

GENERAL ASSEMBLY OF NORTH CAROLINA  
SESSION 2025

S

1

SENATE BILL 963

Short Title: AI Chatbots-Licensing, Safety, & Privacy. (Public)

Sponsors: Senator Burgin (Primary Sponsor).

Referred to: Rules and Operations of the Senate

May 4, 2026

1 A BILL TO BE ENTITLED  
2 AN ACT REGULATING ARTIFICIAL INTELLIGENCE CHATBOT LICENSING, SAFETY,  
3 AND PRIVACY IN NORTH CAROLINA.  
4 The General Assembly of North Carolina enacts:

6 PART I. CHATBOT LICENSING

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

8 "**Chapter 114B.**  
9 "**Licensing of Chatbots.**

10 "**§ 114B-1. Short title.**

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

12 "**§ 114B-2. Definitions.**

13 The following definitions apply in this Chapter:

- 14 (1) Chatbot. – A generative artificial intelligence system with which users can  
15 interact by or through an interface that approximates or simulates conversation  
16 through a text, audio, or visual medium.
- 17 (2) Department. – The North Carolina Department of Justice.
- 18 (3) Generative artificial intelligence system. – Any system that uses artificial  
19 intelligence, as defined in section 238(g) of the John S. McCain National  
20 Defense Authorization Act for Fiscal Year 2019, Public Law No. 115-232,  
21 132 Stat. 1636 (2018), to generate or substantially modify image, video, audio,  
22 multimedia, or text content.
- 23 (4) Health information. – The term:
- 24 a. Includes user information relating to physical or mental health status,  
25 including:
- 26 1. Individual health conditions, treatment, diseases, or diagnosis.
  - 27 2. Social, psychological, behavioral, and medical interventions.
  - 28 3. Health-related surgeries or procedures.
  - 29 4. Use or purchase of prescribed medication.
  - 30 5. Bodily functions, vital signs, symptoms, or health-related  
31 measurements.
  - 32 6. Diagnoses or diagnostic testing, treatment, or medication.
  - 33 7. Gender-affirming care information.
  - 34 8. Reproductive or sexual health information.
  - 35 9. Biometric data.
  - 36 10. Genetic data.



- 1                                    11. Precise location information that could reasonably indicate a  
2                                    consumer's attempt to acquire or receive health services or  
3                                    supplies.  
4                                    12. Data that identifies a consumer seeking health care services.  
5                                    13. Any data inferred by a company or person for use in the  
6                                    treatment, diagnosis, or intervention regarding a mental or  
7                                    physical health condition.  
8                                    b. Does not include publicly available information that is lawfully made  
9                                    available to the general public from federal, State, or local government  
10                                   records.  
11                                   (5) Licensee. – A person holding a license issued and in effect under this Chapter.  
12 **§ 114B-3. Licensing requirements for health information; review standards.**  
13                                   (a) No person shall operate or distribute a chatbot that deals substantially with health  
14 information without first obtaining a health information chatbot license.  
15                                   (b) An application for a health information chatbot license shall include all of the  
16 following:  
17                                   (1) Detailed documentation of the chatbot's:  
18                                   a. Technical architecture and operational specifications.  
19                                   b. Data collection, processing, storage, and deletion practices.  
20                                   c. Security measures and protocols.  
21                                   d. Privacy protection mechanisms.  
22                                   (2) Quality control and testing procedures.  
23                                   (3) Risk assessment and mitigation strategies.  
24                                   (4) Evidence of compliance with applicable federal and State regulations.  
25                                   (5) Proof of insurance coverage.  
26                                   (6) Required application fees.  
27                                   (7) Any additional information required by the Department.  
28                                   (c) The Department shall review applications for health information chatbot licenses  
29 based upon all of the following:  
30                                   (1) Technical competence and reliability as compliant with industry standards.  
31                                   (2) Data protection and security measures as compliant with industry standards.  
32                                   (3) Compliance with applicable regulations.  
33                                   (4) Risk management procedures.  
34                                   (5) Professional qualification requirements, including:  
35                                   a. Evidence-based standards demonstrating substantial efficacy for the  
36 supported use case of health information; and  
37                                   b. Endorsement by qualified experts within the field of the supported use  
38 case.  
39                                   (6) Public safety considerations.  
40                                   (d) The Department shall adopt rules to carry out the purposes of this Chapter.  
41 **§ 114B-4. Operational requirements.**  
42                                   (a) A licensee shall maintain professional liability insurance in an amount not less than  
43 the amount per occurrence required by the Department.  
44                                   (b) A licensee shall do all of the following:  
45                                   (1) Implement industry-standard encryption for data in transit and at rest,  
46 maintain detailed access logs, and conduct regular security audits no less than  
47 once every six months.  
48                                   (2) Report any data breaches within 24 hours to the Department and within 48  
49 hours to affected consumers, notwithstanding any provision of law to the  
50 contrary.  
51                                   (3) Obtain explicit user consent for data collection and use.

- 1           (4)    Provide users with access to their personal data.  
2           (5)    Provide users with the ability to delete their data upon request.  
3       (c)    A licensee must clearly disclose all of the following:  
4           (1)    The artificial nature of the chatbot.  
5           (2)    Limitations of the service.  
6           (3)    Data collection and use practices.  
7           (4)    User rights and remedies.  
8           (5)    Emergency resources when applicable.  
9           (6)    Human oversight and intervention protocols.  
10       (d)   A licensee shall do all of the following:  
11           (1)    Demonstrate effectiveness through peer-reviewed, controlled trials with  
12                   appropriate validation studies done on appropriate sample sizes with  
13                   real-world performance data.  
14           (2)    Demonstrate effectiveness in a comparative analysis to human expert  
15                   performance.  
16           (3)    Meet minimum domain benchmarks as established by the Department.  
17       (e)    A licensee shall conduct regular inspections and perform an annual third-party audit.  
18       Results of all inspections and audits must be made available to the Department.  
19       (f)    A licensee shall implement continuous monitoring systems for safety and risk  
20       indicators and submit quarterly performance reports, including incident reports.  
21       **§ 114B-5. Identification requirements.**  
22        Licensees shall ensure that all interactions between chatbots and users comply with the  
23       provisions of G.S. 170-5.  
24       **§ 114B-6. Enforcement; oversight; inspections.**  
25       (a)    The Department shall enforce the provisions of, and the rules adopted under, this  
26       Chapter.  
27       (b)    The Attorney General shall designate a Director, officers, and employees assigned to  
28       the oversight and enforcement of this Chapter. Upon presenting appropriate credentials and a  
29       written notice to the owner, operator, or agent in charge, those officers and employees are  
30       authorized to enter, at reasonable times, any factory, warehouse, or establishment in which  
31       chatbots licensed under this Chapter are manufactured, processed, or held, and to inspect, in a  
32       reasonable manner and within reasonable limits and in a reasonable time. In addition to physical  
33       inspections, the Department may conduct digital inspections of licensed chatbots under this  
34       Chapter, to include the following:  
35           (1)    Examination of source code, algorithms, and machine learning models.  
36           (2)    Review of data processing and storage practices.  
37           (3)    Evaluation of cybersecurity measures and protocols.  
38           (4)    Assessment of user data privacy protections.  
39           (5)    Testing of chatbot responses and behaviors in various scenarios.  
40           (6)    Audit of data collection, use, and retention practices.  
41           (7)    Inspection of software development and update processes.  
42           (8)    Review of remote access and monitoring capabilities.  
43           (9)    Evaluation of integration with other digital health technologies or platforms.  
44       (c)    As part of any inspection, whether physical or digital, the Director may require access  
45       to all records relating to the development, testing, validation, production, distribution, and  
46       performance of a chatbot licensed under this Chapter.  
47       (d)    Any information obtained during an inspection which falls within the definition of a  
48       trade secret or confidential commercial information, as defined in 21 C.F.R. § 20.61, shall be  
49       treated as confidential and shall not be disclosed under Chapter 132 of the General Statutes,  
50       except as may be necessary in proceedings under this Chapter or other applicable law.

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

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

8 **"§ 114B-7. Prohibited acts.**

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

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

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

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

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

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

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

25 **"§ 114B-8. Miscellaneous.**

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

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

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

33  
34 **PART II. SAFETY AND PRIVACY**

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

36 **"Chapter 170.**

37 **"Chatbot Safety and Privacy Act.**

38 **"§ 170-1. Title.**

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

40 **"§ 170-2. Definitions.**

41 The following definitions apply in this Chapter:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

35 1. Individual health conditions, treatment, diseases, or diagnosis.

36 2. Social, psychological, behavioral, and medical interventions.

37 3. Health-related surgeries or procedures.

38 4. Use or purchase of prescribed medication.

39 5. Bodily functions, vital signs, symptoms, or health-related  
40 measurements.

41 6. Diagnoses or diagnostic testing, treatment, or medication.

42 7. Gender-affirming care information.

43 8. Reproductive or sexual health information.

44 9. Biometric data.

45 10. Genetic data.

46 11. Precise location information that could reasonably indicate a  
47 consumer's attempt to acquire or receive health services.

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

- 1 c. Account login, financial account, debit card, or credit card number in  
2 combination with any required security or access code, password, or  
3 credentials allowing access to an account.  
4 d. Contents of a user's mail, email, and text messages.  
5 e. Financial information, including credit score, bank account balance,  
6 loan information, investment details, and income details.  
7 f. Personal education records.  
8 g. Genetic information of an individual's family members.  
9 h. Information about an individual's minor children.  
10 i. Financial transaction history.  
11 j. Information collected from children under 13 years of age.  
12 (12) Terms of service agreement. – An electronic agreement between a user and a  
13 covered platform that sets forth the terms, conditions, rights, and  
14 responsibilities of the respective parties in connection with the use of the  
15 platform's chatbot services.  
16 (13) Transport encryption. – A security measure wherein data is encrypted during  
17 its transmission from one point to another. The data is typically encrypted by  
18 the sender's system or an intermediary service before being sent over a  
19 network and then decrypted by the recipient's system or an intermediary  
20 service upon arrival. While the data is protected during transit, it may be  
21 accessible in unencrypted form at the endpoints or by the service providers  
22 facilitating the transmission.  
23 (14) Trusting party. – Any user of a covered platform who gives, either voluntary  
24 or involuntary, personal information to a covered platform, or any user who  
25 enters into any information relationship with a covered platform.  
26 (15) User-related data. – Any data collected directly or indirectly from the user and  
27 linked or reasonably linkable to the user by the chatbot, including, but not  
28 limited to, the following:  
29 a. Personal data. – Data that is directly linked to the user or indirectly  
30 identifiable, including by reference to an identifier such as a name, an  
31 identification number, precise geolocation, an online identifier, or one  
32 of several special characteristics, which expresses the physical,  
33 physiological, genetic, mental, commercial, cultural, or social identity  
34 of the user.  
35 b. Usage data. – Data that is gathered about users' interactions, behaviors,  
36 preferences, and usage patterns within the platforms, including, but not  
37 limited to, user engagement and conversation content.  
38 c. Other user data. – Any data not covered by personal data and usage  
39 data concerning a user, including data collected by third-party cookies.

40 **§ 170-3. Duty of loyalty for chatbots.**

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

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

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

- 1           (2) Duty of loyalty regarding emotional dependence. – A covered platform shall  
2 implement and maintain reasonably effective systems to detect and prevent  
3 emotional dependence of a user on a chatbot, prioritizing the user's  
4 psychological well-being over the platform's interest in user engagement or  
5 retention.  
6           a. This duty only applies to any covered platform that utilizes a chatbot  
7 designed to (i) generate social connections with users, (ii) engage in  
8 extended conversation mimicking human interaction, or (iii) provide  
9 emotional support or companionship.  
10          b. The determination required by sub-subdivision a. of this subdivision  
11 shall be based on the chatbot's intended purpose, design features,  
12 conversational capabilities, and interaction patterns with users.  
13          (3) Duty of loyalty in chatbot identity disclosure. – A covered platform has a duty  
14 to clearly and consistently identify the chatbot as an artificial entity when that  
15 fact is not clearly apparent. The platform shall not process data or design  
16 systems in ways that deceive or mislead users about the non-human nature of  
17 the chatbot, prioritizing transparency over any potential benefits of perceived  
18 human-like interaction.  
19          (4) Duty of loyalty in influence. – A covered platform shall not process data or  
20 design chatbot systems and tools in ways that influence trusting parties to  
21 achieve particular results that are against the best interests of trusting parties.  
22          (5) Duty of loyalty in collection. – A covered platform shall collect and store only  
23 that information that does not conflict with a trusting party's best interests.  
24 Such information must be (i) adequate, in the sense that it is sufficient to fulfill  
25 a legitimate purpose of the platform, (ii) relevant, in the sense that the  
26 information has a relevant link to that legitimate purpose, and (iii) necessary,  
27 in the sense that it is the minimum amount of information which is needed for  
28 that legitimate purpose.  
29          (6) Duty of loyalty in personalization. – A covered platform shall be loyal to the  
30 best interests of trusting parties when personalizing content based upon  
31 personal information or characteristics.  
32          (7) Duty of loyalty in gatekeeping. – A covered platform shall be a loyal  
33 gatekeeper of personal information from a trusted party, including avoiding  
34 conflicts to the best interests of trusting parties when allowing government or  
35 other third-party access to trusting parties and their data.

36 **§ 170-4. Contractual requirements.**

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

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

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

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

49 **§ 170-5. Chatbot identification process requirements.**

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

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

- 1                   a.     Not human, human-like, or sentient.  
2                   b.     A computer program designed to mimic human conversation based on  
3                         statistical analysis of human-produced text.  
4                   c.     Incapable of experiencing emotions such as love or lust.  
5                   d.     Without personal preferences or feelings.  
6           (2)     The information required by subdivision (1) of this subsection shall be readily  
7                         accessible, clearly presented, and concisely conveyed in less than 300 words.  
8       (b)     A user shall provide explicit and informed consent to interact with the chatbot. The  
9     consent process shall:  
10           (1)     Require an affirmative action from the user (such as clicking an "I understand"  
11                         button); and  
12           (2)     Confirm the user's understanding of the chatbot's identity and limitations.  
13       (c)     A covered platform is prohibited from using deceptive design elements that  
14     manipulate or coerce users into providing consent or obscure the nature of the chatbot or the  
15     consent process.  
16       (d)     The chatbot identity communication and opt-in consent process shall be repeated at  
17     the start of each new interaction with a user.  
18       (e)     The chatbot identification and consent process required by this section shall be  
19     separate and distinct from any privacy policy agreement or other consent processes required by  
20     law or platform policy.

21     **"§ 170-6. Data privacy requirements.**

- 22       (a)     A covered platform must do all of the following:  
23           (1)     Ensure that all user-related data disclosed collected through conversations  
24                         between users and chatbots or through third-party cookies undergoes a process  
25                         of de-identification prior to storage and analysis.  
26           (2)     Take reasonable care to prohibit the incorporation or inclusion of any sensitive  
27                         personal information derived from a user during the use of a chatbot into an  
28                         aggregate dataset used to train any chatbot or generative artificial intelligence  
29                         system.  
30           (3)     Store all chatbot conversations which does not include sensitive personal  
31                         information for at least 60 days.  
32       (b)     Each covered platform that meets the standard set forth in subsection (a) of this  
33     section shall utilize self-destructing messages with a predetermined destruction period of 30 days  
34     after the data has been acquired.  
35       (c)     The requirements of subsection (b) of this section shall apply to all chatbots which  
36     are employed in healthcare, financial services, the legal field, government services, mental health  
37     support, and education. In general, this applies to any domain, beyond those specifically listed,  
38     where chatbots are employed primarily for the processing or storage of sensitive personal  
39     information.  
40       (d)     All covered platforms shall utilize transport encryption for all messages between a  
41     user and a chatbot.

42     **"§ 170-7. Enforcement.**

- 43       (a)     In any case in which the Attorney General has reason to believe that a covered  
44     platform has violated or is violating any provision of this Chapter, the State, as parens patriae,  
45     may bring a civil action on behalf of the residents of the State to (i) enjoin any practice violating  
46     this Chapter and enforce compliance with the pertinent section or sections on behalf of residents  
47     of the State, (ii) obtain damages, restitution, or other compensation, each of which shall be  
48     distributed in accordance with State law, or (iii) obtain such other relief as the court may consider  
49     to be appropriate.  
50       (b)     Any person who suffers injury in fact as a result of a violation of this Chapter may  
51     bring a civil action against the covered platform to enjoin further the violation, recover damages

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

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

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

10 **"§ 170-8. Miscellaneous.**

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

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

14  
15 **PART III. RULEMAKING AUTHORITY**

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

18  
19 **PART IV. EFFECTIVE DATE**

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