Colorado's Artificial Intelligence Law: What Providers Need to Know

Josh Hansen,
Shook Hardy & Bacon LLP

Colorado's new artificial intelligence (AI) law—colloquially known as the Colorado AI Act[1]—will impact how the Colorado health care community uses AI for hiring, employee evaluations, and even treatment decisions. But don't tune out if you operate outside of Colorado. AI is like catnip for legislators,[2] which means this AI law is likely the first of many that will impact the health care community across the United States. In fact, Connecticut nearly passed a similar bill last year.[3]

With the Colorado AI Act setting the stage for other states' bills governing AI, a closer look is warranted. The Colorado AI Act applies to anyone doing business in the state who uses AI to interact with, or make certain decisions about, Colorado residents. Although the headlines often call the Colorado AI Act a "comprehensive" AI law, that is somewhat of a misnomer because the law neither prohibits AI uses nor adopts

At its core, the Colorado AI Act is a transparency and accountability law: Companies must inform Colorado residents about limited AI uses and establish AI governance measures to prevent discrimination against Colorado residents.

Josh Hansen, an associate at Shook Hardy & Bacon LLP, focuses his practice on privacy and data security issues. He draws on his in-house experience to provide practical, holistic solutions aligned with clients' objectives and risk tolerances. Josh counsels clients on laws governing the appropriate collection, use, and security of customer information. He advises on CCPA, GDPR, GLBA, HIPAA, and similar laws while updating clients on legislative developments and regulators' enforcement activities. Clients seek his guidance on domestic and international contracting, risk assessments, policy development, and product counseling. If things go sideways, clients rely on Josh to interact with regulators and lead all stages of incident response. Outside of work, Josh can be found walking Pliny, his chocolate lab; running on the treadmill; or teaching his one-year-old to root for University of Washington football.

A deployer has four general obligations: use reasonable care to avoid algorithmic discrimination, develop a risk management plan for their high-risk AI, conduct impact assessments for such AI systems, and give notice about their uses of those high-risk AI systems.

sweeping AI regulations. The law has a limited, targeted focus: addressing (already unlawful) discrimination. At its core, the Colorado AI Act is a transparency and accountability law: Companies must inform Colorado residents about limited AI uses and establish AI governance measures to prevent discrimination against Colorado residents. Beyond that, there is a provision that seems to mandate disclosures about certain chatbots too. All these provisions take effect February 1, 2026—unless there are intervening legislative changes (more on that below).

Don't let the limited scope and 2026 effective date lure you into complacency. The law requires attention now, especially as AI becomes integrated into more products and services,[4] including electronic health records (EHRs).[5] Of course, there are some exceptions. But, unlike the Colorado Privacy Act—which largely carved out medical providers[6]—the exceptions in the Colorado AI Act are limited for health care providers. As relevant to the health care community, there are narrow exceptions for medical devices, compliance with federal standards on AI, and treatment decisions by covered entities (but not business associates). This means the health care community will need to consider this law when assessing how they use AI—even when using it to help with medical decisions.

Definitions: Talking the Lingo

The devil is in the details, and the details here start with the definitions. AI is, in some respects, the new "blockchain"—every company is eager to label what they are doing as AI.[7] So the Colorado Legislature had to tackle a threshold issue: What is AI (i.e., what is being regulated by the Colorado AI Act)? Defined too broadly, and the definition of "AI" captures calculators, yet going too narrow risks creating a law with no tangible effect. No easy task. The legislature ultimately settled on a definition that drew from government (EU AI Act and United States Executive Order 14110) and non-government (Organisation for Economic Co-operation and Development AI Principles) sources to define *Artificial Intelligence Systems (AI Systems)* as "any machine-based system that . . . infers from the inputs the system receives how to generate outputs, including content, decisions, predictions, or recommendations, that can influence physical or virtual environments."[8]

But the law, generally, is not regulating all AI systems. The focus is on those systems involved with significant decisions—which the law calls *Consequential Decisions*. A consequential decision is any decision with a material legal or similarly significant effect on the cost, terms, denial, or provision of—as most relevant to physicians—health care services, insurance, and employment or employment opportunities for Colorado residents.[9]

Thus, the focal point of this law is AI systems involved in making Consequential Decisions. These systems are called *High-risk Artificial Intelligence Systems*. Those systems include "any [AI] system that . . . makes, *or is a substantial factor* in making, a consequential decision."[10] The inclusion of "substantial factor" means that the Colorado AI Act cannot be circumvented simply by involving a human in the decision-making process. Even if a human is involved, an AI system is still high risk so long as the AI "assists" in the decision and "is capable of altering the outcome of a consequential decision" (even if it does not do so).[11]

The above terms provide the framework for what systems are being regulated. But the law isn't regulating all uses of those systems. The law is, at its core, an anti-discrimination measure addressing "algorithmic discrimination." *Algorithmic Discrimination* is "the use of an [AI] system result[ing] in an unlawful differential treatment or impact that disfavors an individual or group of individuals" based on certain protected characteristics (e.g., age, disability, race, or veteran status).[12] In short, the crux of the law is a concern about algorithmic discrimination arising from high-risk AI systems (those making consequential decisions).

Obligations: Determining Compliance Measures

The law's requirements differ depending on where in the AI supply chain you sit: developers (creators of high-risk AI systems) versus deployers (users of high-risk AI systems).[13] Developers have one set of obligations, deployers have a separate set of duties, and many requirements apply to both developers and deployers.[14] Given that those in the health care community will often be deployers—the ones using AI—the focus of this article is there.[15]

A deployer has four general obligations: use reasonable care to avoid algorithmic discrimination, develop a risk management plan for their high-risk AI, conduct impact assessments for such AI systems, and give notice about their uses of those high-risk AI systems.[16] There

also is a freestanding provision that appears to require a deployer to disclose when they use an AI-powered chatbot.[17] When considering these obligations, remember that they only: (1) apply to those doing business in Colorado and (2) protect individuals who are Colorado residents.

Reasonable Care

Deployers must use reasonable care to protect individuals from known or reasonably foreseeable risks of algorithmic discrimination.[18] But note that this obligation is not limited to decisions made with high-risk AI systems: A company using a high-risk AI system must take reasonable care to avoid such discrimination by *any* of their AI systems (even those that are not high-risk systems).[19]

Risk Management

Deployers must manage risks of algorithmic discrimination based on their use of high-risk AI-systems. They must adopt a risk-management policy/program to govern their use of high-risk AI systems.[20] The policy and program must (1) be reasonable, (2) be regularly and systematically reviewed and updated, and (3) address how the deployer addresses known or reasonably foreseeable risks of algorithmic discrimination.[21] In addition to the policy and program, deployers must annually review their high-risk AI systems to validate that those systems are not causing algorithmic discrimination.[22]

Impact Assessments

Deployers must perform an "impact assessment" of each high-risk AI system.[23] The assessment must address details such as the purpose, benefits, data involved, metrics for performance, risks of algorithmic discrimination (and measures to mitigate those risks), transparency/disclosure measures, and post-deployment monitoring.[24] Deployers must perform the assessment annually (with the first assessment due by February 1, 2026) *and* within 90 days of making any intentional, substantial modification to the system.[25]

While these impact assessments will be time intensive, the state extended an olive branch for deployers with assessment obligations in multiple jurisdictions. A deployer who completes a legally required impact assessment for another jurisdiction has satisfied Colorado's requirement so long as the assessment is "reasonably similar in scope and effect" to what the Colorado AI Act requires.[26]

Public & Targeted Notices

The Colorado AI Act requires deployers to share certain details about their high-risk AI-systems with individuals. There are two types of notices here: a public notice and a targeted notice directed to impacted individuals.[27]

Beginning with the public notice, deployers must publish a website statement that summarizes:

(1) the type of high-risk AI systems they use;

(2) how the deployer manages the known or reasonably foreseeable risks of algorithmic discrimination from those systems; and

(3) the nature, source, and extent of the data the deployer collects and uses.[28]

In what may be a drafting oversight, the third point is not limited to data used with high-risk AI systems. Taken at face value, a company must address all the information they collect.[29] It is possible this will be cleaned up through the rulemaking that the Colorado Attorney General may, but is not required, to undertake.[30]

The next type of disclosure is the targeted notice. This must be shared with an individual before—and also sometimes after—the high-risk AI system is used to make, or is a substantial factor in making, a consequential decision about the individual.[31] A deployer must notify an individual before using a high-risk AI system for a consequential decision.[32] This pre-use notice must:

(1) describe the system, its purpose, and the decision;

(2) provide the deployer's contact information; and

(3) include instructions for accessing the deployer's public notice (as described in the prior paragraph).[33]

And, when applicable, the pre-use notice must explain the individual's right under the Colorado Privacy Act to opt out of profiling involving their personal information.[34]

Finally, there is the post-use notice. A company must notify an individual after using a high-risk AI system to make a consequential decision that is adverse to the person.[35] The notice must explain the principal reasons for the decision, including: how (and to what extent)

[T]here is no exemption for business associates: Even if they are generating treatment recommendations for the covered entity, they are subject to the law (unless they qualify for another exception).

This law is all but certain to significantly change before it takes effect in February 2026.

the system contributed to the decision, the type of data processed by the system, and the data's source.[36] The company must also provide the individual the opportunity to (1) correct any inaccurate personal data that was involved in the decision[37] and (2) appeal the decision, unless an appeal is not in the individual's best interest.[38]

Both the pre- and post-use notices must be in plain language and translated into languages ordinarily used by the deployer.[39] The deployer must give the notices directly to the individual or, if that is not possible, make the information available in a manner "reasonably calculated to ensure" they receive the information.[40]

Attorney General Notices

Deployers must notify the Colorado Attorney General within 90 days after determining that a high-risk AI system has caused algorithmic discrimination.[41]

Chatbot Disclosures

Deployers are required to inform individuals when they "interact[] with an [AI] system."[42] But companies can avoid this extra disclosure obligation when "it would be obvious to a reasonable person" that they are interacting with AI.[43] Given that "interact" suggests some sort of back-and-forth exchange, and the provision is not part of the statute governing deployers' activities with high-risk AI systems, this disclosure obligation seems geared towards (if not limited to) chatbots. This requirement, while a bit out of left field given the other provisions, is not novel—other states have considered or adopted similar requirements.[44]

Exceptions: Searching for Safe Harbors

There is a lengthy list of exceptions.[45] For example, the Colorado AI Act does not preclude complying with other legal obligations, responding to legal process (such as a subpoena), or defending/prosecuting legal claims.[46] What is missing, however, is a wide-reaching exception for health care providers. In its stead, there are three limited health care carve outs and a more useful small business exception:

- **Medical Devices.** Companies using high-risk AI systems approved by the Food and Drug Administration do not need to comply with the Colorado AI Act for such system.[47]
- **Treatment Recommendations.** A covered entity's use of an AI system to generate health care

recommendations is exempt from the law if (1) the recommendation is not high risk and (2) a health care provider must take action to implement the recommendation.[48]

- **Federal Standards.** Companies using a high-risk AI system that complies with standards set by a federal agency—such as the National Coordinator for Health Information Technology—do not have to comply with Colorado's AI Act for that system only if (and it is big "if") the standards are "substantially equivalent or more stringent" than Colorado's law.[49]
- **Small Business.** A company can avoid some (but not all) obligations if it (1) has fewer than 50 employees, (2) relies on outside data to train their AI system, (3) uses the AI system for its intended purpose, and (4) "makes available" an impact assessment provided by the developer that is substantially similar to what is required of deployers.[50] A company meeting those conditions does not have to provide a public notice, complete impact assessments, or adopt a risk management program.[51] The other obligations, such as using reasonable care and providing targeted notice still apply.

So, one may ask what is missing so far? An exception for business associates. That is right—there is no exemption for business associates: Even if they are generating treatment recommendations for the covered entity, they are subject to the law (unless they qualify for another exception).

Enforcement: Understanding the Risks

The enforcement risks here are (largely) the product of two considerations: (1) the enforcer and (2) the defenses.

In a pro-business move, Colorado assigned exclusive enforcement authority to the Colorado Attorney General—there is no private right of action.[52] While this eliminates nuisance claims and reduces the likelihood of litigation, it does empower a regulator who has shown a significant interest in AI. So, the litigation risk is real. But litigation isn't the only risk: the Colorado Attorney General can also require that deployers turn over records such as risk management policies and impact assessments.[53] Although these requests could lead to a lawsuit under the Colorado AI Act (or potentially expose other issues), it is an open question how aggressive the Colorado Attorney General will be in requesting documentation.

When it comes to defenses, the legislature included some favorable provisions for companies navigating the uncertainty of this new law. First, a company has an affirmative defense when it complies with certain risk management frameworks and proactively addresses violations.[54] Second, a company that complies with the law is entitled to a rebuttable presumption that they used reasonable care to protect individuals from algorithmic discrimination.[55]

Future Changes: Reading the Tea Leaves

This law is all but certain to significantly change before it takes effect in February 2026. The Colorado Attorney General is empowered to, and likely will, engage in rulemaking.[56] And, more importantly, there is widespread agreement that this law is not yet ready for primetime. Governor Polis signed the bill "with reservations"[57] and then business executives shared an open letter voicing concerns about the law's effects.[58] Less than a month later, Governor Polis along with the Colorado Attorney General and the Senate Majority Leader (who sponsored the bill) published a letter outlining a plan to "revise" the law and minimize unintended consequences.[59] They noted the need to focus on improvements in a variety of areas, including: limiting the impact on "smaller companies that may deploy AI within third-party software," refining the scope to target only the "most high-risk systems," and "shifting from a proactive disclosure regime to the traditional enforcement regime managed by . . . investigating matters after the fact."[60] The legislature has a session and a half to work through any changes, so the implemented product is likely to be significantly different than what is in place now.

Practical Impacts: Moving (Somewhat) Beyond the Theoretical

Barring meaningful revision, Colorado's AI Act will have a tangible impact on those in the health care community. Consider a doctor's office that uses an AI tool to help weed through resumes. The Colorado AI Act applies: The office is using a high-risk AI system because they are relying on AI to make employment decisions. Or perhaps a physician is using AI diagnostic tools to generate high-risk treatment recommendations? The Colorado AI Act applies here too. How about a clinic relying on their EHR to suggest treatments without any doctor input? Again, the law applies. Did you skip validating an AI system's ability to provide unbiased results? The law may be an issue: The unfortunate prevalence of biased AI tools (often the result of problematic training data), especially in the

Even if the law doesn't apply to specific health care providers now, AI is growing at such a rapid rate that a provider's situation could be different by the time the law goes into effect.

medical field, creates a meaningful risk for companies that trust without verifying.[61]

The range of possible applications means it is critical that the health care community take steps now to assess whether the law applies to their operations and what is needed to comply. Even if the law doesn't apply to specific health care providers now, AI is growing at such a rapid rate that a provider's situation could be different by the time the law goes into effect.

Preparation: Setting up for Success

With the caveat that the law is likely to change due to rulemaking and legislative tweaks, there are steps the health care and business community should consider now to prepare for the law taking effect in February 2026:

- *Create AI inventory.* Create an inventory that identifies how, when, and where you use AI.
- *Develop a vendor questionnaire.* Ask vendors to explain the AI in their tools you use.[62]
- *Validate AI claims.* Develop a procedure for validating your vendors' representations.[63]
- *Review chatbot usage.* Provide adequate disclosures for any AI-powered chatbots.
- *Identify covered uses.* Build a process to determine when you use AI to make consequential decisions.
- *Monitor developments.* Track what changes the legislature adopts and rules the Colorado Attorney General issues.

This feature article is brought to you by the ***Physician Organizations Practice Group: Christopher Richard,*** *Gilpin Givhan PC (Chair);* ***Adam Laughton,*** *Greenberg Traurig LLP (Vice Chair);* ***Zubin Khambatta,*** *Holland & Knight LLP (Vice Chair);* ***Neerja Razdan*** *(Vice Chair);* ***Mayo Alao****, Hall Render Killian Heath & Lyman PC (Vice Chair); and* ***Jessica Belle,*** *Elevance Health (Vice Chair).*

1 The formal title is "An Act Concerning Consumer Protections with Artificial Intelligence Systems," 2024 Colo. Sess. Law 1199, https://leg.colorado.gov/sites/default/files/documents/2024A/bills/sl/2024a_sl_198.pdf, which makes one thankful for the colloquial name "Colorado AI Act." Although, a catchy backronym could have done wonders for marketing the bill. *But see* Press Release, *Rep. Mike Honda, Rep. Honda Introduces Acronym Act to Clean up Bill Names* (Apr. 1, 2015), (proposing the "Accountability and Congressional Responsibility On Naming Your Motions (ACRONYM) Act of 2014" to "prohibit the addition of words to the title of any bill just to create an acronym").

2 Forty-five states introduced AI legislation during the 2024 legislative session, and 31 states adopted laws or resolutions on AI. *Artificial Intelligence 2024 Legislation*, Nat'l Conf. of St. Legislatures (Sept. 9, 2024), https://www.ncsl.org/technology-and-communication/artificial-intelligence-2024-legislation.

3 S.B. 2, 2024 Gen. Assemb., Reg. Sess. (Conn. 2024), https://www.cga.ct.gov/asp/CGABillStatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB2.

4 Yes, AI is everywhere, even your bird feeder. *Smart Bird Feeder with HD Camera – PF154*, RCA, https://www.rcasmart.com/products/smart-bird-feeder-with-hd-camera-pf147 (last visited Sept. 23, 2024) (advertising "cutting-edge AI Bird Recognition technology").

5 *See* Bill Siwicki, *How Epic is Using AI to Change the Way EHRs Work*, HealthcareITNews (Nov. 28, 2023), https://www.healthcareitnews.com/news/how-epic-using-ai-change-way-ehrs-work.

6 *See* Colo. Rev. Stat. § 6-1-1304(2) (2024) (excluding from the Colorado Privacy Act any protected health information (PHI) or data maintained by a covered entity or business associate in the same manner as PHI).

7 Maybe you recall from the blockchain craze a few years ago when Kodak—yes, the film and camera manufacturer—tried to reinvent itself by launching a cryptocurrency. Shannon Liao, *Kodak Announces Its Own Cryptocurrency and Watches Stock Price Skyrocket*, The Verge (Jan. 9, 2018), https://www.theverge.com/2018/1/9/16869998/kodak-kodakcoin-blockchain-platform-ethereum-ledger-stock-price.

8 Colo. Rev. Stat. § 6-1-1701(2). *Compare id.*, *with* Regulation (EU) 2024/1689 of the European Parliament and of the Council, 2024 O.J. (L 144) 46, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689, *and* Org. for Econ. Co-operation & Dev., *Recommendation of the Council on Artificial Intelligence*, OECD Legal Instruments (May 2, 2024), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449, *and* Exec. Order No. 14110, 88 Fed. Reg. 75191, 75193 (Oct. 30, 2023).

9 Colo. Rev. Stat. § 6-1-1701(3).

10 *Id.* § 6-1-1701(9)(a) (emphasis added).

11 *Id.* § 6-1-1701(11)(a) (defining "substantial factor"). In yet another case of definitions matter, the Colorado Legislature's broad definition of "substantial factor"—merely *assisting* in the decision and *capable* of changing the decision—seemingly flips on its head the layman and legal understanding of the phrase. *See Substantial*, Merriam-Webster, https://www.merriam-webster.com/dictionary/substantial, (defining "substantial" as "important, essential") (last visited Nov. 2, 2024); *Substantial*, Black's Law Dictionary (12th ed. 2019) (defining "substantial" as "[i]mportant, essential, and material; of real worth and importance"). Does this mean that basically any use of AI in connection with a consequential decision is enough to trigger the law? Maybe.

12 Colo. Rev. Stat. § 6-1-1701(1)(a). Note, however, that algorithmic discrimination does not include activities to increase diversity or redress historical discrimination. *Id.* § 6-1-1701(1)(b)(I)(B).

13 *See id.* § 6-1-1701(5)-(7).

14 *Compare id.* § 6-1-1702 (developer obligations), *with id.* § 6-1-1703 (deployer obligations).

15 Apologies to all the doctors using their spare time to create high-risk AI systems.

16 Colo. Rev. Stat. § 6-1-1703.

17 *Id.* § 6-1-1704.

18 *Id.* § 6-1-1703(1).

19 *Id.*

20 *Id.* § 6-1-1703(2)(a).

21 *Id.* Reasonableness requires a consideration of the (1) industry guidance (e.g., National Institute of Standards and Technology standards), (2) deployer's size/complexity, (3) scope and nature of the high-risk AI system (including the intended uses of the system), and (4) volume and sensitivity of data being processed by the system. *Id.* § 6-1-1703(2)(a)(I)-(IV).

22 *Id.* § 6-1-1703(3)(g). The first assessment must be conducted by February 1, 2026. *Id.*

23 *Id.* § 6-1-1703(3)(a).

24 *Id.* § 6-1-1703(3)(b).

25 *Id.* § 6-1-1703(3)(a).

26 *Id.* § 6-1-1703(3)(e).

27 *Id.* § 6-1-1703(4)-(5).

28 *Id.* § 6-1-1703(5)(a).

29 *Id.* § 6-1-1703(5)(a)(III) (requiring "detail" about the information collected and used by a deployer).

30 *Id.* § 6-1-1707(1)(b).

31 *Id.* § 6-1-1703(4).

32 *Id.* § 6-1-1703(4)(a)(I).

33 *Id.* § 6-1-1703(4)(a)(II).

34 *Id.* § 6-1-1703(4)(a)(III).

35 *Id.* § 6-1-1703(4)(b).

36 *Id.* § 6-1-1703(4)(b)(I).

37 *Id.* § 6-1-1703(4)(b)(II). The right to correct is notable in two respects. First, it implicitly creates an obligation to track what information is used in the system. Second, it surreptitiously expands the Colorado Privacy Act: companies must correct personal data even if the company or its data is not subject to that law. Consider: If the personal data is PHI, how does a requirement to correct that information interact with a covered entity's right to deny an individual's request to amend their PHI? *See* 45 C.F.R. § 164.526(a)(2) (2024) (explaining when a covered entity can deny an amendment request).

38 Colo. Rev. Stat. § 6-1-1703(4)(b)(III). Technically, the rights to appeal the decision and correct their information do not have to be in the post-use notice—those opportunities just must be "provided" to the individual. *Id.* § 6-1-1703(4)(b). But, with Colorado having an active privacy regulator, it is probably best to just include the details in the notice.

39 *Id.* § 6-1-1703(4)(c)(I).

40 *Id.* § 6-1-1703(4)(c)(II).

41 *Id.* § 6-1-1703(7). Developers have a similar obligation: They must notify the Colorado Attorney General *and* deployers (plus other developers working on the high-risk AI system) of known or reasonably foreseeable risks of algorithmic discrimination arising from the intended uses of the system. *Id.* § 6-1-1702(5).

42 *Id.* § 6-1-1704(1).

43 *Id.*. § 6-1-1704(2).

44 *E.g.*, Utah Code Ann. § 13-2-12(3) (West 2024) (requiring a chatbot acknowledge its responses are generated by AI when asked by an individual); H.B. 1459, 2024 Leg., Reg. Sess. (Fla. 2024) (requiring a company clearly disclose they are "communicating or interacting with" an individual using AI).

45 Colo. Rev. Stat. § 6-1-1705.

46 *Id.* § 6-1-1705(1).

47 *Id.* § 6-1-1705(5)(a)(I).

48 *Id.* § 6-1-1705(5)(d). Unfortunately, the Colorado AI Act does not define what constitutes a "high-risk" health care recommendation.

49 *Id.* § 6-1-1705(5)(a)(II). But query: Is there a federal standard that has similarly robust notice and disclosure requirements?

50 *Id.* § 6-1-1703(6).

51 Although you aren't required to provide a public notice, a pre-use notice is still needed. *Id.* § 6-1-1703(6). And that pre-use notice must include instructions for accessing the public notice. *Id.* § 6-1-1703(4)(a)(ii).

52 *Id.* § 6-1-1706(1), (6).

53 *Id.* § 6-1-1703(9).

54 *Id.* § 6-1-1706(3).

55 *Id.* § 6-1-1703(1). But one might ask what good is a presumption of compliance if that presumption first requires showing you complied with the law?

56 *Id.* § 6-1-1707(1) (authorizing, but not requiring, the Colorado Attorney General to engage in rulemaking). If it is anything like the Colorado Privacy Act process, one can expect a heavy dose of substantive—not just procedural—obligations that flesh out the bill. *See generally* Colo. Code Regs. § 904-3 (2024).

57 Letter from Jared Polis, Governor of Colorado, to Colorado General Assemb. (May 17, 2024) https://drive.google.com/file/d/1i2cA3IG93VViNbzXu9LPgbTrZGqhyRgM/view. He urged the federal government to act, called on the state legislature to "significantly improve" the law, and said reform was needed so the law "conform[s] with evidence based findings . . . ." *Id.*

58 *See* Tamara Chuang, *Colorado Becomes First State with Law Regulating Potential Consumer Harms of Artificial Intelligence*, Colo. Sun, May 20, 2024, https://coloradosun.com/2024/05/18/colorado-artificial-intelligence-law-signed (discussing a letter from the Colorado Technology Association expressing concerns about the Colorado AI Act).

59 Letter from Jared Polis, Governor of Colorado, *et al.*, to Innovators, consumers, and all those interested in the AI Space, *supra* note 57.

60 *Id.*

61 Because there are known bias issues with commonly used AI tools, *see, e.g.*, Ziad Obermeyer et al., *Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations*, 366 Sci. 447, 447 (2019) (finding that remedying the "significant racial bias" in a "widely used algorithm" would more than double the amount of Black patients referred for additional medical care), it will be difficult to establish that you used reasonable care to avoid algorithmic discrimination if you fail to vet a vendor.

62 Don't skimp on this step just because you are using a hot-shot vendor. A reliance on established vendors is not *per se* sufficient to show you used reasonable care to avoid algorithmic discrimination. There are countless stories about AI bias, even in commonly used AI tools within the medical field. *See, e.g.*, *id.*

63 This point is especially key as it is the wild west out there when it comes to claims about AI. Indeed, one company has already landed in hot water for making deceptive claims about the accuracy of an AI product it sold to health care providers. Press Release, Att'y Gen. Texas, *Attorney General Ken Paxton Reaches Settlement in First-of-its-Kind Healthcare Generative AI Investigation* (Sept. 18, 2024), https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-reaches-settlement-first-its-kind-healthcare-generative-ai-investigation (announcing settlement of claims that a company made false statements about the accuracy and safety of its AI tool that the company sold to hospitals).