

Colorado repeals and replaces landmark AI Act, publishes draft rules for public comment

August 13, 2026 | Client Update | 8-minute read

Colorado replaces its landmark AI Act with a narrower regulatory framework focused on transparency and disclosure, and publishes draft rules for public comment.

Background

Colorado overhauled its regulatory framework for artificial intelligence weeks before the [Colorado AI Act](#) (CAIA) was scheduled to take effect. When passed in May 2024, the CAIA became the nation's first comprehensive state AI law. Among other things, the CAIA imposed a duty of reasonable care on both developers and deployers of certain “high-risk” AI systems and promptly drew scrutiny from the AI industry and ultimately the White House for the breadth of its compliance obligations. In August 2025, a month after the White House released [America's AI Action Plan](#) (see prior DPW coverage of [Pillar 1](#); [Pillar 2](#); and [Pillar 3](#)), Colorado delayed the CAIA's effective date from February 1, 2026 to June 30, 2026. Governor Jared Polis subsequently convened the Colorado AI Policy Work Group comprised of industry experts, business representatives and consumer advocates to consider amendments or replacements to the CAIA and, in March 2026, the Work Group proposed a new legal framework to replace the CAIA. In April 2026, the Department of Justice's AI Litigation Task Force, which was created to challenge state laws deemed harmful to AI innovation, joined xAI's pending lawsuit challenging the CAIA in April 2026. On May 14, 2026, Governor Polis signed the [Automated Decision-Making Technology Act](#) (ADMTA or the Act), which repeals and replaces the CAIA.

The ADMTA establishes a decidedly narrower regulatory framework. It omits many of the most controversial elements of the CAIA, including mandatory risk-management programs, impact assessments, detailed consumer disclosures and the duty of reasonable care. It focuses instead on increased transparency and disclosure about adverse outcomes influenced by automated decision-making technology (ADMT), as discussed below. The ADMTA takes effect January 1, 2027, provided the Colorado Attorney General completes the requisite rulemaking process by that date. On August 11, 2026, the Colorado Attorney General's Office invited [public comment](#) on draft rules for the ADMTA as well as Colorado's Chatbot Safety Act, which Governor Polis signed into law on May 29, 2026.

Applicability

The ADMTA applies to both developers and deployers of certain covered ADMT doing business in Colorado. “Developers” develop, offer, sell, lease, license or otherwise make a covered ADMT commercially available, or intentionally and substantially modify an ADMT such that it becomes a covered ADMT. This extends to parties that develop components intended, designed, advertised or contracted to be used as part of a covered ADMT. A “Deployer” is simply anyone that deploys a covered ADMT.

The Act's scope is demarcated by a series of interlocking definitions, the most consequential of which include:

- “**ADMT**” refers to technology that processes personal data and uses computation to generate output, such as predictions, scores, classifications or other information used to guide decisions.
 - The Act expressly excludes a variety of commonplace technologies from this definition, such as databases, anti-malware and spam-filtering technology, and tools used to organize or present information for human review or administrative processing. It also excludes chatbots that communicate with consumers in natural language to make recommendations, answer questions or generate content, so long as they are not presented or intended to be used in consequential decisions, as defined below, and are subject to an acceptable use policy that prohibits generated content from being used in a consequential decision.
- “**Covered ADMT**” refers to ADMT that is used to materially influence a consequential decision – i.e., the ADMT output is a non-de minimis factor used in making the consequential decision, and that actually affects the outcome, including by constraining, ranking, scoring, recommending, classifying or otherwise meaningfully altering the decision-making process.
- A “**consequential decision**” is a decision, determination or action made about a consumer that “relates to” (1) a consumer’s access to, eligibility for, selection or compensation for a “covered domain” or (2) a differentiated price, cost sharing, compensation or other material term in a manner that is reasonably likely to materially limit, delay or otherwise fundamentally alter the consumer’s access to or eligibility for a covered domain.
 - This definition expressly excludes: (1) low-stakes or routine decisions, actions and business processes; (2) advertising, marketing, search and content moderation; (3) spreadsheets that require manual human analysis and do not use machine learning, foundation models or large language models; (4) tools used to summarize or organize information for human review; (5) narrow procedural tasks or data-processing functions that do not make predictions or inferences about consumers; (6) cybersecurity, spam-filtering and anti-money laundering/counterterrorism financing controls; (7) technologies used for economic sanctions compliance; (8) fraud prevention technologies; and (9) routine academic administration and student support.
- Finally, the “**covered domains**” to which the Act applies include education, employment, residential real estate, financial and lending services, insurance, health-care services, and essential government services.

While the domains covered by the ADMTA and the CAIA are largely the same, scope changes cut in both directions. Despite notable new exemptions from the definition of consequential decisions, the threshold for relevance to a consequential decision is now lower, in that a covered technology need only “relate to” a consumer’s rights, rather than have a material legal or similarly significant effect on them.

Requirements

The ADMTA imposes different requirements on developers and deployers of a Covered ADMT.

Developer obligations

The Act’s developer obligations are decidedly narrower than the duty of reasonable care imposed by the CAIA to protect consumers from known or reasonably foreseeable risks of algorithmic discrimination and the prerequisites to creating a rebuttable presumption of reasonable care. When a developer creates a Covered ADMT that is intended, documented, marketed, advertised, configured or contracted to be used to make consequential decisions, or when a developer is aware that its Covered ADMT is being used to make consequential decisions consistent with its intended use, the ADMTA requires that the developer provide to each deployer of a Covered ADMT:

- A general statement describing the intended uses and known harmful or inappropriate uses of the Covered ADMT;
- A description of the categories of data, including personal data, used to train the Covered ADMT;
- Known limitations of the Covered ADMT, including known risks and circumstances in which the Covered ADMT should not be used;
- Instructions for appropriate use, monitoring and meaningful human review; and
- Information necessary for the deployer to comply with its obligations under the law.

The developer must also disclose to the deployer any material updates, modifications or changes. To provide these disclosures, a developer may use a public release, so long as each deployer is directly notified of this release. In addition to these disclosures, developers are also now required to retain records of compliance with the ADMTA for a

minimum of three years, including records of system versions, changelogs and documentation regarding material updates.

Deployer obligations

First, before a deployer uses a Covered ADMT in a consequential decision, the deployer must provide a “clear and conspicuous” notice to the consumer affected by that decision, explaining that the Covered ADMT is being used and providing instructions for how the consumer may obtain additional information. A prominent public notice can satisfy this requirement, so long as it is accessible at points of consumer interaction, with a link or posting close to the interaction site. This requirement is a narrowing of the disclosure obligations in the original Colorado AI Act, which required deployers to disclose to all consumers when they are interacting with any artificial intelligence system, unless it would be obvious to a reasonable person.

Second, if the use of Covered ADMT in a consequential decision results in an adverse outcome for a consumer, the deployer must provide notice to the consumer within 30 days, containing: (1) a plain language description of the consequential decision and the role the Covered ADMT played in it; (2) instructions for requesting additional information about the Covered ADMT and its inputs; and (3) an explanation of the consumer’s rights and how to exercise them. The original CAIA, by contrast, required that this post-adverse outcome notice include a statement of the principal reasons for the decision, the degree of involvement of AI, and the type and source of data used in the decision.

Third, similar to developers, deployers are required to maintain records demonstrating their compliance with the Act for at least three years.

Consumer rights

If a consumer experiences an adverse outcome resulting from the use of a Covered ADMT in a consequential decision, the consumer may request – and the deployer must provide – (1) instructions for requesting personal data and correcting inaccurate information used in the consequential decision and (2) an opportunity for meaningful human review and reconsideration, to the extent commercially reasonable.

Enforcement

The Colorado Attorney General has sole enforcement authority over the ADMTA via the Colorado Consumer Protection Act, and no private right of action is available. If a cure is deemed possible, the Attorney General must issue a notice of violation, which triggers a 60-day cure period. If a violation is discovered in the course of an enforcement action, the ADMTA permits a court to consider cure within 60 days as a mitigating factor in determining any penalties. There is, however, no right to cure knowing or repeated violations. Beginning in January 2028, and every January thereafter, the Attorney General must issue a report concerning enforcement actions brought, and cure periods offered, under the ADMTA. The right to cure sunsets on January 1, 2030.

Liability

Under the ADMTA, developers and deployers may be held liable in an action alleging unlawful discrimination under state anti-discrimination laws, arising from a consequential decision materially influenced by a Covered ADMT. Liability, however, is not joint and several; it is apportioned between the developers and deployers based on relative fault. Developers are considered responsible for harms arising from their ADMT when it is used as intended, marketed or configured. Deployers, on the other hand, are responsible for their independent actions or omissions, including using the ADMT in an unintended manner. To preserve this liability structure, the Act specifies that indemnification provisions shifting liability away from a developer or deployer will be held void as against public policy.

Rulemaking

The Colorado General Assembly left open certain areas for rulemaking by the Attorney General. For instance, the Attorney General must adopt rules to clarify and implement the post-adverse outcome disclosure requirements, including rules clarifying the content of the required disclosures, sector-specific guidance, and standards for describing the role of the Covered ADMT. The public comment period on the draft ADMTA rules published on August 11, 2026 is scheduled to extend through at least October 26, 2026.

Key takeaways

- Companies operating in Colorado should consider whether they develop or deploy Covered ADMT, even if they did not meet CAIA's prior definition of "high-risk" AI system.
- Companies operating in Colorado, particularly in the covered domains listed above, should socialize the ADMTA's requirements with their legal and compliance functions to ensure compliance readiness by January 1, 2027 and to consider any opportunities to leverage existing AI compliance plans and strategies.
- Companies should monitor the Colorado Attorney General's ongoing rulemaking to clarify certain ADMTA definitions and requirements.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Matthew J. Bacal

+1 212 450 4790
matthew.bacal@davispolk.com

James W. Haldin

+1 212 450 4059
james.haldin@davispolk.com

David Lisson

+1 650 752 2013
david.lisson@davispolk.com

Howard Shelanski

+1 202 962 7060
howard.shelanski@davispolk.com

David I. Feinstein

+1 212 450 3293
david.feinstein@davispolk.com

This communication, which we believe may be of interest to our clients and friends of the firm, is for general information only. It is not a full analysis of the matters presented and should not be relied upon as legal advice. This may be considered attorney advertising in some jurisdictions. Please refer to the firm's privacy notice for further details.