



LEGAL UPDATE May 22, 2026

Colorado Enacts Artificial Intelligence Replacement Law

Seyfarth Synopsis: *On May 14, 2026, Colorado Governor Jared Polis signed SB 26-189, which replaces the state’s previous AI law with a streamlined framework focused on transparency and disclosure. Effective January 1, 2027, the new law imposes targeted obligations on developers and deployers of automated decision-making technology used in consequential decisions (including employment processes), requiring advance notice, post-decision disclosures, and certain consumer rights. The law centralizes enforcement with the Colorado Attorney General and introduces a fault-based apportionment approach to discrimination liability, while leaving key implementation details to forthcoming rulemaking.*

Background

On May 14, 2026, Colorado Governor Jared Polis signed Senate Bill 26-189 (“SB 189”), which substantially revises the state’s existing artificial intelligence regulatory framework and will take effect January 1, 2027. The new law replaces Colorado’s original AI regulation, Senate Bill 24-205, which was adopted in 2024 and following subsequent legislative action, was scheduled to take effect on June 30, 2026. The law reflects a significant shift in regulatory approach after extensive stakeholder feedback and legislative reconsideration. Senate Bill 24-205 originally contained provisions establishing a duty of care, formal risk management requirements, and impact assessment obligations. SB 189 removes several of these provisions and instead imposes a regulatory framework focusing on disclosure, transparency, and targeted consumer protections in connection with the use of automated decision-making technology (“ADMT”) in “consequential decisions.”

While the substantive obligations of SB 189 take effect January 1, 2027, the state's Attorney General's office is charged with adopting rules to implement and clarify the requirements. Covered entities should therefore expect substantive rulemaking activity in the near term and actively monitor those proceedings, as the forthcoming rules will define key terms and requirements essential to compliance planning. The rules will be helpful as various covered industries, including employers, healthcare institutions, insurers, and others, will have unique considerations as they implement the Colorado requirements.

Changes from Previously Enacted AI Law

The contrast between SB 189 and its predecessor is significant. When Governor Polis signed SB 24-205 in May 2024, he did so with publicly stated reservations, explicitly encouraging the legislature to refine the approach before the law took effect. That invitation set in motion a sustained reconsideration process. The Governor convened an AI Policy Working Group, which engaged in approximately six months of structured stakeholder consultation before publishing a proposed framework in March 2026. The legislative process moved quickly from that point, driven in part by the need to finalize a replacement statute before SB 24-205's approaching June 30, 2026 effective date. Industry stakeholders and the AI Policy Working Group's recommendations were central forces shaping the substance of the resulting legislation. SB 189 reflects that recalibration.

SB 24-205 imposed a formal duty of care, required detailed algorithmic impact assessments, and established a rebuttable presumption of compliance for entities following risk management frameworks, such as the NIST AI Risk Management Framework. SB 189 removes each of these provisions entirely as explicit requirements. In their place, the new law substitutes specific disclosure obligations, three-year record-keeping requirements, and a sixty-day pre-enforcement cure period administered by the Attorney General, that sunsets on January 1, 2030. SB 189 also introduces an interesting fault-based framework for allocating discrimination liability between developers and deployers, a concept SB 24-205 did not address.

Scope: Covered Entities, Tools, and Use Cases

Covered ADMT and Exclusions

A covered ADMT is defined broadly as computational technology that processes personal data and generates outputs such as predictions, recommendations,

classifications, or scores that are used to guide or assist decisions about individuals.

The statute excludes basic infrastructure technologies, tools used only to organize or present information for human review, and consumer-facing conversational tools that are not intended for consequential decision-making.

Deployers and Developers

SB 189 applies to both deployers and developers. A deployer is defined as “a person doing business in Colorado that deploys a covered ADMT.” While a developer is defined as a person doing business in Colorado who (1) “develops, offers, sells, leases, licenses, or otherwise makes commercially available a covered ADMT,” (2) “develops a component that is designed, marketed, intended, documented, advertised, configured, or contracted to be used as part of a covered ADMT,” or (3) “intentionally and substantially modifies an ADMT such that it becomes a covered ADMT.” The law creates several exemptions for developers, including ADMTs developed for research or internal development and commercial support functions, so long as the ADMT is not made available to another person for use in a consequential decision.

Consequential Decisions and Covered Domains

SB 189 only governs the use of “covered ADMT” in situations where the technology materially influences a “consequential decision.” A consequential decision involves determinations affecting a consumer’s access to or eligibility for opportunities in defined “covered domains” including employment, education, housing, financial or lending, insurance, healthcare, and essential government services. The definition broadly captures decisions that affect a consumer’s access to, eligibility for, selection for, or compensation within a covered domain, including decisions that could effectively limit or foreclose that access or opportunity.

Not all automated tools trigger the law’s requirements. Routine operations such as scheduling, administrative routing, and workflow management are excluded, as are tools that simply summarize or present information for human review without generating a score, ranking, or prediction that influences an outcome. In welcome news for employers, fraud prevention activities, including identity verification and monitoring controls required by law, are likewise excluded.

The law also adopts a broad definition of “consumer,” which expressly includes Colorado employees and job applicants whose employment opportunities are evaluated through a covered ADMT.

Deployer and Developer Disclosure Obligations

Under the new law, developers will be required to provide deployers with a general statement of the ADMT's intended uses, known risks and limitations, categories of data used to train the system, and any other information necessary for deployers to meet their disclosure obligations. In addition to providing notice with regard to material modifications, developers must also maintain records for at least three years.

For employers and other deployers, SB 189 establishes a multi-stage notice and disclosure process. Before using covered ADMT for consequential employment decisions (among others), a deployer must provide notice regarding the use of such technology which includes a mechanism for obtaining additional information.

When an adverse outcome (e.g., a decision not to hire) occurs, the deployer must provide additional disclosures within thirty days, including a plain-language explanation of the decision and the role of the ADMT, instructions for requesting further information about the system and its inputs, and applicable rights including a request for meaningful human review and reconsideration of the decision. All notices must be accessible to individuals with disabilities and those with limited English proficiency, and deployers must retain relevant records for at least three years.

New Fault-Based Framework for Determining Liability

A notable feature of SB 189 is its framework for apportioning liability. Both developers and deployers may be held liable under existing anti-discrimination laws with liability allocated based on relative fault. Developer liability is limited to situations in which the technology was used as intended or marketed.

In addition, any indemnification provisions between a developer and deployer that are used to shield either party from liability under relevant discrimination laws are void as contrary to public policy under the new Colorado law. This means parties cannot use contract language to shift responsibility for their own violations of the Colorado Anti-Discrimination Act or other Colorado anti-discrimination laws. However, a developer may avoid this restriction if the covered ADMT was used in a way the developer never intended or documented, provided the developer complied with its obligations under the law.

Enforcement Rests With the Attorney General

Enforcement authority under the law rests exclusively with the Colorado Attorney General. The statute does not create a new private right of action but preserves existing legal remedies under other state and federal laws, including anti-discrimination statutes.

Before initiating enforcement proceedings, the Attorney General must generally provide notice and an opportunity to cure within sixty days, where the Attorney General deems a cure to be possible. The cure period is not available where the Attorney General finds and can demonstrate that the violation was knowing or repeated. The opportunity to cure framework sunsets on January 1, 2030. The Attorney General has broad rulemaking authority and must adopt implementing regulations by January 1, 2027.

Implications for Employers

SB 189 represents a significant change for companies with operations in Colorado. Covered entities, including employers, should inventory their ADMT and related use cases, assess whether those tools materially influence consequential decisions, and prepare to implement robust notice, disclosure, and documentation processes ahead of the law's effective date. Key steps before the January 1, 2027 implementation date include:

- Reviewing and updating vendor contracts to ensure third-party ADMT developers provide required disclosures related to intended use cases, limitations, and training data;
- Auditing current tools to determine whether any qualify as covered ADMTs and whether those tools materially influence consequential decisions affecting employees or applicants;
- Developing pre-use notices and creating workflows to process employee and applicant requests to correct inaccurate personal data;
- Devising post-adverse outcome disclosure notices for all employment-related consequential decisions;
- Establishing a meaningful human review process staffed by trained individuals with authority to override ADMT-driven outcomes;
- Implementing methods to ensure compliance with record-retention requirements.

Because the Attorney General's forthcoming rulemaking may materially affect these obligations, employers should treat compliance planning as an iterative process and revisit their programs as additional guidance is issued.

We will continue to monitor SB 189's implementing regulations and related developments across other states as the AI regulatory landscape continues to evolve. For additional information or questions regarding SB 189 and its implications, please contact the authors of this alert, a member of Seyfarth's People Analytics team, or any of Seyfarth's attorneys.

Seyfarth Shaw LLP provides this information as a service to clients and other friends for educational purposes only. It should not be construed or relied on as legal advice or to create a lawyer-client relationship. Readers should not act upon this information without seeking advice from their professional advisers.

Authors



Annette
Tyman
Partner



Joseph R.
Vele
Associate



Christopher J.
Laudenbach
Associate

Related Practices

[People Analytics](#)

[Employment](#)