Proposed Substitute House Bill 2157 (H-3136.1/26)

House Technology, Economic Development, and Veterans Committee

By Representative Ryu

Original Bill:

The bill establishes that developers and deployers of high-risk artificial intelligence (AI) systems are required to use reasonable care to protect consumers from algorithmic discrimination. It also establishes requirements for developers and deployers of high-risk AI systems relating to transparency and risk management.

Proposed Substitute House Bill (H-3136.1/26) compared to the Original Bill:

- Adds creed and citizenship status as protected statuses under the definition of “algorithmic discrimination” and specifies that algorithmic discrimination includes differential treatment based on "the presence of any sensory, mental, or physical disability" instead of "disability," and "honorably discharged veteran or military status" instead of "veteran status;"
- Adds a definition of “personal information” aligned with RCW 19.373.010 and changes one instance of “personal data” in the bill to “personal information;”
- Adds a definition of “predeployment impact assessment;”
- Adds a definition of “system card;”
- Modifies the exemption for financial institutions by exempting financial institutions that are subject to the Equal Credit Opportunity Act, instead of financial institutions that are subject to state or federal regulator guidance that applies to the use of high-risk AI systems;
- Modifies the exemption relating to insurers by specifying that the chapter does not apply to any insurer “regulated under Title 48 RCW” or any high-risk AI system developed “or acquired and” deployed by an insurer, instead of any high-risk AI system “developed by or for or deployed by” an insurer.

Staff: Emily Poole
Date: January 22, 2026

BILL REQUEST - CODE REVISER'S OFFICE

BILL REQ. #: H-3136.1/26

ATTY/TYPIST: CC:ajr

BRIEF DESCRIPTION: Regulating high-risk artificial intelligence system development, deployment, and use.

AN ACT Relating to regulating high-risk artificial intelligence system development, deployment, and use; adding a new chapter to Title 19 RCW; and providing an effective date.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

NEW SECTION. **Sec. 1.** The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1)(a) "Algorithmic discrimination" means the use of an artificial intelligence system that results in an unlawful differential treatment or impact that disfavors an individual or group of individuals on the basis of their color, creed, the presence of any sensory, mental, or physical disability, ethnicity, genetic information, limited proficiency in the English language, national origin, race, religion, reproductive health, sex, sexual orientation, honorably discharged veteran or military status, citizen or immigration status, actual or perceived age, or other classification protected under state or federal law.

(b) "Algorithmic discrimination" does not include:

(i) The offer, license, or use of a high-risk artificial intelligence system by a developer or deployer for the sole purpose of the developer's or deployer's self-testing to identify, mitigate,

or prevent discrimination or otherwise ensure compliance with state and federal law;

(ii) The expansion of an applicant, customer, or participant pool to increase diversity or redress historical discrimination; or

(iii) An act or omission by or on behalf of a private club or other establishment not in fact open to the public, as set forth in Title II of the civil rights act of 1964, 42 U.S.C. Sec. 2000a(e), as subsequently amended.

(2)(a) "Artificial intelligence system" means machine learning systems and related technologies that use data to train statistical models for the purpose of enabling computer systems to perform tasks normally associated with human intelligence or perception, such as computer vision, speech or natural language processing, and content generation.

(b) "Artificial intelligence system" does not include any artificial intelligence system that is used for development, prototyping, and research activities before such artificial intelligence system is made available to deployers or consumers.

(3) "Consequential decision" means any decision that has a material legal, or similarly significant, effect on the provision or denial to any consumer of:

(a) Parole, probation, a pardon, or any other release from incarceration or court supervision;

(b) Education enrollment or an education opportunity;

(c) Access to employment;

(d) A financial or lending service;

(e) Access to health care services;

(f) Housing;

(g) Insurance;

(h) Marital status; or

(i) A legal service.

(4)(a) "Consumer" means a natural person who is a resident of Washington and is acting only in an individual or household context.

(b) "Consumer" does not include a natural person acting in a commercial or employment context.

(5) "Deployer" means any person doing business in Washington that deploys or uses a high-risk artificial intelligence system to make a consequential decision in Washington.

(6) "Developer" means any person doing business in Washington that develops or intentionally and substantially modifies a high-risk

artificial intelligence system that is offered, sold, leased, given, or otherwise made available to deployers or consumers in Washington and who earns more than $100,000 in gross annual revenue.

(7)(a) "Facial recognition" means the use of a computer system that, for the purpose of attempting to determine the identity of an unknown individual, uses an algorithm to compare the facial biometric data of an unknown individual derived from a photograph, video, or image to a database of photographs or images and associated facial biometric data in order to identify potential matches to an individual.

(b) "Facial recognition" does not include facial verification technology, which involves the process of comparing an image or facial biometric data of a known individual, where such information is provided by that individual, to an image database, or to government documentation containing an image of the known individual, to identify a potential match in pursuit of the individual's identity.

(8)(a) "General-purpose artificial intelligence model" means a model used by an artificial intelligence system or other system that: (i) Displays significant generality; (ii) is capable of competently performing a wide range of distinct tasks; and (iii) can be integrated into a variety of downstream applications or systems.

(b) "General-purpose artificial intelligence model" does not include any artificial intelligence model that is used for development, prototyping, and research activities before such artificial intelligence model is made available to deployers or consumers.

(9) "Generative artificial intelligence system" means an artificial intelligence system that generates novel data or content based on a foundation model.

(10)(a) "High-risk artificial intelligence system" means any artificial intelligence system that is specifically intended to autonomously make, or be a substantial factor in making, a consequential decision. A system or service is not a "high-risk artificial intelligence system" if it is intended to: (i) Perform a narrow procedural task; (ii) improve the result of a previously completed human activity; (iii) detect any decision-making patterns or any deviations from preexisting decision-making patterns; or (iv) perform a preparatory task to an assessment relevant to a consequential decision.

(b) "High-risk artificial intelligence system" does not include any of the following technologies:

(i) Antifraud technology that does not use facial recognition technology;

(ii) Antimalware technology;

(iii) Antivirus technology;

(iv) Artificial intelligence-enabled video games;

(v) Autonomous vehicle technology;

(vi) Calculators;

(vii) Cybersecurity technology;

(viii) Databases;

(ix) Data storage;

(x) Firewall technology;

(xi) Internet domain registration;

(xii) Internet website loading;

(xiii) Networking;

(xiv) Spam and robocall filtering;

(xv) Spell-checking technology;

(xvi) Spreadsheets;

(xvii) Web caching;

(xviii) Web hosting or any similar technology; or

(xix) Technology that communicates with consumers in natural language for the purpose of providing users with information, making referrals or recommendations, and answering questions and is subject to an acceptable use policy that prohibits generating content that is discriminatory or unlawful.

(11)(a) "Intentional and substantial modification" means a deliberate change made to: (i) An artificial intelligence system that results, at the time when the change is implemented and any time thereafter, in a new material risk of algorithmic discrimination; or (ii) a general-purpose artificial intelligence model that affects compliance of the general-purpose artificial intelligence model, materially changes the purpose of the general-purpose artificial intelligence model, or results in a new reasonably foreseeable risk of algorithmic discrimination.

(b) "Intentional and substantial modification" does not include:

(i) Any customization made by deployers that:

(A) Is based on legitimate nondiscriminatory business justifications;

(B) Is within the scope and purpose of the artificial intelligence tool; and

(C) Does not result in a material change to the risks of algorithmic discrimination; or

(ii) A change made to a high-risk artificial intelligence system, or the performance of a high-risk artificial intelligence system, if:

(A) The high-risk artificial intelligence system continues to learn after such high-risk artificial intelligence system is offered, sold, leased, licensed, given, or otherwise made available to a deployer, or deployed; and

(B) Such change is made to such high-risk artificial intelligence system as a result of such learning and was predetermined by the deployer or the third party contracted by the deployer and included within the initial impact assessment of such high-risk artificial intelligence system as required by section 3 of this act.

(12) "Machine learning" means the process by which artificial intelligence is developed using data and algorithms to draw inferences therefrom to automatically adapt or improve its accuracy without explicit programming.

(13)(a) "Person" includes any individual, corporation, partnership, association, cooperative, limited liability company, trust, joint venture, or any other legal or commercial entity and any successor, representative, agent, agency, or instrumentality thereof.

(b) "Person" does not include any government or political subdivision.

(14) "Personal information" has the same meaning as defined in RCW 19.373.010.

(15) "Predeployment impact assessment" means a process that helps an organization understand the potential benefits and risks associated with deploying an artificial intelligence system. This includes systematically identifying, evaluating, and managing risks and impacts from the development, deployment, and use of an artificial intelligence system.

(16) "Principal basis" means the use of an output of a high-risk artificial intelligence system to make a decision without human review, oversight, involvement, or intervention or without meaningful consideration by a human.

(17)(a) "Substantial factor" means a factor that: (i) Uses the principal basis for making a consequential decision; (ii) is capable

of altering the outcome of a consequential decision; and (iii) is generated by an artificial intelligence system.

(b) "Substantial factor" includes any use of an artificial intelligence system to generate any content, decision, prediction, or recommendation concerning a consumer that is used as the principal basis to make a consequential decision concerning the consumer.

(18) "Synthetic content" means information, such as images, video, audio clips, and, to the extent practicable, text, that has been significantly modified or generated by algorithms, including by artificial intelligence.

(19) "System card" means a document that outlines how technology is used within an organization, focusing on aspects such as business, technology, and risk. In the context of artificial intelligence, a system card details the model's capabilities, limitations, safety measures, and ethical considerations, and it represents the evaluation of machine learning-based automated decision outcomes.

(20) "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use and is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

NEW SECTION. **Sec. 2.** (1) A developer of a high-risk artificial intelligence system shall use reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination arising from the intended and contracted uses of the high-risk artificial intelligence system. In a civil action brought against a developer pursuant to this chapter, there is a rebuttable presumption that a developer of a high-risk artificial intelligence system used reasonable care as required by this subsection (1) if the developer complied with the requirements of this section.

(2) A developer of a high-risk artificial intelligence system may not offer, sell, lease, give, or otherwise provide to a deployer or other developer a high-risk artificial intelligence system unless the developer makes available to the deployer or other developer:

(a) A statement disclosing the intended uses of such high-risk artificial intelligence system;

(b) Documentation disclosing the following:

(i) The known or reasonably known limitations of such high-risk artificial intelligence system, including any and all known or reasonably foreseeable risks of algorithmic discrimination arising from the intended uses of such high-risk artificial intelligence system;

(ii) The purpose of such high-risk artificial intelligence system and its intended outputs, benefits, and uses;

(iii) A summary describing how such high-risk artificial intelligence system was evaluated for performance and for mitigation of algorithmic discrimination before it was licensed, sold, leased, given, or otherwise made available to a deployer or other developer;

(iv) A description of the measures the developer has taken to mitigate known or reasonably foreseeable risks of algorithmic discrimination that may arise from the reasonably foreseeable deployment or use of such high-risk artificial intelligence system; and

(v) A description of how the high-risk artificial intelligence system should be used, not be used, and be monitored by an individual when such system is used to make, or is a substantial factor in making, a consequential decision; and

(c) Any additional documentation that is reasonably necessary to assist the deployer or other developer in understanding the outputs and monitoring performance of the high-risk artificial intelligence system for risks of algorithmic discrimination.

(3) A developer that offers, sells, leases, gives, or otherwise makes available to a deployer or other developer a high-risk artificial intelligence system shall make available to the deployer or other developer to the extent feasible and necessary, information and documentation to enable the deployer, other developer, or a third party contracted by the deployer to complete an impact assessment required by section 3(3) of this act. Such information and documentation must include artifacts, such as system cards or predeployment impact assessments, including relevant risk management policies and impact assessments.

(4) A developer that also serves as a deployer for a high-risk artificial intelligence system may not be required to generate the documentation required by this section unless such high-risk artificial intelligence system is provided to an unaffiliated entity acting as a deployer or as otherwise required by law.

(5) High-risk artificial intelligence systems that are in conformity with the latest version of the artificial intelligence risk management framework published by the national institute of standards and technology, standard ISO/IEC 42001 of the international organization for standardization, or another nationally or internationally recognized risk management framework for artificial intelligence systems, or parts thereof, are presumed to be in conformity with related requirements set out in this section.

(6) For a disclosure required pursuant to this section, a developer shall, no later than 90 days after the developer performs an intentional and substantial modification to a high-risk artificial intelligence system, update such disclosure as necessary to ensure that such disclosure remains accurate.

(7)(a) A developer of a high-risk generative artificial intelligence system that generates or substantially modifies synthetic content shall ensure that the outputs of such high-risk artificial intelligence system: (i) Are identifiable and detectable in a manner that is accessible by consumers using industry-standard tools or tools provided by the developer; (ii) comply with any applicable accessibility requirements, as synthetic content, to the extent reasonably feasible; and (iii) apply such identification at the time the output is generated.

(b) If such synthetic content is an audio, image, or video format that forms part of an evidently artistic, creative, satirical, fictional, or analogous work or program, the requirement for identifying outputs of high-risk artificial intelligence systems pursuant to (a) of this subsection (7) is limited to a manner that does not hinder the display or enjoyment of such work or program.

(c) The identification of outputs required by (a) of this subsection (7) do not apply to: (i) Synthetic content that consists exclusively of text, is published to inform the public on any matter of public interest, or is unlikely to mislead a reasonable person consuming such synthetic content; or (ii) the outputs of a high-risk artificial intelligence system that performs an assistive function for standard editing, does not substantially alter the input data provided by the developer, or is used to detect, prevent, investigate, or prosecute any crime as authorized by law.

(8) Where multiple developers directly contribute to the development of a high-risk artificial intelligence system, each developer is subject to the obligations and operating standards

applicable to developers pursuant to this section solely with respect to its activities contributing to the development of the high-risk artificial intelligence system.

(9) Nothing in this section may be construed to require a developer to disclose any trade secret, information that could create a security risk, or other confidential or proprietary information protected under state or federal law.

NEW SECTION. **Sec. 3.** (1) A deployer of a high-risk artificial intelligence system shall use reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination. In a civil action brought against a deployer pursuant to this chapter, there is a rebuttable presumption that a deployer of a high-risk artificial intelligence system used reasonable care as required by this subsection (1) if the deployer complied with the provisions of this section.

(2)(a) A deployer may not deploy or use a high-risk artificial intelligence system to make a consequential decision unless the deployer has designed and implemented a risk management policy and program for such high-risk artificial intelligence system. The risk management policy must specify the principles, processes, and personnel that the deployer must use in maintaining the risk management program to identify, mitigate, and document any risk of algorithmic discrimination that is a reasonably foreseeable consequence of deploying or using such high-risk artificial intelligence system to make a consequential decision.

(b) A risk management policy and program designed, implemented, and maintained pursuant to this section is presumed to be in conformity with related requirements set out in this section if the policy and program align with the guidance and standards set forth in the latest version of:

(i) The artificial intelligence risk management framework published by the national institute of standards and technology;

(ii) Standard ISO/IEC 42001 of the international organization for standardization; or

(iii) A nationally or internationally recognized risk management framework for artificial intelligence systems with requirements that are substantially equivalent to, and at least as stringent as, the guidance and standards described in (b)(i) and (ii) of this subsection (2).

(c) High-risk artificial intelligence systems that are in conformity with the latest version of the artificial intelligence risk management framework published by the national institute of standards and technology, standard ISO/IEC 42001 of the international organization for standardization, or another nationally or internationally recognized risk management framework for artificial intelligence systems, or parts thereof, are presumed to be in conformity with related requirements set out in this section.

(3)(a) Except as provided in (c) of this subsection (3), a deployer may not deploy or use a high-risk artificial intelligence system to make a consequential decision unless the deployer has completed an impact assessment for such high-risk artificial intelligence system. The deployer shall complete an impact assessment for a high-risk artificial intelligence system before the deployer initially deploys such high-risk artificial intelligence system and before a significant update to such high-risk artificial intelligence system is used to make a consequential decision.

(b) An impact assessment completed pursuant to (a) of this subsection (3) must include, at a minimum:

(i) A statement by the deployer disclosing the purpose, intended use cases, and deployment context of, and benefits afforded by, the high-risk artificial intelligence system;

(ii) A statement by the deployer disclosing whether the deployment or use of the high-risk artificial intelligence system poses any known or reasonably foreseeable risk of algorithmic discrimination and, if so, the nature of such algorithmic discrimination and the steps that have been taken, to the extent feasible, to mitigate such risk;

(iii) For each postdeployment impact assessment completed pursuant to this section, whether the intended use cases of the high-risk artificial intelligence system as updated were consistent with, or varied from, the developer's intended uses of such high-risk artificial intelligence system;

(iv) A description of the categories of data the high-risk artificial intelligence system processes as inputs and the outputs such high-risk artificial intelligence system produces;

(v) If the deployer used data to customize the high-risk artificial intelligence system, an overview of the categories of data the deployer used to customize such high-risk artificial intelligence system;

(vi) A list of any metrics used to evaluate the performance and known limitations of the high-risk artificial intelligence system;

(vii) A description of any transparency measures taken concerning the high-risk artificial intelligence system, including any measures taken to disclose to a consumer that such high-risk artificial intelligence system is in use when such high-risk artificial intelligence system is in use;

(viii) A description of any postdeployment monitoring performed and user safeguards provided concerning such high-risk artificial intelligence system, including any oversight process established by the deployer to address issues arising from deployment or use of such high-risk artificial intelligence system as such issues arise; and

(ix) An analysis of such high-risk artificial intelligence system's validity and reliability in accordance with standard industry practices.

(c)(i) A single impact assessment may address a comparable set of high-risk artificial intelligence systems deployed or used by a deployer.

(ii) If a deployer completes an impact assessment for the purpose of complying with another applicable law or regulation, such impact assessment satisfies the relevant requirements established in this section if such impact assessment is reasonably similar in scope and effect to the impact assessment that would otherwise be completed pursuant to this section.

(iii) A deployer that completes an impact assessment pursuant to this section shall maintain such impact assessment and all records concerning the impact assessment for three years. Throughout the period of time that a high-risk artificial intelligence system is deployed and for a period of at least three years following the final deployment of the high-risk artificial intelligence system, the deployer shall retain all records concerning each impact assessment conducted on the high-risk artificial intelligence system, including all raw data used to evaluate the performance and known limitations of such system.

(4) Not later than the time that a deployer uses a high-risk artificial intelligence system to interact with a consumer, the deployer shall disclose to the consumer that the consumer is interacting with an artificial intelligence system. At such time, the deployer shall also disclose to the consumer:

(a) The purpose of such high-risk artificial intelligence system;

(b) The nature of such system;

(c) The nature of the consequential decision;

(d) The contact information for the deployer; and

(e) A description of the artificial intelligence system in plain language, which must include:

(i) A description of the personal characteristics or attributes that such system will measure or assess;

(ii) The method by which the system measures or assesses such attributes or characteristics;

(iii) How such attributes or characteristics are relevant to the consequential decisions for which the system should be used;

(iv) Any human components of such system; and

(v) How any automated components of such system are used to inform such consequential decisions.

(5) A deployer that has deployed a high-risk artificial intelligence system to make a consequential decision concerning a consumer shall transmit to the consumer the consequential decision without undue delay. If such consequential decision is adverse to the consumer and based on personal information beyond information that the consumer provided directly to the deployer, the deployer shall provide to the consumer a statement disclosing the principal reason or reasons for the consequential decision, including:

(a) The degree to which and manner in which the high-risk artificial intelligence system contributed to the consequential decision;

(b) The type of data that was processed by such system in making the consequential decision; and

(c) The sources of such data.

(6) A deployer shall make readily available a clear statement summarizing how the deployer manages any reasonably foreseeable risk of algorithmic discrimination that may arise from the use or deployment of the high-risk artificial intelligence system.

(7) For a disclosure required pursuant to this section, each deployer shall, no later than 30 days after the deployer is notified by the developer that the developer has performed an intentional and substantial modification to a high-risk artificial intelligence system, update such disclosure as necessary to ensure that such disclosure remains accurate.

(8) A deployer who performs an intentional and substantial modification to a high-risk artificial intelligence system shall

comply with the documentation and disclosure requirements for developers pursuant to section 2 of this act.

(9) Nothing in this section may be construed to require a deployer to disclose any trade secret, information that could create a security risk, or other confidential or proprietary information protected under state or federal law.

NEW SECTION. **Sec. 4.** (1) Nothing in this chapter may be construed to restrict a developer's or deployer's ability to do the following:

(a) Comply with federal, state, or municipal ordinances or regulations;

(b) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;

(c) Cooperate with law enforcement agencies concerning conduct or activity that the developer or deployer reasonably and in good faith believes may violate federal, state, or local law, ordinances, or regulations;

(d) Investigate, establish, exercise, prepare for, or defend legal claims;

(e) Provide a product or service specifically requested by a consumer;

(f) Perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty;

(g) Take steps at the request of a consumer prior to entering into a contract;

(h) Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual;

(i) Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, or malicious or deceptive activities;

(j) Take actions to prevent, detect, protect against, report, or respond to the production, generation, incorporation, or synthesization of child sex abuse material, or any illegal activity, preserve the integrity or security of systems, or investigate, report, or prosecute those responsible for any such action;

(k) Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable

ethics and privacy laws and is approved, monitored, and governed by an institutional review board that determines, or similar independent oversight entities that determine, that the expected benefits of the research outweigh the risks associated with such research and whether the developer or deployer has implemented reasonable safeguards to mitigate the risks associated with such research;

(l) Assist another developer or deployer with any of the obligations imposed by this chapter; or

(m) Take any action that is in the public interest in the areas of public health, community health, or population health, but solely to the extent that such action is subject to suitable and specific measures to safeguard the public.

(2) The obligations imposed on developers or deployers by this chapter do not restrict a developer's or deployer's ability to:

(a) Conduct internal research to develop, improve, or repair products, services, or technologies;

(b) Effectuate a product recall;

(c) Identify and repair technical errors that impair existing or intended functionality; or

(d) Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the developer or deployer.

(3) Nothing in this chapter may be construed to impose any obligation on a developer or deployer to disclose trade secrets or information protected from disclosure by state or federal law.

(4) The obligations imposed on developers or deployers by this chapter do not apply where compliance by the developer or deployer with such obligations would violate an evidentiary privilege under federal law or the laws of Washington.

(5) Nothing in this chapter may be construed to impose any obligation on a developer or deployer that adversely affects the legally protected rights or freedoms of any person, including the rights of any person to freedom of speech or freedom of the press guaranteed in the First Amendment to the Constitution of the United States.

(6) The obligations imposed on developers or deployers by this chapter do not apply to any artificial intelligence system that is acquired by or for the federal government or any federal agency or department, including the United States department of commerce, the United States department of defense, and the national aeronautics and

space administration, unless such artificial intelligence system is a high-risk artificial intelligence system that is used to make, or is a substantial factor in making, a decision concerning employment or housing.

(7) The obligations imposed on developers or deployers by this chapter are satisfied with respect to a financial institution, if such financial institution is subject to the equal credit opportunity act, 15 U.S.C. Sec. 1691 et seq., and its implementing regulations.

(8)(a) The provisions of this chapter do not apply to any insurer regulated under Title 48 RCW, or any high-risk artificial intelligence system developed or acquired and deployed by an insurer for use in the business of insurance, if such insurer is regulated and supervised by the office of the insurance commissioner or a comparable federal regulating body and subject to examination by such entity under any existing statutes, rules, or regulations pertaining to unfair trade practices and unfair discrimination, or published guidance or regulations that apply to the use of high-risk artificial intelligence systems and such guidance or regulations aid in the prevention and mitigation of algorithmic discrimination caused by the use of a high-risk artificial intelligence system or any risk of algorithmic discrimination that is reasonably foreseeable as a result of the use of a high-risk artificial intelligence system.

(b) Nothing in this chapter may be construed to delegate existing regulatory oversight of the business of insurance to any department or agency other than the office of the insurance commissioner.

(9) The provisions of this chapter do not apply to the development of an artificial intelligence system that is used exclusively for research, training, testing, or other predeployment activities performed by active participants of any sandbox software or sandbox environment established and subject to oversight by a designated agency or other government entity and that is in compliance with the provisions of this chapter.

(10) The provisions of this chapter do not apply to a developer or deployer, or other person who develops, deploys, puts into service, or intentionally modifies, as applicable, a high-risk artificial intelligence system that:

(a) Has been approved, authorized, certified, cleared, developed, or granted by a federal agency acting within the scope of the federal agency's authority, or by a regulated entity subject to the supervision and regulation of the federal housing finance agency; or

(b) Is in compliance with standards established by a federal agency or by a regulated entity subject to the supervision and regulation of the federal housing finance agency, if the standards are substantially equivalent or more stringent than the requirements of this chapter.

(11) The provisions of this chapter do not apply to a developer or deployer, or other person that facilitates or engages in the provision of telemedicine, as defined in RCW 70.41.020, or is a covered entity within the meaning of the federal health insurance portability and accountability act of 1996 (42 U.S.C. Sec. 1320d et seq.) and the regulations promulgated under such federal act, as both may be amended from time to time, if such developer, deployer, or person is providing:

(a) Health care recommendations that are generated by an artificial intelligence system and require a health care provider subject to RCW 18.130.040 to take action to implement the recommendations; or

(b) Services utilizing an artificial intelligence system for an administrative, quality measurement, security, or internal cost or performance improvement function.

(12) If a developer or deployer engages in any action authorized by an exemption set forth in this section, the developer or deployer bears the burden of demonstrating that such action qualifies for such exemption.

(13) If a developer or deployer withholds information pursuant to an exemption set forth in this chapter for which disclosure would otherwise be required by this chapter, including the exemption from disclosure of trade secrets, the developer or deployer shall notify the subject of disclosure and provide a basis for withholding the information. If a developer or deployer redacts any information pursuant to an exemption from disclosure, the developer or deployer shall notify the subject of disclosure that the developer or deployer is redacting such information and provide the basis for such decision to redact.

(14) For purposes of this section:

(a) "Financial institution" means a bank, out-of-state bank, credit union, out-of-state credit union, federal credit union, mortgage lender, or savings institution organized under state or federal law, or any subsidiary, affiliate, or service provider of a financial institution.

(b) "Insurer" has the same meaning as defined in RCW 48.01.050.

NEW SECTION. **Sec. 5.** (1) In addition to any other remedy provided by law, a person may file a civil action against a developer or deployer for a violation of this chapter. If a court finds that the developer or deployer violated this chapter, the court may enjoin the violation and award reasonable attorneys' fees and costs.

(2) In an action brought pursuant to this section, it is an affirmative defense that the developer or deployer:

(a) Discovered a violation of any provision of this chapter;

(b) Cured such violation no later than 45 days after discovering the violation;

(c) Provided notice to the person bringing the civil action pursuant to this section that such violation has been cured and provides accompanying evidence that the violation has been cured; and

(d) Is otherwise in compliance with the requirements of this chapter.

NEW SECTION. **Sec. 6.** This chapter is declared to be remedial, with the purposes of protecting consumers and ensuring consumers receive information about consequential decisions affecting them. The provisions of this chapter granting rights or protections to consumers are construed broadly and exemptions construed narrowly.

NEW SECTION. **Sec. 7.** If any provision of this act or its application to any person or circumstance is held invalid, the remainder of the act or the application of the provision to other persons or circumstances is not affected.

NEW SECTION. **Sec. 8.** Sections 1 through 6 and 9 of this act constitute a new chapter in Title 19 RCW.

NEW SECTION. **Sec. 9.** This act takes effect January 1, 2027.

--- END ---