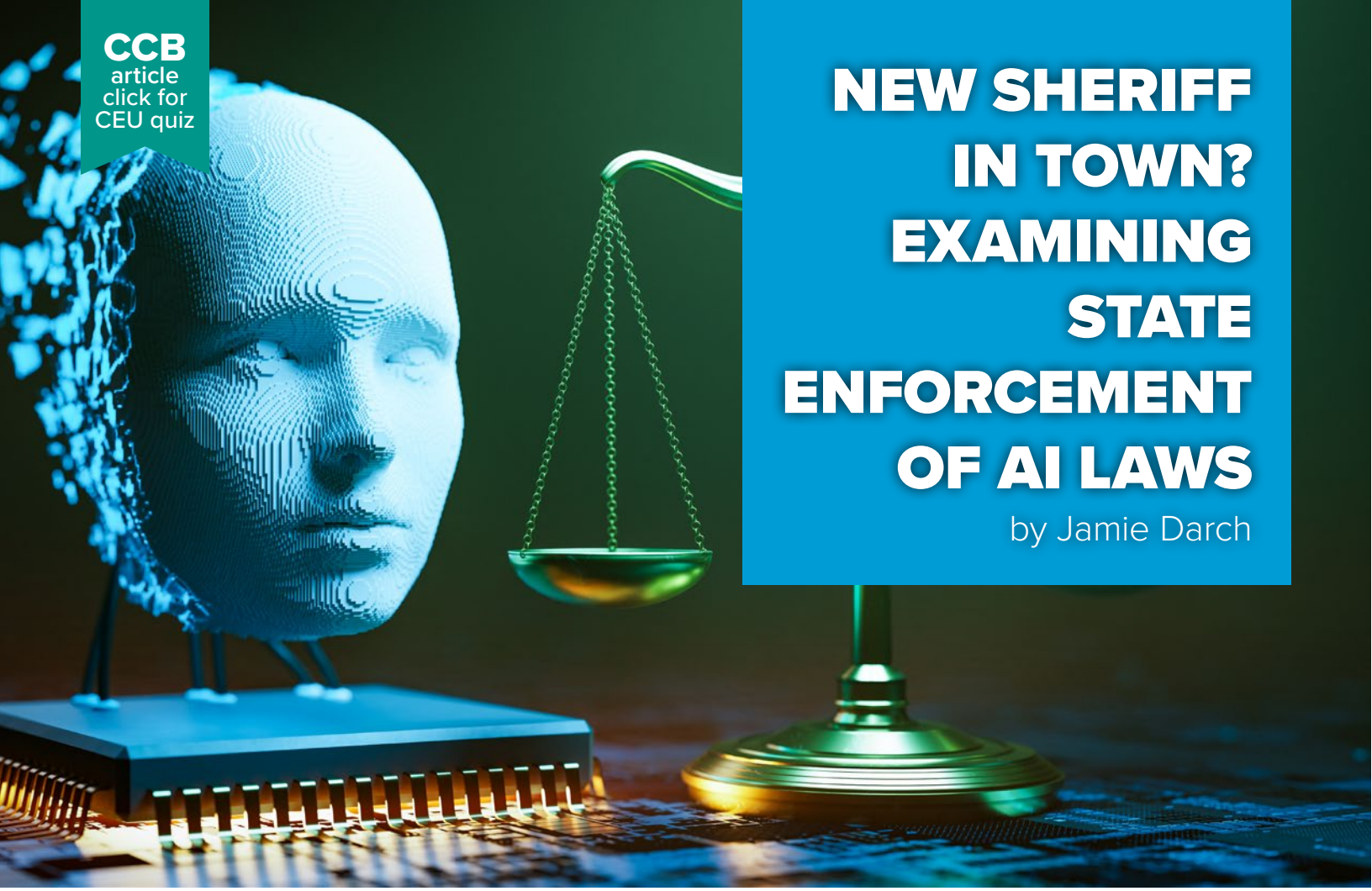
CCB article click for CEU quiz



# NEW SHERIFF IN TOWN? EXAMINING STATE ENFORCEMENT OF AI LAWS

by Jamie Darch


**Jamie Darch**

*(Jamie.Darch@ropesgray.com, https://bit.ly/linkedin-JamieDarch) is a Partner in Ropes & Gray's health care practice in Chicago, IL.*


States have enacted laws targeting AI development and deployment by healthcare stakeholders, including payers, providers, and developers. These laws reflect growing concern about healthcare-specific risks of leveraging AI in insurance coverage decisions, clinical care, and patient communications, as well as broader risks like algorithmic bias, discrimination, privacy breaches, and consumer harm.[1]

In enacting such laws, states have empowered different state agencies and regulators to oversee compliance and initiate enforcement actions if noncompliance is identified. These AI-specific laws create an additional pathway for enforcement, augmenting existing mechanisms based on generally applicable laws regulating consumer protection and deceptive trade practices.

In this article, we review these newly available enforcement mechanisms, as well as past enforcement actions involving AI in healthcare, to forecast how these new mechanisms may be used in the future.

## New mechanisms for state enforcement of health AI laws

In enacting AI-specific laws, states have authorized several different state agencies to oversee compliance. Many AI laws for healthcare stakeholders are enforced by the agencies already regulating them. For example, state laws regulating AI in payer coverage decisions and utilization review (UR) authorize state departments of insurance (e.g., Alaska Director of Insurance)[2] and state departments of health (e.g., California Department of Managed Health Care)[3] to oversee compliance by payers and their vendors.

In contrast, many state AI laws targeting use of AI by licensed healthcare professionals authorize the

corresponding professional board to enforce violations of such laws (e.g., in Nevada, professional boards enforce provisions governing AI use in patient communications by licensed professionals).[4] State AI laws with broader reach—like the Texas Responsible Artificial Intelligence Governance Act[5] or Utah's Artificial Consumer Protection Amendment[6]—often equip state attorneys general and consumer protection bureaus with enforcement power.

The menu of enforcement options available to state agencies varies significantly by state. Several states authorize civil and administrative fines ranging from $5,000 (e.g., in Alaska, administrative fines may not exceed $5,000 for a violation that occurred with such frequency as to indicate a general business pattern or practice)[7] to $200,000 (e.g., in Texas, penalties range from $2,000 to $40,000 for each day a violation continues, or between $10,000 and $12,000 for each discrete violation that is curable or between $80,000 and $200,000 for each violation that is not curable)[8] per violation. Some states define each day an entity is out of compliance as a separate violation (e.g., under California's AI Transparency Act, each day is a discrete violation subject to a $5,000 penalty).[9] Total potential liability under these laws can thus escalate rapidly.

In addition to monetary penalties, some states allow regulatory bodies to seek equitable relief, such as injunctions or specific remedies.[10] For example, in Georgia, failing to meet the physician oversight requirement for UR results in automatic approval of the healthcare service.[11] In Pennsylvania, the Pennsylvania Insurance Department may prohibit insurers or care plans that violate AI laws from enrolling new members.[12] Moreover, violation of certain laws could result in suspension, probation, or revocation of professional licenses (e.g., in Texas, sanctions include suspension, probation, or revocation of a license, registration, certificate, or other authorization to engage in an activity, as well as a monetary penalty not to exceed $100,000)[13] or certification (e.g., certain insurance boards, like the Rhode Island Office of the Health Insurance Commissioner, may suspend or revoke certification for UR programs and impose fines up to $50,000 per violation if a review agent fails to comply with the law's requirements, which do not expressly mention AI but nonetheless prevents the use of AI to make UR decisions by requiring a licensed practitioner to make such decisions).[14] California even authorizes criminal penalties for willful violations of healthcare service plan requirements, punishable by not more than one year of imprisonment.[15]

Many of these laws are newly enacted—and some are being slow-rolled or even reconsidered by state legislatures (e.g., while Colorado's landmark AI law was initially passed in 2024, its effective date was postponed to 2026, then ultimately repealed and replaced with a less burdensome framework now set to go into effect on January 1, 2027)[16]—so enforcement under such laws has not yet occurred. However, we look to AI-focused enforcement actions and litigation trends as potential predictors of future state enforcement priorities.

### State enforcement spotlight: *Texas AG v. Pieces Technologies*

The most significant example of state AI enforcement to date is the Texas attorney general (AG)'s action against Pieces Technologies Inc., a health tech company that develops AI tools for hospitals and clinicians.[17] While this example was brought forth under the Texas Deceptive Trade Practices—Consumer Protection Act (DTPA), and not any AI-specific law, the underlying fact pattern would likely implicate newly enacted state AI laws, and it could result in additional penalties under those laws.

**In addition to monetary penalties, some states allow regulatory bodies to seek equitable relief, such as injunctions or specific remedies.**

In *Texas AG v. Pieces Technologies* (*Pieces*), the Texas AG alleged that the developer misrepresented the accuracy of its AI products; specifically, the state alleged that the company advertised and marketed the accuracy of its generative AI products by claiming that they have extremely low hallucination rates, without sufficient substantiation in place to support such rates.[18] The Texas AG also raised concerns that the developer's marketing and disclosure practices ran afoul of state consumer protection standards because such representations regarding its generative AI products "may have violated the DTPA because they were false, misleading, or deceptive."[19]


While the Texas AG had the authority under the relevant law to seek injunctive relief, restitution, or civil penalties of up to $10,000 per violation,[20] the matter was resolved through an assurance of voluntary compliance (AVC), a negotiated settlement that does not impose monetary penalties or constitute an admission of liability, but creates ongoing compliance obligations.[21]

During the five-year term of the AVC, the developer must clearly disclose and substantiate any performance metrics featured in its marketing materials, refrain from making false or unsubstantiated claims about its AI products, provide customers with documentation about risks and limitations of its AI products, disclose any financial arrangements with individuals or entities that are endorsing or marketing the product, and respond to compliance information requests from the Texas AG within 30 business days of receipt of a written request.[22] The AVC does not preclude future enforcement actions or private rights of action.[23] Indeed, the AVC specifies that "[n]othing herein constitutes approval or acquiescence by the State of [Pieces Technology]'s past practices, current efforts to reform their practices, or any future practices," thereby leaving open the door for additional enforcement if issues arise.[24]

The issues underlying *Pieces* are likely to arise in future enforcement actions by states under AI-specific laws that apply additional scrutiny to claims made by healthcare industry developers and deployers about AI systems. In addition to focusing squarely on how AI developers create AI models, leverage training data, mitigate bias and discrimination, and otherwise ensure the accuracy of their products, the new wave of AI laws creates additional regulatory touchpoints that give state regulators the opportunity and requisite information, to pursue enforcement.

For example, states like California (which requires healthcare service plans to ensure that disclosures "pertaining to the use and oversight of the artificial intelligence, algorithm, or other software tool are contained in the written policies and procedures")[25] and Maryland (which similarly requires healthcare payers to ensure that written policies and procedures are included in the utilization plan "including how an artificial intelligence, algorithm, or other software tool will be used and what oversight will be provided")[26] require proactive submissions to regulators by entities that deploy AI in insurance and UR, requiring entities to submit AI-related policies, procedures, and algorithms for approval prior to deployment. State AI laws have also expanded the authority of regulatory agencies to conduct ad hoc audits (e.g., in California, the Department of Managed Health Care is authorized to inspect AI tools in UR for audit or compliance reviews)[27] and inspections (e.g., in Maryland, payers deploying AI tools must ensure that such tools are "open to inspection for audit or compliance reviews" by the Commissioner of Insurance)[28] of AI systems and governance structures.

Such laws also impose ongoing obligations on entities to audit and monitor their AI systems and report issues to regulatory agencies within timelines specified by state law (e.g., in California, beginning in July 2027, entities that operate companion chatbots must submit annual reports to the California Department of Public Health's Office of Suicide Prevention).[29] While these reporting obligations do not automatically trigger formal investigations or enforcement actions, they create a clear pathway for regulators to initiate inquiries, such as demanding disclosure

of documents (e.g., in Maryland, a payer's mandatory quarterly reporting of adverse decisions, including those based on utilizing AI services, to the Commissioner of Insurance provides the basis for the Commissioner to demand disclosure of the payer's AI compliance and oversight policies and audit materials)[30] or issuing a civil investigative demand (e.g., in Texas, if the AG receives a complaint through the online mechanism alleging a violation, the AG may issue a civil investigative demand to determine if a violation has occurred).[31] Moreover, expanded requirements to disclose the use of AI tools to patients and beneficiaries are likely to trigger additional complaints that may result in regulatory inquiries (e.g., in California, health facilities and clinics are required to provide clear disclaimers when AI-generated communications are used).[32]

## Litigation focus

Most state AI laws regulating healthcare stakeholders enacted to date have not created additional private rights of action. However, existing private rights of action under state consumer protection statutes (e.g., California's Consumer Privacy Act provides a limited private right of action for data breaches, permitting the recovery of damages between $150 and $750 per consumer per incident or actual damages, whichever is greater)[33] remain available to litigants, and an increase in scrutiny and state enforcement actions under these new AI laws may bring into focus AI issues that could be pursued by litigants under existing avenues.

We have already seen such litigation[34] take shape over AI use in healthcare insurance decisions, with beneficiaries suing insurers for violating both specific statutes that require meaningful physician review for coverage denials and general consumer protection statutes, as well as underlying health plan agreements.[35] Further, one recently enacted law in California covering companion chatbots, as previously mentioned, scheduled to go into effect in July 2027, creates a private right for impacted users of a companion chatbot by permitting a person who suffers injury as a result of a violation of the companion chatbot law to bring a civil action to recover injunctive relief and actual damages.[36] To the extent more states follow suit, we can expect additional litigation to follow.

## The federal overlay — or lack thereof

The federal approach to regulating and enforcing AI in healthcare has shifted rapidly across administrations. The Biden administration took numerous steps to implement an AI regulatory framework,[37] and prompted federal agencies to initiate high-profile inquiries related to AI products and services. For example, in September 2024, the Federal Trade Commission (FTC) initiated Operation AI Comply, an enforcement sweep targeting five companies that made exaggerated or false claims about their AI tools' capabilities.[38] Similarly, the U.S. Department of Justice began investigating Troy Health, a Medicare Advantage plan provider, for its use of AI to unlawfully access beneficiary information, enroll individuals in its plans without their knowledge or consent, and offer kickbacks to pharmacies for enrollment referrals through its AI platform.[39]

In contrast, the Trump administration has consistently sought to deregulate the development and deployment of AI across sectors, including healthcare.[40] Most recently, a sweeping executive order titled "Ensuring a National Policy Framework for Artificial Intelligence"[41] aims to create a preemption framework and task force to challenge state AI laws.[42]

Though the Trump-era FTC has continued to review AI for specific priorities, such as children's privacy and safety,[43] broader federal enforcement efforts during President Donald Trump's second term seem unlikely given the administration's deregulatory priorities. Even more, Trump's executive order suggests that the federal government could focus its preemption efforts on state AI laws that are more actively being enforced, teeing up a battle between state and federal governments over the scope of federal preemption.

## Final thoughts

The proliferation of state AI laws regulating healthcare stakeholders has created a potential enforcement minefield, with a range of state agencies poised to scrutinize and penalize entities that fail to comply with the patchwork of state AI regulations. The federal overlay remains fluid and potentially volatile, as states that have challenged President Trump on other fronts may welcome the opportunity to spar with the Trump administration over preemption grounds — particularly over concerns with AI that reverberate with the general public on both sides of the aisle.

Given the looming threat of enforcement, entities that seek to use AI in healthcare must implement a robust AI governance function to ensure that development and deployment of AI models withstand regulatory scrutiny and continue to monitor ongoing state and federal regulatory and enforcement developments in this space. CT

**Endnotes**

1. Ropes & Gray, "Ropes & Gray Launches Health AI Atlas, A Health Care AI State Laws Tracker," news release, January 6, 2026, https://www.ropesgray.com/en/news-and-events/news/2026/01/ropes-gray-launches-health-ai-atlas-a-health-care-ai-state-laws-tracker.
2. Alaska Admin. Code tit. 3, § 28.989.
3. Cal. Health & Safety Code § 1367.01(h)(6).
4. A.B. 406, § 8(5), 83d Leg. (Nev. 2025).
5. Tex. Bus. & Com. Code § 552.106.
6. Utah Code Ann. § 13-75-101 et seq.
7. Ala. Code § 27-3A-5.
8. Tex. Bus. & Com. Code § 552.
9. Cal. Bus. & Prof. Code § 22757.4.
10. Cal. Civ. Code § 1798.199.90(a); Utah Code Ann. § 13-72a-204.
11. Ga. Code Ann. § 33-46-29.
12. 40 Pa. Stat. § 991.2182.
13. Tex. Bus. & Com. Code § 552.106.
14. R.I. Gen. Laws § 27-18.9-13.
15. Cal. Health & Safety Code § 1390(a).
16. Colo. Rev. Stat. § 6-1-1701 *et seq*. For more information on the new Colorado AI law, see Ropes & Gray, "Colorado Scales Back AI Law, with Targeted Implications for Health Care," client alert, May 19, 2026, https://www.ropesgray.com/en/insights/alerts/2026/05/colorado-scales-back-ai-law-with-targeted-implications-for-health-care.
17. Petition, In re State of Texas & Pieces Techs., Inc., No. DC-24-13476 (Dist. Ct. ____) (hereinafter Pieces AVC).
18. Pieces AVC ¶ 13.
19. Pieces AVC ¶ 14.
20. Tex. Bus. & Com. Code § 17.47(c).
21. Pieces AVC.
22. Pieces AVC ¶¶ 17–19.
23. Pieces AVC ¶¶ 24–26.
24. Pieces AVC ¶ 25.
25. Cal. Health & Safety Code § 1367.01(k)(1).
26. Md. Code Ann., Ins. § 15-10B-05.1(c)(8).
27. Cal. Health & Safety Code § 1367.01(k)(1)(G).
28. Md. Code Ann., Ins. § 15-10B-05.1(c)(7).
29. S.B. 243 § 22603, 2023 -2024 Reg. Sess. (Cal. 2024).
30. Md. Code Ann., Ins. § 15-10B-05.1(c)(8).
31. Tex. Bus. & Com. Code § 552.103.
32. Cal. Health & Safety Code § 1339.75(a).
33. Cal. Civ. Code § 1798.150.
34. For example, in Kisting-Leung v. Cigna Corp., 780 F. Supp. 3d 985 (E.D. Cal. 2025) insured individuals alleged that Cigna used an automated algorithm known as "PxDx" to deny claims for medical necessity without meaningful physician review. Plaintiffs brought claims under ERISA § 1132(a)(1)(B) for wrongful denial of benefits, Employee Retirement Income Security Act (ERISA) § 1132(a)(3) for breach of fiduciary duty, and California's Unfair Competition Law (UCL), Cal. Bus. & Prof. Code § 17200 (2025). Under UCL, plaintiffs alleged that Cigna violated the "unlawful" prong by failing to comply with California Health & Safety Code § 1367.01(e), a specific statute requiring that medical necessity determinations be made by a licensed physician or licensed healthcare professional. The court granted in part and denied in part the defendants' motion to dismiss, allowing claims to proceed and granting leave to amend.
35. *Estate of Lokken v. UnitedHealth Group*, 765 F. Supp. 3d 835 (D. Minn. 2025). Allowing breach of contract claims to proceed where Medicare Advantage customers alleged that UnitedHealth used an AI program to determine post-acute care coverage amounts without regard to treating physicians' recommendations, despite plan language promising that clinical services staff and physicians make decisions on healthcare services.
36. S.B. 243, 2023–2024 Reg. Sess. (Cal. 2024).
37. The American Presidency Project, "Executive Order 14110—Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," October 30, 2023, https://www.presidency.ucsb.edu/documents/executive-order-14110-safe-secure-and-trustworthy-development-and-use-artificial.
38. The sweep included actions against DoNotPay Inc., which marketed itself as an "AI lawyer," as well as companies like Ascend Ecom Operations LLC, Ecommerce Empire Builders, Rytr LLC, and TheFBAMachine Inc. for promoting AI tools that enabled fake reviews or promised unrealistic business success; Federal Trade Commission, "FTC Announces Crackdown on Deceptive AI Claims and Schemes," news release, September 25, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes.
39. At the height of the scheme, during the Medicare Advantage open enrollment period between January 1, 2022, and March 31, 2022, Troy enrolled over 2,700 new Medicare Advantage members, many through automatic or batch enrollments. The company agreed to pay a $1,430,008 criminal penalty, cooperate with ongoing investigations, and implement enhanced compliance and internal controls; U.S. Department of Justice, Office of Public Affairs, "Troy Health, Inc. Enters Non-Prosecution Agreement and Admits to Fraudulently Enrolling Medicare Beneficiaries and Identity Theft," news release, August 20, 2025, https://www.justice.gov/opa/pr/troy-health-inc-enters-non-prosecution-agreement-and-admits-fraudulently-enrolling-medicare.
40. These efforts include the release of "America's AI Action Plan" in July 2025, which outlined deregulatory priorities for AI; and Congress's consideration of a provision in the "One Big Beautiful Bill" that would have broadly preempted state regulation of AI technologies for a 10-year period, though these provisions were ultimately removed following significant pushback from states.
41. The White House, "Ensuring a National Policy Framework for Artificial Intelligence," Executive Order 14,365, December 11, 2025, https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/.
42. Jamie E. Darch et al., "Trump Attempts to Preempt State AI Regulation Through Executive Order," Ropes & Gray, December 12, 2025, https://www.ropesgray.com/en/insights/alerts/2025/12/trump-attempts-to-preempt-state-ai-regulation-through-executive-order.
43. For example, in September 2025, the FTC issued orders under Section 6(b) of the FTC Act to seven companies—Alphabet Inc., Character Technologies Inc., Instagram LLC, Meta Platforms Inc., OpenAI OpCo LLC, Snap Inc., and X.AI Corp.—seeking information about their consumer-facing AI chatbots, focusing on safety measures, privacy practices, and data handling, particularly as they relate to children's privacy and safety; Federal Trade Commission, "FTC Launches Inquiry into AI Chatbots Acting as Companions," news release, September 11, 2025, https://www.ftc.gov/news-events/news/press-releases/2025/09/ftc-launches-inquiry-ai-chatbots-acting-companions.

## Takeaways

- State laws impacting use of AI in healthcare are proliferating, creating new enforcement pathways and regulatory risks for payers, providers, and developers.
- Enforcement authority varies by state, with penalties ranging from civil fines to license suspension, and in some cases, criminal liability.
- State AI laws impose additional regulatory oversight touchpoints that could trigger enforcement.
- Federal regulatory approaches to AI in healthcare are shifting, with future preemption battles likely between state and federal authorities.
- Healthcare entities must implement robust AI governance to ensure compliance with evolving state and federal AI regulatory frameworks.

# Stay ahead of risks impacting your managed care organization

## Managed Care Compliance Conference

January 25–26, 2027 • Phoenix, AZ

Make plans now to attend our annual conference devoted specifically to the key topics that impact compliance professionals in a managed care setting. Learn about emerging trends and best practices, network with peers and industry leaders, and come away with strategies that can help you maximize compliance program effectiveness.

**Past topics include:**

- Third-party marketing
- Navigating the CMS audit
- AI and Prior Authorization
- Social Determinants of Health
- Data security
- FCA enforcement
- Risk assessment & adjustment
- Managed care litigation landscape

**Learn more**

hcca-info.org/2027managedcare

HCCA Health Care Compliance Association