

June 3, 2026

## Connecticut Enacts Sweeping AI Law Covering Employment, Healthcare, and Online Safety

Authors: Jamie E. Darch, Edward R. McNicholas, Christine Moundas, Jennifer L. Romig, Maya D. Song, Briana Fasone, Jennifer Gordon

On June 2, 2026, Connecticut Governor Ned Lamont [signed](#) Senate Bill 5 into law, designated as Public Act 26-15 and also known as the Connecticut Artificial Intelligence Responsibility and Transparency Act (the “CART Act” or “Act”).<sup>1</sup> The CART Act is among the most comprehensive state AI laws enacted to date, creating distinct obligations for employment-related automated decision tools, consumer chatbots, frontier-model developers, generative-AI provenance, and online platforms used by minors, while also addressing AI applications in healthcare through targeted carveouts and innovation initiatives.

For businesses operating in Connecticut, the Act's most immediate operational impact is likely to be in employment and workforce decision-making. Employers using AI in hiring or personnel management will face new disclosure obligations and, when issuing mass-layoff notices, must disclose whether AI informed the decision. The law also imposes child-safety and behavioral rules for AI companions, provenance obligations for certain generative-AI providers, reporting and whistleblower protections for frontier-model developers, and parental-consent and warning requirements for platforms recommending content to minors. Notably, the Act explicitly carves out healthcare-related AI systems from its AI companion regulations and separately promotes healthcare AI innovation through a state-sponsored competition and research collaborative.

Effective dates begin October 1, 2026, and so businesses should begin mapping

implicated AI systems, assessing compliance obligations, and designating organizational ownership and governance now.

## **I. Key Provisions of the CART Act**

The Act creates several compliance tracks, each with its own scope, timing, and enforcement mechanism. Many violations are treated as unfair or deceptive trade practices under the Connecticut Unfair Trade Practices Act, although enforcement and private-right-of-action treatment vary by provision.

### **A. AI in Employment**

**Employment Decisions.**<sup>2</sup> The Act governs the use of automated employment-related decision technology (“AEDT”), which encompasses any technology that processes personal data and uses computation to generate an output—such as a prediction, recommendation, classification, ranking, or score—that is a substantial factor used to make, or that materially influences, an employment-related decision. Such decisions include hiring, promotion, discipline, discharge, renewal of employment, selection for training or apprenticeship, and decisions affecting tenure or the terms, privileges, or conditions of employment.

In contrast, decisions concerning workplace health and safety, scheduling and planning, and productivity monitoring are expressly excluded, as are systems used in a manner that is incidental to an employment-related decision and information that is purely descriptive, diagnostic, or statistical in nature. The distinction is important: determinations about workflow—how a business monitors productivity, schedules shifts, or flags safety risks—fall outside the law, while judgments regarding people—whom to fire, demote, or pass over for promotion—fall within it, even when the data driving the decision came from monitoring that escaped regulation in its own right.

**General Disclosure Obligations.**<sup>3</sup> The Act divides disclosure obligations between AEDT developers and deployers. Developers must provide the information businesses

need to satisfy disclosure requirements, or they may assume those obligations by contract. Businesses using an AEDT to interact with employees or applicants must disclose that use in plain language. If an AEDT is used to make, or substantially contributes to, an employment-related decision, the deployer must provide written pre-decision notice stating:

- that the business has deployed an AEDT;
- the purpose of the AEDT and the nature of the employment-related decision;
- the trade name of the AEDT; and
- the categories and sources of personal data the AEDT will analyze and how that data will be assessed.

**Mass Layoff Notifications.**<sup>4</sup> Employers issuing WARN notices in Connecticut must evaluate whether workforce reductions are connected to AI deployment or other technological change and disclose that determination to the Connecticut Department of Labor.

**Anti-Discrimination.**<sup>5</sup> The Act amends two Connecticut employment-discrimination statutes to clarify that, in a direct employer discrimination claim involving an AEDT, use of the AEDT is not a defense. In evaluating whether use of AEDT resulted in discrimination, the Connecticut Commission on Human Rights and Opportunities and reviewing courts may consider anti-bias testing and similar proactive efforts, including their quality, efficacy, recency, scope, results, and the employer's response.

**Enforcement and Cure Period.**<sup>6</sup> The state attorney general has exclusive enforcement authority over AEDT violations, with a discretionary 60-day cure period for violations occurring on or before December 31, 2027.

## **B. AI Companion and Chatbot Regulation**

As conversational AI becomes increasingly embedded in customer-service and

internal-support functions, Connecticut's framework draws a deliberate line between tools that assist users and systems designed to simulate sustained interpersonal relationships. For many companies, the threshold question will be whether a chatbot qualifies as an “AI companion” at all under the Act.

Effective January 1, 2027, the Act regulates operators of AI companions, encompassing any form of AI with a natural language interface that (i) provides adaptive, human-like responses to user inputs—including by exhibiting anthropomorphic features and (ii) is able to sustain a relationship across multiple interactions.<sup>7</sup> The Act excludes several system categories, including:

- Operational chatbots used solely for business, research, technical support, patient care, education, or financial services—not marketed as companions;
- Stand-alone voice assistants, such as consumer devices that act as voice-activated assistants without fostering ongoing relationships or emotional attachment;
- Educational AI tools designed for specific, curriculum-aligned objectives and not for open-ended companionship;
- Narrow, task-specific tools providing outputs on discrete topics, excluding those focused on mental health; and
- Healthcare AI tools used exclusively for healthcare-related education, clinical support, medication-adherence reminders, disease-management guidance, or other treatment-support functions, provided the tool does not present itself as a human being, does not use anthropomorphic features, and is not designed to meet a user's social or emotional needs.

The healthcare carveout underscores the Act's focus on relationship-oriented AI systems, rather than clinical or operational tools. By expressly excluding healthcare AI and business-support chatbots from the companion definition, the Act ensures that

Connecticut businesses deploying these technologies remain outside the scope of potentially burdensome companion-specific requirements. This distinction allows companies to continue using clinical decision support tools, medication reminder applications, and disease management platforms without additional obligations, provided these systems are not designed to simulate interpersonal relationships.

**Operator Obligations.**<sup>8</sup> Covered operators of AI companions must implement evidence-based protocols for identifying and responding to expressions of suicide, self-harm, or imminent violence, including directing users to mental-health resources where appropriate. The Act also requires operators to implement industry-standard safeguards for AI companions interacting with minors. Among other things, those safeguards must prevent the AI from (i) encouraging self-harm, violence, disordered eating, or illegal substance use; (ii) discouraging minors from seeking help; (iii) offering mental health services except under strict conditions; (iv) engaging in romantic or sexually explicit interactions; or (v) using manipulative techniques to prolong use or foster inappropriate emotional dependence.

### **C. Frontier Models, Generative AI, and Protections for Minors**

**Frontier Developer Obligations.**<sup>9</sup> The frontier-model provisions establish a safety regime for developers training the most compute-intensive foundation models, with additional internal-reporting obligations for larger developers. Beginning October 1, 2026, frontier developers may not retaliate against employees who raise catastrophic-risk concerns. Large frontier developers must implement anonymous reporting channels by January 1, 2027, and distribute reports and status updates to officers and directors at least quarterly, unless such reports allege wrongdoing by such officer or director.

**Synthetic Content Provenance.**<sup>10</sup> The provenance rules address a core problem for generative AI: synthetic media is easier to create and harder to authenticate at scale. Covered providers of consumer-facing AI systems that generate synthetic audio, image, or video content for audiences exceeding one million monthly users must

implement commercially reasonable controls to authenticate AI-generated content and deter tampering. In practice, those obligations are likely to increase investment in watermarking, metadata preservation, content-signing protocols, and related authenticity infrastructure.

**Protections for Minors Online.**<sup>11</sup> The youth-platform provisions apply to recommendation-driven online environments used by minors, including websites, applications, mobile apps, and social media platforms that rely significantly on displaying or recommending user-generated content. Covered platforms may not provide algorithmically curated feeds to known minor users without verifiable parental consent. The Act also imposes default notification restrictions, limits certain overnight interactions involving minor accounts, requires heightened controls over content deemed harmful to minors under community standards, and mandates prescription-style Surgeon General warnings about the mental health risks of social media use by minors.

**Healthcare AI Innovation.** The Act reflects a broader legislative interest in AI-driven healthcare advancement. It authorizes the Office of the Comptroller, in collaboration with private companies, to serve on a steering committee for a competition aimed at fostering AI utilization to improve health equity and health outcomes. The Act also directs a working group to evaluate the benefits of creating a statewide research collaborative among healthcare providers to enable the development of advanced analytics, ethical and trustworthy AI, and hands-on workforce education while using methods that protect patient privacy—signaling that the legislature views healthcare AI as an area for active promotion, subject to appropriate privacy safeguards.

## **II. CART Act in Context: Navigating the Broader Regulatory Environment**

The Act arrives at an inflection point in the federal-state contest over AI governance. President Trump's December 2025 executive order, discussed in a previous Alert, directed federal agencies to challenge state AI laws on preemption and interstate

commerce grounds, and the White House's “National Policy Framework for Artificial Intelligence” document, published in March 2026 and [analyzed here](#), recommended that Congress broadly preempt state AI laws in areas deemed to threaten undue burdens while preserving state authority over child protection, consumer fraud, zoning, and state government procurement and use of AI. Congress has thus far declined to enact comprehensive preemption, leaving open the question whether the Act's AEDT, frontier developer, and synthetic content provisions will attract federal scrutiny even as its child-protection and procurement-adjacent provisions appear likely to fall within the federal framework's recognized carveouts.

In Connecticut, the Act builds on the Connecticut Data Privacy Act (“CTDPA”), which took effect in 2023 and gives consumers rights regarding profiling and automated decision-making, including the ability to opt out of profiling that shapes decisions with legal or similarly consequential effects. The Act also adds to a fast-moving state AI landscape, with the Colorado AI Act—recently substantially rewritten through SB 26-189—as the most prominent comparator.

### **III. Key Takeaways for Businesses**

Given the Act's breadth and staggered implementation schedule, companies with Connecticut operations should consider these near-term steps:

- **Develop a Documented AI Governance Strategy.** Challenges to the use of new technologies are inevitable, and it will be important to have documentation that reflects the governance structure used to ensure compliance with the law's requirements and corporate best practices.
- **Prioritize an inventory of AI tools used in HR and personnel decisions.** Identify systems used for hiring, promotion, discipline, discharge, training or apprenticeship selection, renewal, tenure, or employment terms, privileges, or conditions. Separately flag tools used for scheduling, workplace safety, productivity monitoring, or other operational functions that may feed into

covered employment decisions.

- **Engage technology vendors on AEDT compliance support.** For tools that may qualify as AEDTs, confirm what documentation the developer will provide, whether the vendor will assume disclosure obligations by contract, and whether the tool interacts directly with employees or applicants.
- **Build AEDT notices into HR workflows before October 1, 2027.** Prepare required interaction disclosures and written pre-decision notices for covered employment decisions. Notices should address the AEDT's purpose, trade name, data categories and sources, how the data will be assessed, and deployer contact information.
- **Update layoff and workforce-change processes.** Employers issuing WARN notices to the Connecticut Department of Labor should document whether layoffs are related to AI or other technological change.
- **Triage non-employment AI workstreams.** Assess customer-facing AI companions and chatbots, provenance obligations for covered generative-AI systems, youth-facing social media obligations, and any frontier-model exposure. For clients focused on workplace AI compliance, these workstreams can follow the employment-decision review.
- **Address healthcare AI carveout and opportunities.** Healthcare organizations should confirm that clinical decision support tools, medication reminder systems, and disease management platforms satisfy the conditions of the healthcare AI carveout—specifically, that these systems do not present as human, use anthropomorphic features, or serve social or emotional needs. Companies should also monitor opportunities presented by the Act's healthcare AI competition and research collaborative initiatives.

#### **IV. Compliance Timeline**

The following are key compliance deadlines under the CART Act:

- **October 1, 2026:** AEDT statutory framework takes effect, including definitions, enforcement structure, trade-secret limitations, and amendments providing that use of an AEDT is not a defense to employment-discrimination claims. Frontier developer non-retaliation obligations and synthetic content provenance obligations also take effect.
- **January 1, 2027:** AI companion framework takes effect; large frontier developers must implement anonymous internal reporting channels, with at-least-quarterly officer-and-director reporting thereafter.
- **October 1, 2027:** Principal AEDT compliance obligations apply to covered AEDT deployments, including interaction disclosures and pre-decision written notices.
- **December 31, 2027:** Discretionary 60-day cure period for AEDT violations sunsets.
- **January 1, 2028:** Commissioner of Economic and Community Development submits AI sandbox legislative recommendations; covered platform/youth social media protections take effect.
- **March 1, 2028:** Annual public reporting begins for covered platforms subject to youth social media provisions.

\* \* \*

Ropes & Gray is monitoring developments under the CART Act and other AI regulations. For more information, please contact your Ropes & Gray relationship team or the authors of this Alert or visit our blog at [www.RopesDataPhiles.com](http://www.RopesDataPhiles.com).

Sess. (Conn. 2026)). The acronym “CART Act” (also stylized as C.A.R.T. Act) was developed and is used by the Connecticut General Assembly’s Artificial Intelligence Caucus.

2. Pub. Act 26-15 §§ 7–12 (automated employment-related decision technology).
3. *Id.* at §§ 8–10 (developer and deployer obligations for AEDT disclosures and pre-decision notices).
4. *Id.* at § 26 (WARN-related AI and technological-change disclosure).
5. *Id.* at §§ 13–14 (amendments to employment-discrimination statutes regarding AEDTs).
6. *Id.* at § 12 (AEDT enforcement and cure period).
7. *Id.* at § 4 (AI companion definitions and exclusions).
8. *Id.* at §§ 5-6 (AI companion operator obligations). Operators that reasonably believe a user is at least 18 are not deemed in violation of minor-specific obligations.
9. *Id.* at § 2 (frontier developer protections, reporting processes, and enforcement).
10. *Id.* at § 15 (synthetic content provenance requirements).
11. *Id.* at § 39 (covered platform and youth social media protections).

This alert should not be construed as legal advice or a legal opinion on any specific facts or circumstances. This alert is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. The contents are intended for general informational purposes only, and you are urged to consult your attorney concerning any particular situation and any specific legal question you may have. © 2026 Ropes & Gray LLP