GENERAL ASSEMBLY OF NORTH CAROLINA
SESSION 2025

S D

SENATE BILL DRS45523-BCfa-7

Short Title:	AI Chatbots-Licensing, Safety, & Privacy.	(Public)
Sponsors:	Senator Burgin (Primary Sponsor).	
Referred to:		

A BILL TO BE ENTITLED

AN ACT REGULATING ARTIFICIAL INTELLIGENCE CHATBOT LICENSING, SAFETY, AND PRIVACY IN NORTH CAROLINA.

The General Assembly of North Carolina enacts:

PART I. CHATBOT LICENSING

SECTION 1.(a) The General Statutes are amended by adding a new Chapter to read:

"**Chapter 114B.**

"**Licensing of Chatbots.**

"**§ 114B-1. Short title.**

This Chapter shall be known and may be cited as the Chatbot Licensing Act.

"**§ 114B-2. Definitions.**

The following definitions apply in this Chapter:

(1) Chatbot. – A generative artificial intelligence system with which users can interact by or through an interface that approximates or simulates conversation through a text, audio, or visual medium.

(2) Department. – The North Carolina Department of Justice.

(3) Generative artificial intelligence system. – Any system that uses artificial intelligence, as defined in section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Public Law No. 115-232, 132 Stat. 1636 (2018), to generate or substantially modify image, video, audio, multimedia, or text content.

(4) Health information. – The term:

a. Includes user information relating to physical or mental health status, including:

1. Individual health conditions, treatment, diseases, or diagnosis.
2. Social, psychological, behavioral, and medical interventions.
3. Health-related surgeries or procedures.
4. Use or purchase of prescribed medication.
5. Bodily functions, vital signs, symptoms, or health-related measurements.
6. Diagnoses or diagnostic testing, treatment, or medication.
7. Gender-affirming care information.
8. Reproductive or sexual health information.
9. Biometric data.
10. Genetic data.

11. Precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies.
12. Data that identifies a consumer seeking health care services.
13. Any data inferred by a company or person for use in the treatment, diagnosis, or intervention regarding a mental or physical health condition.

b. Does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records.

(5) Licensee. – A person holding a license issued and in effect under this Chapter.

"**§ 114B-3. Licensing requirements for health information; review standards.**

(a) No person shall operate or distribute a chatbot that deals substantially with health information without first obtaining a health information chatbot license.

(b) An application for a health information chatbot license shall include all of the following:

(1) Detailed documentation of the chatbot's:
a. Technical architecture and operational specifications.
b. Data collection, processing, storage, and deletion practices.
c. Security measures and protocols.
d. Privacy protection mechanisms.
(2) Quality control and testing procedures.
(3) Risk assessment and mitigation strategies.
(4) Evidence of compliance with applicable federal and State regulations.
(5) Proof of insurance coverage.
(6) Required application fees.
(7) Any additional information required by the Department.

(c) The Department shall review applications for health information chatbot licenses based upon all of the following:

(1) Technical competence and reliability as compliant with industry standards.
(2) Data protection and security measures as compliant with industry standards.
(3) Compliance with applicable regulations.
(4) Risk management procedures.
(5) Professional qualification requirements, including:
a. Evidence-based standards demonstrating substantial efficacy for the supported use case of health information; and
b. Endorsement by qualified experts within the field of the supported use case.
(6) Public safety considerations.

(d) The Department shall adopt rules to carry out the purposes of this Chapter.

"**§ 114B-4. Operational requirements.**

(a) A licensee shall maintain professional liability insurance in an amount not less than the amount per occurrence required by the Department.

(b) A licensee shall do all of the following:

(1) Implement industry-standard encryption for data in transit and at rest, maintain detailed access logs, and conduct regular security audits no less than once every six months.
(2) Report any data breaches within 24 hours to the Department and within 48 hours to affected consumers, notwithstanding any provision of law to the contrary.
(3) Obtain explicit user consent for data collection and use.

(4) Provide users with access to their personal data.
(5) Provide users with the ability to delete their data upon request.

(c) A licensee must clearly disclose all of the following:
(1) The artificial nature of the chatbot.
(2) Limitations of the service.
(3) Data collection and use practices.
(4) User rights and remedies.
(5) Emergency resources when applicable.
(6) Human oversight and intervention protocols.

(d) A licensee shall do all of the following:
(1) Demonstrate effectiveness through peer-reviewed, controlled trials with appropriate validation studies done on appropriate sample sizes with real-world performance data.
(2) Demonstrate effectiveness in a comparative analysis to human expert performance.
(3) Meet minimum domain benchmarks as established by the Department.

(e) A licensee shall conduct regular inspections and perform an annual third-party audit. Results of all inspections and audits must be made available to the Department.

(f) A licensee shall implement continuous monitoring systems for safety and risk indicators and submit quarterly performance reports, including incident reports.

"**§ 114B-5. Identification requirements.**

Licensees shall ensure that all interactions between chatbots and users comply with the provisions of G.S. 170-5.

"**§ 114B-6. Enforcement; oversight; inspections.**

(a) The Department shall enforce the provisions of, and the rules adopted under, this Chapter.

(b) The Attorney General shall designate a Director, officers, and employees assigned to the oversight and enforcement of this Chapter. Upon presenting appropriate credentials and a written notice to the owner, operator, or agent in charge, those officers and employees are authorized to enter, at reasonable times, any factory, warehouse, or establishment in which chatbots licensed under this Chapter are manufactured, processed, or held, and to inspect, in a reasonable manner and within reasonable limits and in a reasonable time. In addition to physical inspections, the Department may conduct digital inspections of licensed chatbots under this Chapter, to include the following:
(1) Examination of source code, algorithms, and machine learning models.
(2) Review of data processing and storage practices.
(3) Evaluation of cybersecurity measures and protocols.
(4) Assessment of user data privacy protections.
(5) Testing of chatbot responses and behaviors in various scenarios.
(6) Audit of data collection, use, and retention practices.
(7) Inspection of software development and update processes.
(8) Review of remote access and monitoring capabilities.
(9) Evaluation of integration with other digital health technologies or platforms.

(c) As part of any inspection, whether physical or digital, the Director may require access to all records relating to the development, testing, validation, production, distribution, and performance of a chatbot licensed under this Chapter.

(d) Any information obtained during an inspection which falls within the definition of a trade secret or confidential commercial information, as defined in 21 C.F.R. § 20.61, shall be treated as confidential and shall not be disclosed under Chapter 132 of the General Statutes, except as may be necessary in proceedings under this Chapter or other applicable law.

(e) Following any inspection, the Director shall provide a detailed report of findings to the manufacturer or importer, including any identified deficiencies and required corrective actions.

(f) Every person who is a manufacturer or importer of a licensed chatbot under this Chapter shall establish and maintain such records, and make such reports to the Director, as the Director may by regulation reasonably require to assure the safety and effectiveness of such devices.

"**§ 114B-7. Prohibited acts.**

(a) It is unlawful for any person to do any of the following:

(1) Introduce or deliver for introduction into State commerce any chatbot that deals substantially with health information without complying with the licensing requirement of this Chapter.

(2) Fail to comply with any requirement of this Chapter or any rule adopted hereunder.

(3) Refuse to permit access to or copying of any record as required by this Chapter.

(4) Fail to report adverse events as required under this Chapter.

(b) The Department may, at its discretion, exempt certain prohibited acts from some or all of these prohibitions if it determines that the exemption is consistent with the protection of the public.

(c) Any person who violates any provision of G.S. 114B-5 or G.S. 114B-6 shall be subject to civil penalties in the amount of fifty thousand dollars ($50,000). The clear proceeds of fines and forfeitures provided for in this Chapter shall be remitted to the Civil Penalty and Forfeiture Fund in accordance with G.S. 115C-457.2.

"**§ 114B-8. Miscellaneous.**

If any provision of this Chapter is determined to be unenforceable or invalid by a court of competent jurisdiction, the remaining provisions of this Chapter shall not be affected."

SECTION 1.(b) There is appropriated from the General Fund to the Department of Justice the sum of fifty thousand dollars ($50,000) in nonrecurring funds for the 2026-2027 fiscal year to be used to publicize the provisions of this section.

SECTION 1.(c) Subsection (a) of this section becomes effective January 1, 2027. Subsection (b) of this section becomes effective July 1, 2026.

PART II. SAFETY AND PRIVACY

SECTION 2.(a) The General Statutes are amended by adding a new Chapter to read:

"**Chapter 170.**

"**Chatbot Safety and Privacy Act.**

"**§ 170-1. Title.**

This act shall be known and may be cited as the Chatbot Safety and Privacy Act.

"**§ 170-2. Definitions.**

The following definitions apply in this Chapter:

(1) Best interests. – Those interests affected by the entrustment of data, labor, or attention from a user to a covered platform.

(2) Chatbot. – As defined in G.S. 114B-2.

(3) Conversation. – In reference to a chatbot, a series of inputs from a human user and responses from a chatbot that often have sequential flow and the maintenance of conversation context by the chatbot.

(4) Covered platform. – Any person that provides chatbot services to users in this State, if the person (i) has annual gross revenues exceeding one hundred thousand dollars ($100,000) in the last calendar year or any of the two preceding calendar years or (ii) has more than 5,000 monthly active users in

the United States for half or more of the months during the last 12 months. The term does not include any person that provides chatbot services solely for educational or research purposes and does not monetize such services through advertising or commercial uses or any government entity providing chatbot services for official purposes.

(5) Dataset. – The structured collection of data, typically stored in electronic form, organized in a way that allows for easy retrieval, analysis, and information.

(6) De-identification. – The process of removing all pieces of data that link a specific user to a particular interaction, including the following:

a. Methods which replace identifiable information, including names, addresses, identification numbers, or any other distinctive data, with pseudonyms or unique identifiers not linked to a user's identity.

b. Methods which aggregate and generalize the data to such an extent that it becomes statistically improbable to re-identify any user from the de-identified data.

c. Methods which eliminate any context, metadata, or information that can be traced back to a specific user or interaction, including timestamps and geolocation data.

(7) Emergency situation. – A situation where a user using a chatbot indicates that they intend to either commit harm to themselves or commit harm to others.

(8) Generative artificial intelligence system. – As defined in G.S. 114B-2.

(9) Legitimate purpose. – A purpose that is lawful and in line with the stated objectives, functionalities, core services, and reasonable expectation of users on a platform.

(10) Self-destructing messages. – A type of data that is programmed to automatically and irreversibly delete and become inaccessible to both the sender and the recipient after a predetermined period.

(11) Sensitive personal information. – The term does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records. The term does include user information relating to any of the following:

a. Includes user information relating to physical or mental health status, including:

1. Individual health conditions, treatment, diseases, or diagnosis.
2. Social, psychological, behavioral, and medical interventions.
3. Health-related surgeries or procedures.
4. Use or purchase of prescribed medication.
5. Bodily functions, vital signs, symptoms, or health-related measurements.
6. Diagnoses or diagnostic testing, treatment, or medication.
7. Gender-affirming care information.
8. Reproductive or sexual health information.
9. Biometric data.
10. Genetic data.
11. Precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services.

b. Social security, drivers license, state identification card, or passport number.

c. Account login, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.
d. Contents of a user's mail, email, and text messages.
e. Financial information, including credit score, bank account balance, loan information, investment details, and income details.
f. Personal education records.
g. Genetic information of an individual's family members.
h. Information about an individual's minor children.
i. Financial transaction history.
j. Information collected from children under 13 years of age.

(12) Terms of service agreement. – An electronic agreement between a user and a covered platform that sets forth the terms, conditions, rights, and responsibilities of the respective parties in connection with the use of the platform's chatbot services.

(13) Transport encryption. – A security measure wherein data is encrypted during its transmission from one point to another. The data is typically encrypted by the sender's system or an intermediary service before being sent over a network and then decrypted by the recipient's system or an intermediary service upon arrival. While the data is protected during transit, it may be accessible in unencrypted form at the endpoints or by the service providers facilitating the transmission.

(14) Trusting party. – Any user of a covered platform who gives, either voluntary or involuntary, personal information to a covered platform, or any user who enters into any information relationship with a covered platform.

(15) User-related data. – Any data collected directly or indirectly from the user and linked or reasonably linkable to the user by the chatbot, including, but not limited to, the following:

a. Personal data. – Data that is directly linked to the user or indirectly identifiable, including by reference to an identifier such as a name, an identification number, precise geolocation, an online identifier, or one of several special characteristics, which expresses the physical, physiological, genetic, mental, commercial, cultural, or social identity of the user.
b. Usage data. – Data that is gathered about users' interactions, behaviors, preferences, and usage patterns within the platforms, including, but not limited to, user engagement and conversation content.
c. Other user data. – Any data not covered by personal data and usage data concerning a user, including data collected by third-party cookies.

"**§ 170-3. Duty of loyalty for chatbots.**

(a) A covered platform shall not process data or design chatbot systems and tools in ways that significantly conflict with trusting parties' best interests, as implicated by their interactions with chatbots.

(b) A covered platform shall, in fulfilling their duty of loyalty, abide by the following subsidiary duties:

(1) Duty of loyalty in emergency situations. – A covered platform shall implement and maintain reasonably effective systems to detect, promptly respond to, report, and mitigate emergency situations in a manner that prioritizes the safety and well-being of users over the platform's other interests.

(2) Duty of loyalty regarding emotional dependence. – A covered platform shall implement and maintain reasonably effective systems to detect and prevent emotional dependence of a user on a chatbot, prioritizing the user's psychological well-being over the platform's interest in user engagement or retention.

a. This duty only applies to any covered platform that utilizes a chatbot designed to (i) generate social connections with users, (ii) engage in extended conversation mimicking human interaction, or (iii) provide emotional support or companionship.

b. The determination required by sub-subdivision a. of this subdivision shall be based on the chatbot's intended purpose, design features, conversational capabilities, and interaction patterns with users.

(3) Duty of loyalty in chatbot identity disclosure. – A covered platform has a duty to clearly and consistently identify the chatbot as an artificial entity when that fact is not clearly apparent. The platform shall not process data or design systems in ways that deceive or mislead users about the non-human nature of the chatbot, prioritizing transparency over any potential benefits of perceived human-like interaction.

(4) Duty of loyalty in influence. – A covered platform shall not process data or design chatbot systems and tools in ways that influence trusting parties to achieve particular results that are against the best interests of trusting parties.

(5) Duty of loyalty in collection. – A covered platform shall collect and store only that information that does not conflict with a trusting party's best interests. Such information must be (i) adequate, in the sense that it is sufficient to fulfill a legitimate purpose of the platform, (ii) relevant, in the sense that the information has a relevant link to that legitimate purpose, and (iii) necessary, in the sense that it is the minimum amount of information which is needed for that legitimate purpose.

(6) Duty of loyalty in personalization. – A covered platform shall be loyal to the best interests of trusting parties when personalizing content based upon personal information or characteristics.

(7) Duty of loyalty in gatekeeping. – A covered platform shall be a loyal gatekeeper of personal information from a trusted party, including avoiding conflicts to the best interests of trusting parties when allowing government or other third-party access to trusting parties and their data.

"**§ 170-4. Contractual requirements.**

(a) The duties between a covered platform and an end-user shall be established through a terms of service agreement which is presented to the end-user in clear, conspicuous, and easily understandable language. The terms of service agreement must (i) explicitly outline the online service provider's obligations, (ii) describe the rights and protections afforded to the end-user under this relationship, and (iii) require affirmative consent from the end-user before the agreement takes effect.

(b) The covered platform must provide clear notice to end-users of any material changes to the terms of service agreement and obtain renewed consent for such changes.

(c) The terms of service agreement must be easily accessible to users at all times through the covered platform's application or the covered platform's website.

(d) A covered platform shall implement a chatbot identification disclosure process that meets the requirements outlined in G.S. 170-5.

"**§ 170-5. Chatbot identification process requirements.**

(a) The chatbot identification process shall include all of the following elements:

(1) A covered platform shall clearly inform users that the chatbot is:

a. Not human, human-like, or sentient.
b. A computer program designed to mimic human conversation based on statistical analysis of human-produced text.
c. Incapable of experiencing emotions such as love or lust.
d. Without personal preferences or feelings.

(2) The information required by subdivision (1) of this subsection shall be readily accessible, clearly presented, and concisely conveyed in less than 300 words.

(b) A user shall provide explicit and informed consent to interact with the chatbot. The consent process shall:

(1) Require an affirmative action from the user (such as clicking an "I understand" button); and

(2) Confirm the user's understanding of the chatbot's identity and limitations.

(c) A covered platform is prohibited from using deceptive design elements that manipulate or coerce users into providing consent or obscure the nature of the chatbot or the consent process.

(d) The chatbot identity communication and opt-in consent process shall be repeated at the start of each new interaction with a user.

(e) The chatbot identification and consent process required by this section shall be separate and distinct from any privacy policy agreement or other consent processes required by law or platform policy.

"**§ 170-6. Data privacy requirements.**

(a) A covered platform must do all of the following:

(1) Ensure that all user-related data disclosed collected through conversations between users and chatbots or through third-party cookies undergoes a process of de-identification prior to storage and analysis.

(2) Take reasonable care to prohibit the incorporation or inclusion of any sensitive personal information derived from a user during the use of a chatbot into an aggregate dataset used to train any chatbot or generative artificial intelligence system.

(3) Store all chatbot conversations which does not include sensitive personal information for at least 60 days.

(b) Each covered platform that meets the standard set forth in subsection (a) of this section shall utilize self-destructing messages with a predetermined destruction period of 30 days after the data has been acquired.

(c) The requirements of subsection (b) of this section shall apply to all chatbots which are employed in healthcare, financial services, the legal field, government services, mental health support, and education. In general, this applies to any domain, beyond those specifically listed, where chatbots are employed primarily for the processing or storage of sensitive personal information.

(d) All covered platforms shall utilize transport encryption for all messages between a user and a chatbot.

"**§ 170-7. Enforcement.**

(a) In any case in which the Attorney General has reason to believe that a covered platform has violated or is violating any provision of this Chapter, the State, as parens patriae, may bring a civil action on behalf of the residents of the State to (i) enjoin any practice violating this Chapter and enforce compliance with the pertinent section or sections on behalf of residents of the State, (ii) obtain damages, restitution, or other compensation, each of which shall be distributed in accordance with State law, or (iii) obtain such other relief as the court may consider to be appropriate.

(b) Any person who suffers injury in fact as a result of a violation of this Chapter may bring a civil action against the covered platform to enjoin further the violation, recover damages

in an amount equal to the greater of actual damages or one thousand dollars ($1,000) per violation, obtain reasonable attorneys' fees and litigation costs, and obtain any other relief that the court deems appropriate.

(c) An action under subsection (b) of this section may not be brought more than two years after the date on which the person first discovered or reasonably should have discovered the violation. No person shall be permitted to bring more than one action under this subsection against the same covered platform for the same alleged violation.

(d) The rights and remedies provided for in this section may not be waived by any agreement, policy, form, or condition of service.

"**§ 170-8. Miscellaneous.**

If any provision of this Chapter is determined to be unenforceable or invalid, the remaining provisions of this Chapter shall not be affected."

SECTION 2.(b) This Part becomes effective January 1, 2027.

PART III. RULEMAKING AUTHORITY

SECTION 3. No later than January 1, 2027, the Department of Justice shall adopt rules necessary to implement the provisions of Part I and Part II of this act.

PART IV. EFFECTIVE DATE

SECTION 4. Except as otherwise provided, this act is effective when it becomes law.