bureau of Investigation upon receiving fingerprints from the personnel designated by the State Auditor. For designated personnel who have been residents of this State for less than five years, the background report shall include a review of criminal information from both the State and National Repositories of Criminal Histories. The criminal background reports shall be provided to the State Auditor. Criminal histories provided pursuant to this subdivision are not public records under Chapter 132 of the General Statutes.

(5) Completing mandatory annual security and privacy awareness training and reporting compliance for all personnel, including contractors and other users of State information technology systems.

(b) The information provided by State agencies to the State CIO under this section is protected from public disclosure pursuant to G.S. 132-6.1(c).

(c) Local government entities, as defined in G.S. 143-800(c)(1), shall report cybersecurity and privacy incidents to the Department. Information shared as part of this process will be protected from public disclosure under G.S. 132-6.1(c). Private sector entities are encouraged to report cybersecurity and privacy incidents to the Department.

"**§ 143B-1380:** Reserved for future codification purposes."

SECTION 2.3. G.S. 143B-1320(a) is amended by adding a new subdivision to read:

"(14.1) Privacy incident. – An occurrence which raises a reasonable risk of harm, whether suspected or confirmed:

a. Where a person other than an authorized user has actual or potential access to identifying information as defined in G.S. 14-113.20(b),

personal information as defined in G.S. 75-66(c), or protected health information in usable physical or electronic form;

b. Where an authorized user has access to identifying information as defined in G.S. 14-113.20(b) or personal information as defined in G.S. 75-66(c) for an unauthorized purpose; or

c. That otherwise involves loss of control, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar compromise affecting information defined in sub-subdivisions a. and b. of this subdivision."

CODIFY AGENCY ANNUAL REPORT

SECTION 3.1. G.S. 143B-1322(c) is amended by adding a new subdivision to read:

"(23) Beginning February 1, 2024, and then annually thereafter, submit an annual report on State government information technology and governance with a focus on broadband and connectivity, cybersecurity, privacy, procurement, and digital transformation to the Joint Legislative Oversight Committee on Information Technology and the Fiscal Research Division."

NORTH CAROLINA LONGITUDINAL DATA SYSTEM MODIFICATIONS

SECTION 4.1. Chapter 116E of the General Statutes is recodified into Part 13 of Article 15 of Chapter 143B of the General Statutes, renumbered as G.S. 143B-1430 through G.S. 143B-1434, respectively, and reads as rewritten:

"Part 13. North Carolina Longitudinal Data System.

"**§ 143B-1430. 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.

(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.

(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.

(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 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.

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

"**§ 143B-1431. 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.

"**§ 143B-1432. Powers and duties of the Center.**

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

(1) Develop an implementation plan to phase in the establishment and operation of the System.

(2) Provide general oversight and direction to the System.

(3) Approve the annual budget for the System.

(4) Before the use of any individual data in the System, the Center shall do the following:

a. Create 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.

b. Develop and implement policies to comply with FERPA and any other privacy measures, 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 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.

"**§ 143B-1433. North Carolina Longitudinal Data System.**

(a) There is created the North Carolina Longitudinal Data ~~System.~~ System (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.~~within the Department.

(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, 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.
(2) Ensure routine and ongoing compliance with FERPA, 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 shall only use aggregate data in the release of data in reports and in response to data requests.~~
(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, 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, 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) The System shall facilitate the sharing of data with approved requestors at the individual record level in accordance with memoranda of understanding executed by current data contributors.

"**§ 143B-1434. Data sharing.**

(a) Local school administrative units, 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."

GOVERNMENT DATA ANALYTICS CENTER

SECTION 5.1. G.S. 93B-14 reads as rewritten:

"**§ 93B-14. Information on applicants for licensure.**

Every occupational licensing board shall require applicants for licensure to provide to the Board the applicant's social security number. This information shall be treated as confidential and may be released only as follows:
(1) To the State Child Support Enforcement Program of the Department of Health and Human Services upon its request and for the purpose of enforcing a child support order.
(2) To the Department of Revenue for the purpose of administering the State's tax laws.
(3) To the Government Data Analytics Center of the Department of Information Technology for purposes authorized under Article 15 of Chapter 143B of the General Statutes."

SECTION 5.2. G.S. 143B-1385(b)(5) reads as rewritten:

"(b) GDAC. – The Government Data Analytics Center is established as a unit of the Department.

…

(5) Project management. – The State CIO and State agencies, with the assistance of the Office of State Budget and Management, shall identify potential funding sources for expansion of existing projects or development of new projects. No GDAC project shall be initiated, extended, or ~~expanded:~~expanded without the approval of the State CIO.

~~a. Without the specific approval of the General Assembly, unless the project can be implemented within funds appropriated for GDAC projects.~~

~~b. Without prior consultation to the Joint Legislative Commission on Governmental Operations and a report to the Joint Legislative Oversight Committee on Information Technology if the project can be implemented within funds appropriated for GDAC projects.~~"

SECTION 5.3. G.S. 116E-2 reads as rewritten:

"**§ 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.~~"

GEOGRAPHIC INFORMATION/NAME CHANGE

SECTION 6.1. G.S. 143B-1421(f) reads as rewritten:

"(f) Administration. – The ~~Director of the CGIA~~ Chief Geographic Information Officer shall be secretary of the Council and provide staff support as it requires."

FIVE-YEAR STRATEGIC PLAN

SECTION 7.1. G.S. 143B-1330(b)(6) reads as rewritten:

"(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~~ five years."

CLARIFY DEFINITION OF "IDENTIFYING INFORMATION"

SECTION 8.1. G.S. 14-113.20(b) reads as rewritten:

"(b) The term "identifying information" as used in this Article includes the following:

(1) Social security or employer taxpayer identification numbers.

(2) Drivers license, State identification card, or passport numbers.
(3) Checking account numbers.
(4) Savings account numbers.
(5) Credit card numbers.
(6) Debit card numbers.
(7) Personal Identification (PIN) Code as defined in G.S. 14-113.8(6).
(8) Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names.
(9) Digital signatures.
(10) Any other numbers or information that can be used to access a person's ~~financial resources.~~resources to cause harm, including embarrassment, inconvenience, reputational harm, emotional harm, financial loss, unfairness, risk to personal safety, fiscal damage, or loss or misuse of information which adversely affects one or more individuals or undermines the integrity of a system or program.
(11) Biometric data.
(12) Fingerprints.
(13) Passwords.
(14) Parent's legal surname prior to marriage.
(15) Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."

SECTION 8.2. G.S. 75-66(c) reads as rewritten:

"(c) As used in this section, the phrase "personal information" includes a person's first name or first initial and last name in combination with any of the following information:

(1) Social security or employer taxpayer identification numbers.
(2) Drivers license, State identification card, or passport numbers.
(3) Checking account numbers.
(4) Savings account numbers.
(5) Credit card numbers.
(6) Debit card numbers.
(7) Personal Identification (PIN) Code as defined in G.S. 14-113.8(6).
(8) Digital signatures.
(9) Any other numbers or information that can be used to access a person's financial resources.
(10) Biometric data.
(11) Fingerprints.
(12) Passwords.
(13) Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."

NORTH CAROLINA HEALTH INFORMATION EXCHANGE ACT CHANGES

SECTION 9.1. G.S. 90-414.4 reads as rewritten:

"**§ 90-414.4. Required participation in HIE Network for some providers.**

…

(a1) Mandatory Connection to HIE Network. – Notwithstanding the voluntary nature of the HIE Network under G.S. 90-414.2, the following providers and entities shall be connected to the HIE Network and begin submitting data through the HIE Network pertaining to services rendered to Medicaid beneficiaries and to other State-funded health care program beneficiaries

and paid for with Medicaid or other State-funded health care funds in accordance with the following time line:

…

(4) The following entities shall begin submitting demographic and clinical data by January 1, 2023:

a. Physicians who perform procedures at ambulatory surgical centers as defined in G.S. 131E-146.

~~b. Dentists licensed under Article 2 of Chapter 90 of the General Statutes.~~

c. Licensed physicians whose primary area of practice is psychiatry.

d. The State Laboratory of Public Health operated by the Department of Health and Human Services.

…

(e) Voluntary Connection for Certain Providers. – Notwithstanding the mandatory connection and data submission requirements in subsections (a1) and (b) of this section, the following providers of Medicaid services or other State-funded health care services are not required to connect to the HIE Network or submit data but may connect to the HIE Network and submit data voluntarily:

(1) Community-based long-term services and supports providers, including personal care services, private duty nursing, home health, and hospice care providers.

(2) Intellectual and developmental disability services and supports providers, such as day supports and supported living providers.

(3) Community Alternatives Program waiver services (including CAP/DA, CAP/C, and Innovations) providers.

(4) Eye and vision services providers.

(5) Speech, language, and hearing services providers.

(6) Occupational and physical therapy providers.

(7) Durable medical equipment providers.

(8) Nonemergency medical transportation service providers.

(9) Ambulance (emergency medical transportation service) providers.

(10) Local education agencies and school-based health providers.

(11) Dentists licensed under Article 2 of this Chapter.

(12) Chiropractors licensed under Article 8 of this Chapter.

…."

SECTION 9.2. G.S. 90-414.8(a) reads as rewritten:

"(a) Creation and Membership. – There is hereby established the North Carolina Health Information Exchange Advisory Board within the Department of Information Technology. The Advisory Board shall consist of the following ~~12~~ 14 members:

(1) The following ~~four~~ five members appointed by the President Pro Tempore of the Senate:

a. A licensed physician in good standing and actively practicing in this State.

b. A patient representative.

c. An individual with technical expertise in health data analytics.

d. A representative of a behavioral health provider.

e. A provider of Medicaid or other State-funded health care services that is connected to the Health Information Exchange Network.

(2) The following ~~four~~ five members appointed by the Speaker of the House of Representatives:

a. A representative of a critical access hospital.

b. A representative of a federally qualified health center.

c. An individual with technical expertise in health information technology.
d. A representative of a health system or integrated delivery network.
e. A provider of Medicaid or other State-funded health care services that is connected to the Health Information Exchange Network.

(3) The following three ex officio, nonvoting members:
a. The State Chief Information Officer or a designee.
b. The Director of GDAC or a designee.
c. The Secretary of Health and Human Services, or a designee.

(4) The following ex officio, voting member:
a. The Executive Administrator of the State Health Plan for Teachers and State Employees, or a designee."

EFFECTIVE DATE

SECTION 10.1. Except as otherwise provided, this act is effective when it becomes law.