

State AI Safety Laws Raise New Liabilities For Healthcare Cos.

By **Jennifer Filippazzo, Melissa Alvarez and Corey Kraftsow** (September 10, 2026)

Artificial intelligence liability is no longer a future concern; it is arriving now — state by state, statute by statute, and, for many companies, through new disclosure, documentation, reporting, safety and consumer protection obligations.

While the federal AI Lead Act, proposed last September as S. 2937, would create a direct product liability framework for artificial intelligence systems if enacted, the more immediate compliance risk is already emerging through state laws that regulate how companies develop, deploy, disclose and oversee AI-enabled tools.[1]

As AI becomes increasingly embedded across healthcare, clinical research and life sciences, companies face a rapidly evolving set of regulatory and compliance obligations, along with new sources of potential liability.

Healthcare and life sciences companies should pay particular attention to this changing legal landscape, especially when AI is incorporated into products or platforms that handle protected health information, optimize administrative functions, process claims, accelerate research or data delivery, or personalize engagement with patients, members, or providers.

Companies should begin a cross-functional AI regulatory readiness review. Emerging AI rules increasingly attach obligations across the full AI lifecycle, including design, development, deployment, customer-facing disclosures, documentation, human oversight, vendor information flows, incident response and consumer rights. These obligations may also affect contractual risk allocation, including limitations of liability, indemnification provisions and insurance coverage.

Several states have enacted AI-focused statutes addressing automated decision-making, companion chatbots and patient disclosures when AI is used in clinical care and expanded developer liability for AI-generated harms.

These laws create statutory duties, enforcement mechanisms, disclosures and compliance records that may become relevant in enforcement actions or private litigation.

This article reviews AI legislation with compliance obligations taking effect on Jan. 1, 2027, with a particular focus on requirements that affect healthcare and life sciences companies, including reporting and disclosure obligations, audit and documentation expectations, and potential enforcement exposure.



Jennifer Filippazzo



Melissa Alvarez



Corey Kraftsow

State AI Laws Emerge as Federal AI Lead Act Remains Pending

The AI Lead Act would create a federal product liability framework for AI systems, allowing civil actions by federal and state attorneys general, individuals and classes. The act would treat covered AI systems as products and permit claims for negligent design, inadequate warnings, breach of express warranty, and defective or unreasonably dangerous AI products.

For healthcare companies using AI tools, the act underscores the need to document intended use, testing, warnings, physician oversight, deployment controls and postlaunch monitoring.

Developers could face strict liability for defective AI systems, while deployers could face liability if they materially modify or misuse the system, or if the developer cannot be sued or satisfy liability.[2]

While the federal bill remains pending, state legislatures have moved more quickly — but through narrower statutes focused on AI disclosure, safety, transparency, reporting, consumer protection and targeted civil-litigation rules, rather than a comprehensive AI product liability regime.[3]

State AI statutes increasingly address frontier model transparency, consumer protection, privacy, safety, mental health representations and related compliance obligations.

Healthcare and life sciences companies are confronting these requirements as they seek to use AI to improve administrative and operational efficiency while preserving access to current medical research, treatment innovation and high-quality patient care.

States Advance Targeted AI Laws Expanding Liability and Compliance Exposure

Several states, including California, Colorado, New York, Tennessee and Washington, have enacted AI legislation regulating developers, deployers, operators or other entities that make AI systems available to consumers.[4]

Colorado

On May 14, Colorado Gov. Jared Polis signed S.B. 26-189, the Automated Decision-Making Technology Act, which takes effect Jan. 1, 2027. This statute addresses and requires transparency when automated decision-making technology is used in areas of insurance, healthcare services and public benefits. Violations are enforceable by the attorney general through the Colorado Consumer Protection Act.[5]

On May 29, Colorado also enacted H.B. 26-1263, the Chatbot Safety Act, effective Jan. 1, 2027.[6] The statute requires operators of public conversational AI services to provide disclosures, restrict harmful outputs, maintain suicide and self-harm protocols, provide privacy tools and avoid presenting AI outputs as licensed professional services.

Under the Chatbot Safety Act an operator is "a person, partnership, corporation, or entity that: (I) develops and makes publicly available a conversation artificial intelligence service; or (II) offers a conversational artificial intelligence service to a consumer." [7] A violation constitutes a deceptive trade practice enforced by the attorney general.

New York

New York has enacted AI-specific legislation including the Responsible AI Safety and Education, or RAISE, Act, codified in General Business Law Article 44-B.[8] The act, effective Jan. 1, 2027, requires large frontier developers to publish and follow safety frameworks and transparency reports addressing catastrophic risk assessment, mitigation, cybersecurity, incident response, governance and internal-use risk management.

The RAISE Act also requires frontier developers to publish transparency reports before or when deploying a new or substantially modified frontier model.[9] Although the RAISE Act does not create a private right of action, it authorizes enforcement by the New York Attorney General's Office and provides civil penalties of up to \$1 million for a first violation and up to \$3 million for subsequent violations.

The RAISE Act's required frameworks, transparency and incident reports, and retained unredacted materials may become relevant in regulatory investigations and may also be sought in later private litigation depending on the claims, parties and applicable discovery rules.[10]

Washington

Washington has enacted H.B. 2225, a law that regulates AI companion chatbots, effective Jan. 1, 2027. The statute requires operators to disclose that an AI companion chatbot is artificially generated, provide recurring disclosures during continued interaction, implement protections for minors, and maintain protocols for detecting and addressing suicidal ideation or self-harm.[11]

Washington's statute imposes affirmative duties on operators and requires suicide and self-harm protocols.

Tennessee

Tennessee has enacted AI regulation with S.B. 1580, a healthcare law that became effective July 1.[12] This act targets and restricts AI advertising by prohibiting developers and deployers from publicly representing that an AI system is, or can act as, a qualified mental health professional.[13]

California

California has led the charge establishing consumer protection statutes by regulating AI systems through three specific pieces of legislation.

S.B. 243 requires operators of companion chatbots to disclose when end users interact with an AI system. It mandates that chatbots not produce self-harm content, requires crisis service referrals when a user expresses suicidal ideation and, beginning July 1, 2027, will require operators to submit annual reports to the Office of Suicide Prevention.[14]

S.B. 53, the Transparency in Frontier Artificial Intelligence Act, requires that developers "write, implement, comply with, and clearly and conspicuously publish" a frontier AI framework. This must describe how developers incorporate standards and best practices, define and assess catastrophic risk thresholds, apply mitigations, identify and respond to critical safety incidents, and assess and manage catastrophic risk from internal model use.[15]

A.B. 316 limits the "AI did it" defense by providing that "in an action against a defendant who developed, modified, or used AI that is alleged to have caused harm," the defendant may not assert as an affirmative defense that the AI "autonomously caused the harm." [16] It does not limit the developer or deployer from presenting any other affirmative defense.

Legislators in other states have proposed civil liability legislation similar to A.B. 316. Vermont's H.B. 855, first introduced in February, relates to defenses in civil actions based on harm caused by AI. In Virginia, S.B. 365 proposes language barring a defense that AI autonomously caused the harm. This February in Maryland, lawmakers introduced H.B. 712, which similarly states that it is not a defense that an AI system autonomously caused the harm. [17]

Illinois

In February, Illinois Sen. Mary Edly-Allen introduced legislation that would explicitly create an AI product liability cause of action. S.B. 3590, the proposed Artificial Intelligence Product Liability Act, would go the furthest of any state, establishing an AI-specific product liability framework for actions against AI developers involving defective design, failure to warn and failure to conform to an express warranty. [18]

The bill defines "product" to mean a "high-impact artificial intelligence system or a generative artificial intelligence system." A deployer would be deemed liable as a developer only if the deployer makes a material and substantial change to the product or intentionally misuses the product contrary to the express warranty such that it proximately causes harm to the plaintiff. S.B. 3590 was rereferred to assignments on May 22. [19]

State AI Laws Create Emerging Compliance Risks for Health and Life Sciences Companies

These state statutes signal a growing trend of protecting consumers and patients against an evolving artificial intelligence landscape. For healthcare and life science companies using developers, deployers and vendors integrating third-party AI tools, the practical takeaway is clear: AI governance can no longer be treated as a purely internal policy exercise.

Healthcare companies using AI in patient-facing and clinical workflows should assess whether their AI systems are covered by these new laws and whether required disclosures, safety protocols, incident-reporting procedures, and record-retention processes are operational. They should also review contracts with AI vendors to ensure appropriate allocation of responsibility for compliance, data access, documentation and litigation cooperation.

This obligation cannot be ignored, even when development and integration of the AI system are outsourced to an AI engineering platform for design and implementation. Companies deploying AI in healthcare workflows should ensure that vendor agreements address regulatory compliance, documentation, testing, monitoring, disclosures, incident support, indemnification and insurance.

Safety frameworks, transparency reports, user disclosures, human review procedures, self-harm protocols and incident reports may become key materials in future regulatory investigations, enforcement actions, discovery disputes and civil litigation.

Companies that develop, deploy or rely on AI should use the current implementation period

to identify applicable obligations and document governance decisions and protocols.

This is especially critical as the demand for personalized medicine continues to grow and encourages the ongoing development of new AI tools in the healthcare sectors. Indeed, the desire to enhance patient engagement and expedite backend record processes should not come at the expense of insuring that patient care decisions and treatments comply with rigorous standards of care.

Healthcare AI Litigation Tests Traditional Liability Theories Against AI Providers

Indeed, state enforcement agencies and plaintiffs have begun testing legal theories against AI providers, including consumer protection, professional licensing, negligence, nuisance and product liability doctrines. Three matters from this year illustrate the trend.

The plaintiff in *Pennsylvania Board of Medicine v. Character Technologies Inc.*, filed May 1 in the Commonwealth Court of Pennsylvania, is pursuing a professional licensing theory, alleging Character.AI chatbot personas misrepresented themselves as licensed medical professionals and provided medical advice. The action sought injunctive relief to stop alleged unauthorized practice of medicine, including based on interactions with a chatbot called Emilie.[20]

Florida Attorney General v. OpenAI Global LLC, filed June 1 in the 10th Judicial Circuit Court of Florida, alleges that ChatGPT was marketed safe for use despite risks involving false information, inadequate age verification and engagement-reinforcing design. The complaint asserts misrepresentation, nuisance, negligence, gross negligence and strict product liability claims for design defects and failure to warn.[21]

In *Winters v. OpenAI INC.*, filed July 21 in California's San Francisco County Superior Court, Scott Winters filed a private personal-injury suit alleging that reliance on ChatGPT-4o for medical guidance contributed to a near-fatal pulmonary embolism. The suit pleads product liability and negligence theories, including allegations that the model's engagement-optimizing features constitute a design defect or failure to warn by intentionally prioritizing continued engagement over safety.[22]

Key Takeaways for Health and Life Science Companies Using AI

Recent actions involving Character Technologies and OpenAI show that regulators and plaintiffs are already testing traditional legal theories against generative AI providers, including consumer protection, negligence, licensing, nuisance and product liability.

Although courts have not yet resolved how these theories will apply, healthcare and life sciences companies should not wait for comprehensive federal AI legislation.

Companies using patient-facing AI tools should evaluate whether they have clear transparency disclosures, defined physician oversight, limits on chatbot-generated advice, escalation protocols and ongoing monitoring of patient interactions.

For healthcare developers, vendors and deployers, the immediate priority is to identify applicable obligations, assign compliance responsibility, document governance decisions and preserve records that may later be reviewed by regulators or litigants.

The next wave of AI liability may turn less on new federal law than on the strength of a company's own compliance record.

Jennifer L. Filippazzo is a partner, Melissa R. Alvarez is counsel and Corey Kraftsow is an associate at McDermott Will & Schulte.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] See S. 2937, 119th Cong. (2025).

[2] S. 2937, 119th Cong. §§ 3(3) 302 (2025).

[3] See S. 2937, 119th Cong. (2025); see also, e.g., Cal. Civ. Code § 1714.46; Cal. Bus. & Prof. Code §§ 22601-22603; N.Y. Gen. Bus. Law art. 44-B.

[4] See, e.g., Cal. Bus. & Prof. Code §§ 22601-22603; Cal. Civ. Code § 1714.46; N.Y. Gen. Bus. Law art. 44-B; Tenn. Code Ann. § 33-1-205; H.B. 2225, 69th Leg., Reg. Sess. (Wash. 2026).

[5] S.B. 26-189, 75th Gen. Assemb., Reg. Sess. (Colo. 2026).

[6] H.B. 26-1263, 75th Gen. Assemb., Reg. Sess. (Colo. 2026).

[7] *Id.*

[8] N.Y. Gen. Bus. Law arts. 44-B.

[9] N.Y. Gen. Bus. Law § 1421.

[10] See N.Y. Gen. Bus. Law §§ 1421, 1427.

[11] H.B. 2225, 69th Leg., Reg. Sess. §§ 3-5 (Wash. 2026).

[12] Tenn. Code Ann. § 33-1-205; S.B. 1580, 114th Gen. Assemb. (Tenn. 2026).

[13] *Id.*

[14] Cal. Bus. & Prof. Code §§ 22601-22603.

[15] Cal. Bus. & Prof. Code § 22757.12; S.B. 53, 2025-2026 Reg. Sess. (Cal. 2025).

[16] Cal. Civ. Code § 1714.46.

[17] H. 855, 2025-2026 Gen. Assemb., Reg. Sess. § 1 (Vt. 2026); S.B. 365, 2026 Gen. Assemb., Reg. Sess. § 59.1-617(A)-(B) (Va. 2026); H.B. 712, 2026 Gen. Assemb., Reg. Sess. § 3-2705(c) (Md. 2026).

[18] S.B. 3590, 104th Gen. Assemb. (Ill. 2026).

[19] LegiScan, S.B. 3590, 104th Gen. Assemb. (Ill. 2026), <https://legiscan.com/IL/bill/SB3590/2025> (last visited Aug. 4, 2026).

[20] Commonwealth of Penn. v. Character Techs., Inc., Case No. 2020 MD 2026. Pet. (Pa. Commw. Ct. May 1, 2025).

[21] Office of Att'y Gen. v. OpenAI Global, LLC et al., Compl. ¶¶ 172-308 (Fla. Cir. Ct. June 1, 2026).

[22] Winters v. OpenAI, et al., Case No. TC26-2457, Compl. at ¶¶ 76-210 (San Francisco Super. Ct., CA, July 21, 2026).