

Blog Post

New Year, New AI Rules: Healthcare AI Laws Now in Effect

January 5, 2026

By Jordan T. Cohen and Elizabeth F. Hodge

As healthcare organizations ring in 2026, they will also be ringing in a new era of AI regulation. With Congress yet to pass comprehensive AI legislation and federal regulatory guidance in flux, states have stepped in to fill the void. The new year will see several new laws imposing disclosure, transparency, and data protection requirements on those developing, deploying, or using AI in healthcare settings. This post highlights the key laws healthcare organizations should have on their radar.

California: No More Pretending to Be a Doctor

California has been particularly active in regulating AI in healthcare. Building on AB 3030 and SB 1120, which went into effect in January 2025, the state has added new requirements targeting AI systems that may mislead patients into believing they are interacting with licensed healthcare professionals.

Effective January 1, 2026, AB 489 prohibits developers and deployers of AI systems from using terms, letters, phrases, or design elements that indicate or imply the AI possesses a healthcare license. The law also bars AI advertising or functionality that suggests care is being provided by a natural person with the appropriate license when it is not.

Related People

Jordan T. Cohen
Elizabeth F. Hodge

Related Work

Data Privacy and Security
Healthcare
Healthcare Legislation and Government Affairs
Healthcare Licensure and Compliance

Related Offices

New York
West Palm Beach

Health Law Rx

Akerman Perspectives on the Latest Developments in Healthcare Law

[Read blog posts](#)

What makes AB 489 notable is its enforcement mechanism: healthcare professional licensing boards now have jurisdiction over these violations and may pursue injunctions under existing licensing law.

California also enacted SB 243, effective the same day, which regulates “companion chatbots” that are designed to provide ongoing interaction and emotional support. The law requires clear notification that users are interacting with AI and mandates protocols to (i) prevent responses about suicidal ideation or actions with the user that could encourage self-harm or suicidal ideation and (ii) provide a notification to the user that refers the user to a crisis service provider if the user “expresses suicidal ideation, suicide, or self-harm.”

Organizations offering mental health support apps, patient engagement chatbots, wellness platforms, or communication tools should pay close attention.

California is not alone; Illinois, Nevada, and Utah have all begun regulating chatbots to varying extents.

Texas: New Disclosure Requirements for the Use of AI

Meanwhile, Texas has enacted one of the most far-reaching AI laws in the country. The Texas Responsible Artificial Intelligence Governance Act (TRAIGA), signed into law in June 2025 and effective January 1, 2026, establishes a broad range of governance and other requirements for the use of AI systems. However, it also contains specific disclosure requirements for licensed healthcare practitioners. Under TRAIGA, practitioners must provide patients (or their personal representatives) with conspicuous written disclosure of the provider’s use of AI in the diagnosis or treatment of the patient. This disclosure must occur before or at the time of interaction. In emergencies, disclosure must be provided as soon as reasonably practicable.

In addition to the disclosure requirement, TRAIGA prohibits the use of AI systems that have the specific intent to discriminate against individuals based on protected characteristics, though a disparate impact alone is not sufficient to establish discriminatory intent.

Enforcement of TRAIGA rests with the Texas Attorney General, who can impose civil penalties ranging from \$10,000 to \$200,000 per violation, with amounts varying based on whether the violation is curable. Those penalties can accrue daily for ongoing violations, so compliance is not something to postpone.

TRAIGA follows a separate Texas law (SB 1188) that became effective on September 1, 2025. SB 1188 allows practitioners to use AI for diagnostic or treatment purposes provided that the practitioner is acting within the scope of the practitioner's license and personally reviews all AI-generated content or recommendations before a clinical decision is made. Like TRAIGA, SB 1188 also requires professionals to disclose the use of AI to their patients.

AI Transparency: What's Under the Hood?

Beyond healthcare-specific requirements, several states are imposing broader AI transparency obligations that will affect healthcare organizations. For example, California's AI Transparency Act ([SB 942](#)), also effective January 1, 2026, requires "covered providers" (defined as those with one million or more monthly users) to offer free tools allowing users to determine whether content was AI-generated. Telehealth platforms, patient portals, and healthcare marketing operations with significant user bases should assess whether these requirements apply to them.

Similarly, California's [AB 2013](#) requires AI developers to disclose information about the data used to train their generative AI systems. Healthcare AI vendors must be prepared to answer questions

about what data trained the clinical decision support, diagnostic, or communication tools they are selling.

Organizations should not assume vendors “own” compliance. Deployers remain accountable, and contracts, diligence practices, and governance expectations must evolve accordingly. Key questions for vendor relationships now include training data sources, bias testing protocols, validation controls, and ongoing performance monitoring.

The Virginia Model Hits the Midwest and New England

If the consumer privacy laws taking effect in [Indiana](#), [Kentucky](#), and [Rhode Island](#) on January 1, 2026, look remarkably similar, that is no coincidence. All three are based on the Virginia Consumer Data Protection Act (VCDPA), which has served as a template for state privacy legislation across the country. The VCDPA model provides consumers with rights to access, correct, delete, and port their data, as well as the right to opt out of targeted advertising, data sales, and, importantly for AI, profiling that produces legal or similarly significant effects.

These laws also require data protection impact assessments for high-risk processing activities, including profiling. The good news for HIPAA-regulated entities is that all three laws exempt protected health information and provide carve-outs for covered entities and business associates acting within the scope of HIPAA. But this is not a blanket exemption for healthcare organizations as it applies to the *data* and *activities* regulated by HIPAA, not to everything a healthcare organization does.

A Wrench in the Works: The December 11 Executive Order

Just as healthcare organizations were gearing up for January 1 compliance, the White House threw a curveball. On December 11, 2025, President Donald

Trump signed an executive order, titled “[Ensuring a National Policy Framework for Artificial Intelligence](#)” (the AI Executive Order), that aims to preempt state AI laws and establish a “single national framework” for AI regulation.

The order directs the U.S. Attorney General to establish an AI Litigation Task Force within 30 days, charged with challenging state AI laws that the administration deems inconsistent with federal policy — including on grounds that such laws unconstitutionally regulate interstate commerce or are preempted by federal regulations. The U.S. Secretary of Commerce must identify “onerous” state AI laws within 90 days, and the order specifically calls out Colorado’s AI Act as an example of problematic state regulation.

What does this mean for the laws discussed above? Uncertainty. The AI Executive Order does not immediately invalidate any state law, and critics have already suggested it will face legal challenges. But it does signal that the federal government may actively oppose enforcement of certain state AI requirements, potentially including some of the laws that took effect on January 1, 2026.

For now, these state laws remain on the books. Organizations should continue compliance preparations while closely monitoring federal developments. The patchwork of state regulation that prompted this AI Executive Order is unlikely to disappear overnight, and healthcare organizations operating in multiple states will need to navigate this evolving legal landscape carefully.

Next Steps

Healthcare organizations developing, deploying, or using AI should consider the following as the new year begins:

- **Audit patient-facing AI systems.** Identify any AI tools that interact with patients and assess

whether their design or functionality could be interpreted as implying licensure or human oversight that does not exist.

- **Implement disclosure protocols.** For organizations operating in Texas, develop workflows to ensure patients are informed of AI use in diagnosis or treatment before or at the point of care.
- **Assess privacy law applicability.** Determine whether consumer data processing activities fall outside HIPAA's scope and may trigger obligations under Indiana, Kentucky, Rhode Island, or other state privacy laws.
- **Continue to monitor developments in healthcare AI at the state level.** As of now, state legislators continue to propose bills regulating the use of AI in healthcare. These proposals include preventing the unauthorized practice of medicine or other professions requiring licensure and overseeing the use of AI by health insurers in utilization review, claims handling, and other areas of concern.

The patchwork of state AI regulation is only going to grow more complex, and the December 11 AI Executive Order adds a new layer of federal-state tension. Organizations that invest in compliance infrastructure now will be better positioned to adapt as the legal landscape continues to shift. Health Law Rx will continue to monitor these developments and provide updates as states, courts, and the federal government refine their approaches to AI governance in healthcare.

This information is intended to inform firm clients and friends about legal developments, including recent decisions of various courts and administrative bodies. Nothing in this Practice Update should be construed as legal advice or a legal opinion, and readers should not act upon the information contained in this Practice Update

without seeking the advice of legal counsel. Prior results do not guarantee a similar outcome.