Colorado AI Act Two-Pager Cheat Sheet

Created by: **Tatiana Rice**, Deputy Director for U.S. Legislation

Overview: The Colorado AI Act (CAIA) is the first comprehensive and risk-based approach to artificial intelligence (AI) regulation in the United States. This overview highlights the law's requirements governing the private sector's use of AI, including developer and deployer obligations, consumer rights for transparency and the ability to appeal, and enforcement. CAIA will become effective February 1, 2026.

Scope

High-Risk AI System: Any artificial intelligence system that when deployed, makes, or is a substantial factor in making, a consequential decision. (Sec. 6-1-1601(9(a)).

Developer: Any person doing business in the state that develops, or intentionally and substantially modifies an artificial intelligence system, including a general-purpose or high-risk AI system. (Sec. 6-1-1601(7)).

Deployer: Any person doing business in the state that deploys a high-risk AI system. (Sec. 6-1-1601(6)).

Key Terms

Consequential Decision: Any decision that has a material, legal or similarly significant effect on the provision or denial to any consumer of, or the cost or terms of: (A) Education; (B) Employment; (C) Financial or lending services; (D) Essential government services; (E) Healthcare service; (F) Housing, (G) Insurance, or (H) Legal services. (Sec. 6-1-1601(3)).

Substantial Factor: A factor generated by an AI system that is used to assist in making, and is capable of altering the outcome of, a consequential decision (Sec. 6-1-1601(11)).

Algorithmic Discrimination: Any condition where the use of an AI system results in unlawful differential treatment or impact that disfavors an individual or group of individuals based on their protected class. (Sec. 6-1-1601(1)(a)).

**Subject to certain exemptions and carve-outs set forth in Sec. 6-1-1605, including engaging in public interest research, pre-market testing and development, using an AI system approved by a federal agency, such as the FDA or FAA, using an AI system as a HIPAA-covered entity, insurer, or bank, amongst others.*

High-Risk AI Systems

Developer Obligations

Duty of Care: Use reasonable care to protect consumers from known or reasonably foreseeable risks of algorithmic discrimination. (Sec. 6-1-1602(1)).

Deployer Disclosure: Provide disclosures and documentation to deployers regarding intended use, known or foreseeable risks, a summary of data used to train the system, possible biases, risk mitigation measures, and performance, amongst other items. (Sec. 6-1-1602(2)-(3)).

Publicly Available Statement: Maintain a publicly available summary of high-risk systems made available to deployers and risk management for algorithmic discrimination. (Sec. 6-1-1602(4)).

Deployer Obligations

Duty of Care: Use reasonable care to protect consumers from known or reasonably foreseeable risks of algorithmic discrimination. (Sec. 6-1-1603(1)).

Risk Management Policy: Maintain a risk management policy that governs high-risk AI use, which specifies processes and personnel used to identify and mitigate algorithmic discrimination. (Sec. 6-1-1603(2)).

Impact Assessment: Annually conduct (and upon each intentional and substantial modification) an impact assessment that details the purpose, intended use, risk of algorithmic discrimination, steps to mitigate such risks, description of data used and produced, performance, transparency measures, and post-deployment monitoring. Impact assessments must be retained for at least three years. (Sec. 6-1-1603(3)(a)-(b)).

Pre-Deployment Statement of Use: Provide consumers subject to a high-risk system with a statement disclosing information about the high-risk AI system in use, including purpose, nature of the consequential decision, description of how the system assesses information to reach a decision, and

Consumer Rights

Right to Pre-Use Notice: Must be informed of any high-risk AI system used to make, or be a substantial factor in making, a consequential decision about the consumer, and a statement disclosing the purpose and nature of the system. (Sec. 6-1-1603(4)(a)).

Right to Exercise Data Privacy Rights: Must be informed of the right to opt-out of profiling in furtherance of solely automated decisions, under the Colorado Privacy Act, and have the means to exercise those rights, if the deployer is a controller under the CPA. (Sec. Sec. 6-1-1603(4)(a)(III)).

If an adverse consequential decision is made from the use of a high-risk AI system: (Sec. 6-1-1603(4)(b)).

- **Right to Explanation:** The consumer must be provided a statement

Incident Reporting: Must report to the Attorney General when algorithmic discrimination is discovered, either through self-testing or deployer notice. (Sec. 6-1-1602(5)).	sources of personal data processed, among other details. (Sec. 6-1-1603(4)(a)). **Provide Consumer Rights:** Must inform consumers of their rights under the Act and the Colorado Privacy Act and provide the means for the consumer to exercise such rights. Must respond to consumer rights requests within 45 days. (Sec. 6-1-1603(4)(a)(III), (b)). **Publicly Available Statement:** Must make a statement regarding the use of a high-risk AI system available for public inspection. (Sec. 6-1-1603(5)). **Incident Reporting:** Must report to the Attorney General when algorithmic discrimination is discovered. (Sec. 6-1-1603(7)).	explaining the principal reason for the decision, the degree in which the high-risk AI system contributed to the decision, the type of data used in the decision, and the data source. • **Right to Correct:** The consumer must be provided the opportunity to correct any inaccurate personal data used by the high-risk AI system in the decision. • **Right to Appeal:** The consumer must be provided an opportunity to appeal that decision for human review, if technically feasible.

Other Requirements

Attorney General Disclosures: Developers and deployers must provide all required documentation to the Attorney General upon request. (Sec. 6-1-1602(7), 6-1-1603(9)).

AI Interaction Disclosure: Any person or entity that deploys an artificial intelligence system intended to interact with consumers must disclose to the consumer that they are engaging with an AI system. (Sec. 6-1-1604).

Attorney General Enforcement and Rulemaking

Enforcement: The Attorney General shall have the sole exclusive authority to enforce. (Sec. 6-1-1606(1)).

Rulemaking: The Attorney General may promulgate rules to implement and enforce this Act, including requirements regarding:

- Developer documentation;
- Notice;
- Risk management;
- Impact assessment;
- Rebuttable presumptions; and
- Affirmative defenses, including other risk management frameworks that may be acknowledged for compliance.

Defenses and Safe Harbors

Rebuttable Presumption: Developers and deployers of high-risk AI systems maintain a rebuttable presumption of using reasonable care if they are compliant with the relevant bill provisions. (Secs. 6-1-1602(a), 6-1-1603(a)).

Impact Assessment Interoperability: If a deployer completes an impact assessment to comply with another relevant law or regulation, such impact assessment may be used to satisfy this Act's impact assessment requirements. (Sec. Sec. 6-1-1603(3)(e)).

Small Business: If a small business deployer (employing 50 or fewer full-time employees) meets certain requirements, they do not need to maintain a risk management program, conduct an impact assessment, or create a public statement. They are still subject to a duty of care and must provide the relevant consumer notices and rights. (Sec. 6-1-1603(6)).

Affirmative Defense: A developer or deployer that (1) discovers and cures a violation through internal testing or red-teaming, and (2) otherwise complies with the National Institute of Standards and Technology Artificial Intelligence Risk Management Framework or another nationally or internationally recognized risk management framework will have an affirmative defense against any enforcement action commenced by the Attorney General. (Sec. 6-1-1606(3)).