# Health Law Developments

*The Newsletter of the Health Law Section*
*State Bar of Georgia*
*Spring 2026*

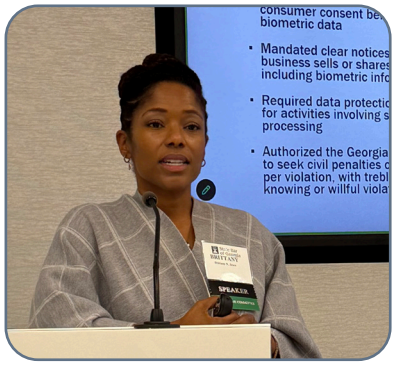
## From the Chair

Wade Pearson Miller

Thank you to everyone who attended our Annual Business Meeting and Lunch and Learn on May 14, 2026. We were pleased to hear from Brittany Jones of Kolibri Advisors, PC, who presented on biometric privacy law trends and developments; Scott Grubman of Grubman Warner Berry LLP, who provided a fraud and abuse enforcement update; and Gregory Tanner, Senior Associate at Baker Hostetler, who delivered an insightful presentation on hospital outpatient department and reimbursement regulatory updates. We also extend our sincere thanks to Baker Hostetler for hosting the event.

Congratulations to the newly elected officers of the Health Law Section for the 2026–2027 Bar Year:

*Brittany Jones*




**Chair**:
Brittany Jones

**Vice-Chair**:
Dawn Benson

**Treasurer**:
Scott Grubman

**Secretary**:
Lindsey Lonergan

It has been an honor and a privilege to serve as Chair of the Health Law Section over the past year. I would like to thank the Executive Committee for its dedication and hard work in making this such a successful year.

*Scott Grubman*

## Inside This Issue

# The Cost of Cost-Share: How Payors Leverage Patient Responsibility in SUD Audits

Tom Kelly, Arnall Golden Gregory LLP

One of the most common — and consequential — issues in payor audits of behavioral health and substance use disorder ("SUD") providers involves the collection of patient responsibility amounts: deductibles, copayments, and coinsurance. What may look like a billing formality often becomes the centerpiece of a payor's allegation that a provider engaged in "fee forgiveness," a label that can escalate into fraud investigations, corrective action plans, and multimillion-dollar recoupment demands.

Payors argue that collection of cost-sharing is not optional. These amounts are embedded in the member's plan design for both in-network and out-of-network arrangements and forgiving them effectively gives patients a benefit unavailable to other plan members. In the SUD context, this rule can feel especially harsh. Families seeking treatment are already stretched thin emotionally and financially, and providers often put access to care above aggressive collections. That tension, however, is exactly what payors exploit in audits, reframing compassion as noncompliance.

**From Audit to Recoupment**

An audit often begins with a comprehensive request for patient records — typically a "random" sample drawn from a defined timeframe. Payors usually demand treatment records, billing and collection ledgers, patient statements, and the provider's billing and collection policies. After reviewing these materials, the payor issues follow-up correspondence outlining its findings, often referred to as a "damages letter."

While the damages letter may highlight a range of compliance issues in the sample—such as documentation deficiencies, medical necessity, and patient care—the real showstopper almost always involves the provider's handling of cost-share obligations and balance billing. If the provider cannot demonstrate consistent efforts to pursue patient responsibility, the payor concludes that fee forgiveness occurred. That finding quickly escalates into allegations of fraud and justifies demands for repayment of not only the uncollected cost-share, but also *all claims paid during the audit period*.

The financial consequences of a fee forgiveness finding can be staggering. What begins as a narrow review of patient billing often morphs into a full-scale recoupment effort with exposure in the millions.

**In-Network vs. Out-of-Network Considerations**

Collection obligations can differ depending on whether a provider is in-network or out-of-network. In-network providers contractually agree both to collect patient responsibility amounts and to accept a negotiated rate for their services. This arrangement eliminates the need to issue balance bills, but it also creates a contractual obligation to make meaningful efforts to collect patient responsibility amounts. Providers should carefully review their network agreements to determine whether they contain specific requirements regarding cost-share collection practices.

Out-of-network providers, by contrast, often face heightened scrutiny of both cost-share collection and balance billing. In some cases, payors — or third-party administrators — will enter into single-case agreements that include provisions limiting balance billing. Importantly, these provisions do not relieve providers of their obligation to pursue cost-share amounts reflected on the remittance advice. Payors take the position that they would not enter such arrangements absent an expectation that the provider intends to hold the patient responsible for both the contracted rate and any applicable cost-sharing obligations.

**Defining "Commercially Viable" Efforts to Collect**

Providers frequently ask what efforts they must undertake prior to writing off balances as uncollectible. While contracts may include some specifics, this is often undefined. In one recent matter, a payor's investigator provided unusual clarity about what is considered acceptable. To avoid fee forgiveness findings, providers should engage in all "commercially viable" efforts to collect patient responsibility amounts, including:

- Bill patients for both the full treatment charges and the member's plan-based cost-share;
- Send multiple written statements (*at least* three), each reflecting the full

outstanding balance;

- Follow up with documented phone calls if payment is not received;
- Send a final written notice warning that the account may be referred to collections; and
- For larger balances, refer the account to collections if unpaid after thirty days.

Simply "checking the box" will not be enough to resolve these audits. Mailing statements without genuine follow-up—or continuing to provide services while accounts remain delinquent—suggests bad faith. At the same time, payors have acknowledged that providers are not expected to spend more on collection efforts than the balance justifies. What matters is showing a consistent, good-faith process aimed at enforcing the obligation.

**Balancing Compliance with Compassion**

For SUD providers, the challenge is to comply with payor expectations without abandoning compassion for families in crisis. Payment plans are one way to strike that balance. A family may not be able to cover a large coinsurance bill in a lump sum, but a signed installment agreement demonstrates that the obligation was not forgiven.

Documentation is equally important. Implementing written policies and procedures, and maintaining copies of billing statements, call logs, notes of payment-plan discussions, and final collection notices, together form the paper trail that can rebut allegations of systemic fee forgiveness. These practices may not prevent a payor from pursuing recoupment, but they change the narrative. Instead of appearing to ignore patient responsibility altogether, the provider can show it acted consistently, reasonably, and in good faith.

**When Audits Escalate into Arbitration and Litigation**

If an audit cannot be resolved informally, providers are often forced to litigate disputed amounts — particularly if claims have been pended during the review. Most network agreements include arbitration clauses, meaning in-network providers are typically required to arbitrate.

At this stage, fee forgiveness findings become even more dangerous. What begins as a billing dispute over patient responsibility often morphs into counterclaims for fraud, dramatically increasing both the financial and reputational stakes. The provider must not only defend its collection practices but also rebut allegations that it engaged in intentional misconduct. Here, documentation becomes the decisive factor. Providers who can demonstrate a clear pattern of billing full charges, pursuing cost-share, and offering commercially viable payment alternatives are far better positioned to argue that the dispute is contractual, not fraudulent.

**Conclusion**

The issue of collecting patient responsibility may seem technical, but for SUD providers it has become a flashpoint with life-or-death financial consequences. Payors frame failures to pursue cost-share as systemic fee forgiveness, audits escalate into recoupments, and unresolved disputes often spill into arbitration with fraud counterclaims attached.

Providers cannot eliminate these risks, but they can prepare for them. By implementing written policies and procedures and following consistent billing and collection practices, offering payment plans where appropriate, and documenting every effort to collect patient responsibility amounts, providers can demonstrate good faith and create evidence that will be invaluable if an audit escalates. In an environment where payors are always looking for opportunities to claw back money, those safeguards may make all the difference.

# Access Granted in Georgia: Avoiding Pitfalls in HIPAA's Most Common Compliance Failure

Kim Cunningham, Cunningham Law

**HIPAA Right of Access: Operational Compliance for Georgia Health Care Entities**

Ensuring patients can promptly access their own medical records remains the most enforced and deceptively challenging obligation under the Health Insurance Portability and Accountability Act (HIPAA). Since the Office for Civil Rights (OCR) launched its Right of Access Initiative in 2019, enforcement actions have made clear that failures are not theoretical. Delayed, incomplete, or improperly conditioned responses trigger patient complaints and six-figure settlements.

Georgia practitioners advising health systems, physician groups, and Health Information Management (HIM) teams must translate published OCR enforcement actions into practical, state-specific workflows that protect patient rights while managing risk. Covered entities often underestimate the operational complexity of fulfilling requests that span multiple systems, involve business associates, or require verification of a representative's authority.

Common failure points include missed thirty-day deadlines, partial productions, unlawful procedural barriers (such as requiring portal enrollment or unnecessary notarization), and improper fee practices. These recurring themes repeatedly result in substantial penalties.

Of the many failure points, few are more operationally fraught than correctly identifying who is legally authorized to receive records, a question that turns on state law rather than HIPAA. What follows addresses that state law foundation, the emerging complexity of patient-directed apps and Application Programming Interfaces (APIs), and the compliance strategies needed to hold it all together.

**Georgia Focus: Patient Representatives and State Law**

HIPAA defers to state law when determining who qualifies as a personal representative authorized to receive a patient's records. For example, HIPAA protects a deceased patient's Protected Health Information (PHI) for fifty years following the date of death to the same extent it protects a living patient's PHI but defers to state law on who may access a deceased patient's records during those fifty years. Under O.C.G.A. § 31-33-2, authority over a deceased patient's records flows first to an appointed executor or administrator. Where no fiduciary has been appointed, it passes to the surviving spouse, then to children, then to parents. Georgia also permits releases in specific circumstances, including but not limited to attorney requests accompanied by valid consent, court-ordered subpoenas, and bona fide emergencies.

These priorities differ from other states and must be embedded in local policies. A two-track workflow helps operationalize them:

1. Rapid verification track. A standardized, checklist-based review of representative authority that resolves straightforward requests the same day.
2. Escalation track. A designated privacy lead empowered to make same-day decisions on ambiguous cases, so that verification does not become a de facto denial or delay. This privacy lead might also have other resources for the most complex questions, such as an in-house attorney or outside counsel available for consultation.

When authority is reasonably documented, favor a good-faith release, document the decision, and remediate if an error is later identified. This approach reduces the risk of missing the thirty-day deadline and the OCR scrutiny that follows.

**Emerging Technology Pressures**

*Patient-directed apps and APIs*

When a patient invokes the Right of Access to direct ePHI to a third-party app, covered entities generally must comply and are not liable for the app's subsequent use of that data unless the app is itself a business associate of the provider (e.g., a patient portal like MyChart or a telehealth platform like Teladoc). Providers must document patient consent of risk when patients request unsecure transmission, such as unencrypted email. This is easy to say but difficult to put into practice. Be prepared to think through when the patient will be asked for that consent (first encounter, registration, as part of consent for treatment, etc.), how they will consent (checkbox, electronic

signature), the duration of the consent, and where the consent will be stored.

Compliance Strategies

1. Enterprise access policy with state-specific addenda. Draft a single access policy with an addendum for each state where the enterprise serves patients, specifying representative hierarchies, acceptable proof, and state-specific exceptions. Pro tip: include each state's breach notification rules in the same addendum; it will meaningfully improve your breach response when the time comes.

2. Map intake to fulfillment. Document every step, including but not limited to the request, identity verification, scope assessment, cross-department coordination, delivery method, and quality review. Incorporate internal turnaround targets shorter than HIPAA's deadlines and a clear escalation path for disputes by patients and representatives. Like whistleblowers, patients will often complain to the provider first. Ensure the provider receives, acknowledges, and resolves the complaint at this stage.

3. Strengthen business associate oversight. Embed service-level timelines, secure transfer requirements, and escalation clauses in business associate agreements. OCR holds covered entities accountable for business associate delays, so contractual remedies and proactive monitoring are essential.

4. Deliver scenario-based training on a recurring basis. Train front desk, HIM, clinical staff, Release of Information (ROI) vendors, and Information Technology (IT) using realistic vignettes like an unclear power of attorney, a next-of-kin request before probate closes, a patient-directed app transfer, and a disputed fee calculation. Resist the one-and-done approach by calendaring recurring sessions of increasing complexity.

5. Monitor and audit. Regular audits identify bottlenecks and create documentary evidence of good-faith compliance efforts, which matter enormously if OCR comes calling.

**Part 2 Records Update**

As of February 16, 2026, medical records maintained in connection with Part 2 programs[1] are subject to a HIPAA-style right of access to their substance use disorder treatment records. This is new. Providers receiving Part 2 records must incorporate this change into workflows and training so that SUD requests receive the same timeliness and documentation discipline as all other medical record requests. Enforcement priorities with respect to SUD records have been in flux, and practitioners who represent these providers are cautioned to remain alert to further guidance.

**Conclusion**

HIPAA's Right of Access remains the single most common compliance failure. That is not because the rules are ambiguous but because operational execution is genuinely hard across complex, multi-system environments.

For health care entities, the path to fewer complaints and lower enforcement risk is straightforward in concept and exacting in practice. The steps outlined here protect patient rights, reduce staff anxiety around breach, and demonstrate the good faith efforts OCR expects when access disputes arise.

1 42 U.S.C. § 290dd-2

# Closing the Ambulance Gap: Georgia's Latest Legislative Efforts to Address Surprise Billing

Douglas J. Witten, Innovative ADR International LLC

**Introduction**

In recent years, federal and state lawmakers have taken significant steps to address "surprise" medical billing. The federal No Surprises Act (NSA) and Georgia's Surprise Billing Consumer Protection Act established protections for insured patients receiving out-of-network care, limiting patient cost-sharing, prohibiting balance billing in defined circumstances, and creating mechanisms to resolve payment disputes between insurers and providers.

Yet one category remains outside these protections: ground ambulance transportation. Both the federal NSA and Georgia's statute exclude most ground ambulance services from their balance-billing provisions, leaving patients potentially exposed to significant out-of-network charges and leaving insurers and ambulance providers without a consistent statutory framework governing reimbursement disputes.[1]

During the 2026 legislative session, the Georgia General Assembly introduced two bills aimed at addressing this gap: House Bill 961 and Senate Bill 462. While neither bill passed in its original form, the General Assembly ultimately advanced the proposal through House Bill 506,[2] a retooled legislative vehicle incorporating SB 462's 325% Medicare reimbursement benchmark. As of this writing, the measure awaits gubernatorial action.

**Existing Statutory Framework**

Georgia's Surprise Billing Consumer Protection Act addresses unexpected out-of-network medical charges and generally prohibits balance billing when insured patients receive emergency services or certain non-emergency services from out-of-network providers at in-network facilities.[3]

In those circumstances, the law limits the patient's financial responsibility to in-network cost-sharing amounts and establishes a structured mechanism for resolving payment disputes between insurers and out-of-network providers. Under the Act, disputes regarding reimbursement may ultimately be resolved through the Act's independent arbitration process, in which each party submits a final proposed payment amount and a neutral arbitrator selects one of the competing offers after considering statutory and regulatory factors.

However, the statute expressly excludes ground ambulance transportation services from its balance-billing protections.[4] As a result, ambulance transports—often occurring in emergency circumstances where patients have little or no ability to choose their provider—remain one of the most visible gaps in current surprise-billing protections.

**The Legislative Solution: Passage of HB 506**

The bills introduced during the 2026 session sought to close this regulatory gap by extending certain consumer protections to emergency ground ambulance transportation.

Both HB 961 and SB 462 would have amended Code Section 33-20E-23 to require health plans to treat certain "emergency transport services" as covered services when the transport is requested by a first responder or healthcare practitioner responsible for the patient's care.[5] Under both proposals, patients receiving such services would have been responsible only for the copayment, coinsurance, or deductible applicable under their healthcare plan.

The legislation also would have established a hierarchical reimbursement structure governing payments to out-of-network ambulance providers. First, the minimum allowable reimbursement rate would have been the rate established by contract or through a local ordinance, resolution, rule, or regulation adopted by a county, municipality, special district, or other governmental authority within the jurisdiction where the service is provided.[6]

If no such local or contractual rate exists, the statutory benchmark would apply. Under HB 961, the fallback benchmark would have been 300 percent of the applicable Medicare ambulance reimbursement rate.[7] Under SB 462, the benchmark would have been the lesser of 325 percent of the applicable Medicare rate or the charges billed by the ambulance provider.[8]

Both bills also included procedural provisions governing insurer payments. Each proposal defined a "clean claim" and would have required payment within 30 days of receipt. If the insurer determined that a claim was not clean, the insurer would have been required to notify the ambulance provider within the same 30-day period and specify the reasons for denial or the

additional information required.[9]

As described in the Legislative Status section below, neither HB 961 nor SB 462 ultimately passed in the form described above. The ambulance billing reform that did cross the finish line—HB 506—carried the substantive framework of SB 462, including its 325% Medicare benchmark. HB 961's 300% Medicare rate did not survive the legislative process.

**Legislative Status**

Both bills advanced through their chambers of origin with overwhelming bipartisan support. On February 18, 2026, the Senate approved SB 462 by a vote of 51-1, and on March 4, 2026, the House passed HB 961 by a vote of 174-1.

Neither bill, however, completed the legislative process in its original form. Instead, during the closing days of the session, the General Assembly incorporated the substantive framework of SB 462 into HB 506, which passed both chambers on April 2, 2026 (Sine Die) and was sent to Governor Brian Kemp on April 10, 2026.

Under Georgia law, the Governor has 40 days following adjournment to act on legislation. If signed or allowed to become law, HB 506 would take effect January 1, 2027.

**Payment Benchmarks and Dispute Resolution**

From a dispute-resolution perspective, the proposed legislation illustrates an important policy shift in how healthcare reimbursement conflicts may be addressed.

Georgia's existing surprise-billing statute relies on independent arbitration to resolve payment disputes between insurers and out-of-network providers. The ambulance bills, by contrast, rely primarily on statutory reimbursement benchmarks tied to Medicare payment rates.

Benchmark frameworks may narrow disputes over reimbursement amounts by establishing predetermined reimbursement floors. At the same time, they often generate new categories of disagreements. Questions may arise regarding whether a transport qualifies as an "emergency transport service," whether a claim qualifies as a "clean claim," or whether a locally established reimbursement rate applies within a particular jurisdiction, an issue that may be dispositive under the statutory hierarchy.

Even in a benchmark system, such issues frequently require negotiation, mediation, or arbitration to resolve. In practice, reimbursement disputes often turn on fact-specific questions—such as claim classification, documentation sufficiency, or the applicability of local reimbursement provisions—that lend themselves to structured dispute-resolution processes.

For attorneys advising healthcare providers, insurers, and emergency medical service organizations, these proposals illustrate how evolving reimbursement frameworks can reshape, rather than eliminate, the need for effective dispute-resolution mechanisms.

**Looking Ahead**

The passage of HB 506 represents a significant, if procedurally unconventional, development in Georgia's surprise-billing framework. After years in which ground ambulance services remained a notable gap in consumer protections, the General Assembly acted to address that gap—though not through the two bills that initially defined the debate.

As HB 506 awaits gubernatorial action, the focus for practitioners shifts from legislative advocacy to implementation and interpretation. Healthcare attorneys, insurers, and emergency medical service organizations should begin reviewing existing contracts, local reimbursement arrangements, and claims-processing workflows in anticipation of the January 1, 2027, effective date.

Regardless of the precise framework ultimately adopted, the evolution of surprise-billing law ensures that reimbursement disputes—both procedural and substantive—will remain a central feature of the healthcare regulatory landscape.

---

1 See 42 U.S.C. § 300gg-111 et seq.; O.C.G.A. § 33-20E-23.
2 Ga. H.B. 506, 2025-2026 Reg. Sess. (Ga. 2026).
3 O.C.G.A. §§ 33-20E-1 to 33-20E-23.
4 O.C.G.A. § 33-20E-23.
5 Ga. H.B. 961 (Comm. Sub.), 2025-2026 Reg. Sess., § 1(b); Ga. S.B. 462 (as passed Senate), 2025-2026 Reg. Sess., § 1(b) (Ga. 2026).
6 Id. § 1(c)(1).
7 Ga. H.B. 961 (Comm. Sub.), 2025-2026 Reg. Sess., § 1(c)(2) (Ga. 2026).
8 Ga. S.B. 462 (as passed Senate), 2025-2026 Reg. Sess., § 1(c)(2) (Ga. 2026).
9 Id. § 1(f).

# Artificial Intelligence in U.S. Healthcare: Navigating the Uncertain Regulatory Landscape

Scott Robertson and Justin Chavez, Baker Hostetler

Artificial intelligence (AI) is reshaping healthcare at extraordinary speed, revolutionizing diagnostics, enhancing clinical decision-making, streamlining operations, and redefining how patients interact with providers. But as adoption accelerates, the rules governing AI remain amorphous, a patchwork of fast-changing, and often difficult to navigate regulations, guidance, and state laws. This article is a high-level overview of the current legal and regulatory landscape governing the use of AI in healthcare.

## FDA Regulation of AI as Medical Devices

U.S. Food and Drug Administration (FDA) regulations govern AI and machine learning technology when it functions as a medical device, including Software as a Medical Device. Software intended to diagnose, treat, mitigate, prevent disease, or affect the structure or function of the body could be considered a device,[1] which would be regulated according to FDA's three risk-based classifications, which determine the device's approval pathway.[2]

If considered a medical device, manufacturers must comply with general FDA device requirements, including software validation, risk management, documentation, and quality-system obligations, in addition to postmarket obligations, like adverse event reporting, registration and listing, device identification, and in some instances, cybersecurity related requirements and postmarket surveillance.[3]

While certain medical and decision support software is excluded from FDA oversight,[4] FDA may determine the device is not excluded from regulation if the use of the software could result in serious adverse health consequences. In August 2025, FDA sent a warning letter to SeniorLife Technologies for marketing its mobile app without the required premarket approval because it was intended for diagnostic use in screening mobility and cognitive health conditions, and not merely as measuring exercise equipment.[5]

## Privacy and Data Protection

The increasing use of AI in healthcare presents unique risks to health care data, which is inherently sensitive, due to the volume of data ingested by and potential uses in AI technology. Because HIPAA generally requires patient authorization for uses and disclosures of protected health information (PHI) that are not for treatment, payment, or health care operations, it is prudent to understand how an AI tool will be using or disclosing PHI, including for training AI tools, research, de-identification, or the sale of PHI.[6] Business associates, including vendors of AI software, are also directly regulated under HIPAA, and are subject to the same restrictions, and bound by the terms of the business associate agreements that govern their use of PHI. State privacy laws provide fragmented, and sometimes more restrictive regulation of health information via complex privacy laws[7] – some of which exempt entities covered by HIPAA– or legislation targeting how AI is used in certain sectors, requiring a review of applicable state laws to understand compliance obligations.

## Anti-Discrimination and Civil Rights

Section 1557 of the Affordable Care Act (ACA) prohibits discrimination in health programs receiving federal financial assistance.[8] In May 2024, HHS's Office for Civil Rights issued a final rule addressing the use of patient care decision-support tools, including AI-driven and algorithmic systems used in clinical decision-making, prohibiting covered entities from relying on these tools in a manner that results in discrimination based on race, color, national origin, sex, age, or disability, and it requires reasonable efforts to identify and

1 21 U.S.C. 321(h)(1).

2 21 U.S.C. 360c.

3 21 U.S.C. §§ 360, 360i, 360l, 360n-2 and 21 C.F.R. Part 820.

4 21 U.S.C. § 360j(o); see also General Wellness: Policy for Low Risk Devices, https://www.fda.gov/regulatory-information/search-fda-guidance-documents/general-wellness-policy-low-risk-devices.

5 Warning Letter, SeniorLife Technologies, Inc. (August 21, 2025), https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/seniorlife-technologies-inc-707021- 08212025.

6 Artificial Intelligence and Health Privacy, Shannon Britton Hartsfield, 70 Lol. L. Rev. For., https://loynolawreview.org/theforum/artificial-intelligence-and-health-privacy1442024.

7 Digital Diagnosis: Health Data Privacy in the U.S., Gabriela Rios, Stanford Law School, Law and Biosciences, Blog (Feb. 26, 2025), https://law.stanford.edu/2025/02/26/digital-diagnosis-health-data-privacy-in-the-u-s/.

8 45 C.F.R. pt. 92.

mitigate such risks.[9]

Title VI of the Civil Rights Act and the Federal Trade Commission (FTC) enforcement against unfair or deceptive practices also provide additional anti-discrimination and consumer protection backstops.[10] The FTC previously asserted such authority in its settlement with Rite Aid Corporation (Rite Aid) after it found that Rite Aid failed to implement reasonable procedures to prevent harm to consumers while using facial recognition technology.[11] At the state level, Colorado laws impose duties to prevent algorithmic discrimination and require risk management practices for both developers and deployers of AI systems making consequential decisions about healthcare access.[12] California laws require disclosure when generative AI is used in clinical communications and prohibit health insurers from denying coverage solely based on AI-driven decisions without meaningful human oversight.[13] However, although a number of states have enacted or proposed laws aimed at regulating AI, these measures have been accompanied by little, if any, authoritative guidance or enforcement.

## Federal Executive Orders and Agency Guidance

Recent executive orders have directed federal agencies to develop AI governance strategies, promote trustworthy AI, and address privacy, and safety in healthcare AI. The Biden administration's Executive Order 14110 (rescinded but still influential) and Trump administration orders have shaped agency priorities, including HHS' development of an AI Task Force.[14] The National Institute of Standards and Technology (NIST) published a voluntary AI Risk Management Framework (AI RMF), widely referenced as a best practices for the use of AI.

Congress is considering bills that would require impact assessments for high-risk AI systems, mandate transparency, and address algorithmic bias, but no comprehensive federal AI law has been enacted. These executive actions and agency initiatives are shaping both current compliance obligations and the likely direction of future standards for oversight of AI.[15]

## ASTP/ONC Health IT Certification and Transparency

The Assistant Secretary for Technology Policy/Office of the National Coordinator for Health Information Technology's (ASTP/ONC) "HTI-1 Rule"[16] updated Certification Program criteria to require transparency for AI in predictive algorithms offered as part of certified health technology, including that developers implement risk management practices and make publicly available summary information about these practices, and models or algorithms, related designs, tests, and evaluations. However, ASTP/ONC recently proposed its "HTI-5 Rule"[17] which, if finalized, would remove these transparency requirements regarding predictive algorithms in an effort to reduce regulatory burdens and encourage AI innovation. A review of the finalized HTI-5 rule is crucial for stakeholders to understand their compliance obligations with regards to AI transparency.

## Conclusion

Without comprehensive federal AI law regulations, health care industry stakeholders are forced to navigate a legal environment characterized by a mix of federal regulations, industry guidance, and a rapidly expanding array of state statutes. As the legal framework develops, stakeholders must remain adaptable amid a shifting landscape, while adopting a robust governance framework, and monitoring legal developments to ensure compliance.

9 *Nondiscrimination in Health Programs and Activities,* 89 Fed. Reg. 37542-51 (May 6, 2024).

10 42 U.S.C. § 2000d et seq.; 15 U.S.C. § 45(a)

11 FTC, Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology Without Reasonable Safeguards, Resulting in Harm to Consumers, Fed. Trade Comm'n (Dec. 19, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without; FTC, FTC Announces Crackdown on Deceptive AI Claims and Schemes (Sept. 25, 2024).

12 Colo. Rev. Stat. § 6-1-1701 et seq.

13 Cal. Health & Safety Code §1339.75; Cal. Health & Safety Code § 1367.01; Cal. Ins. Code § 10123.135; Cal. Code Regs. tit. 10, § 2562.09.

14 Exec. Order No. 14,110, 88 Fed. Reg. 75,191 (Oct. 30, 2023); Exec. Order No. 14,179, 90 Fed. Reg. 8,741 (Jan. 23, 2025); 15 U.S.C. § 9401.

15 NIST, AI Risk Management Framework, Nat'l Inst. of Standards & Tech. (Jan. 2023)

16 Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing, 89 Fed. Reg. 1192 (Jan. 9, 2024).

17 Health Data, Technology, and Interoperability: ASTP/ONC Deregulatory Actions To Unleash Prosperity, 90 Fed. Reg. 60970 (Dec. 29, 2025).

# AI, Automation, and Medical Necessity: Are Algorithms Driving the Next Wave of Payor-Provider Litigation?

Rachel Leff Blumberg, Senior Associate, Alston & Bird LLP

## Introduction

Commercial payors, Medicare Advantage plans, and third party administrators increasingly rely on machine learning and automated or semi-automated tools, including algorithms, to conduct utilization management. These machine-learning or algorithmic systems are designed to process high claim volumes efficiently and to control administrative and medical costs, but they are also drawing heightened scrutiny from regulators and courts.[1]

Legislatures and agencies have begun focusing on how these technologies interact with long-standing medical necessity requirements, clinician review obligations, and contractual promises to providers and members.[2] For example, CMS's recent guidance in the context of Medicare Advantage emphasizes that while algorithms may assist in utilization management, they cannot replace individualized medical necessity determinations grounded in Medicare coverage criteria and patient-specific facts.[3]

As payors increasingly integrate algorithmic systems into claims processing and prior authorization, litigation risk tied to transparency, fairness, and contractual authority has accelerated. The next generation of payor-provider disputes is therefore likely to focus not only on coverage outcomes, but on the decision-making processes that produced them.

## Legal Risk When AI Tools Are Used to Deny or Adjust Healthcare Claims

Automation in utilization management encompasses a range of tools operating at different stages of the claims lifecycle. Some systems apply rule-based edits that automatically adjust or deny claims based on internal policies; others rely on predictive models to identify outlier claims, services deemed low value, or cases requiring additional scrutiny.[4] Algorithmic prior authorization platforms may triage requests and evaluate documentation, while retrospective auditing tools flag paid claims for post-payment review and potential recoupment.[5] Each of these technologies can be deployed as a support mechanism, but legal risk increases as automation moves closer to the final determination of medical necessity.

A central pressure point is the delegation of medical necessity decisions. Disputes arise from allegations that payors have effectively outsourced medical judgment to vendor-developed systems or implemented workflows in which clinicians play only a nominal role.[6] Federal oversight

1 National Ass'n of Ins. Comm'rs, *Health Insurance Artificial Intelligence/Machine Learning Survey Results* (2025), https://content.naic.org/sites/default/files/inline-files/NAIC%20AI%20Health%20Survey%20Report%20.pdf (finding that 84% of ninety-three large health insurers surveyed used AI for operational functions).

2 Cong. Rsch. Serv., *Artificial Intelligence (AI) in Health Care*, R48319 (Dec. 30, 2024), https://www.congress.gov/\crs-product/R48319; Nat'l Conf. of State Legislatures, *Artificial Intelligence 2025 Legislation* (last updated July 10, 2025), https://www.ncsl.org/technology-and-communication/artificial-intelligence-2025-legislation; Staff of S. Permanent Subcomm. on Investigations, *Refusal of Recovery: How Medicare Advantage Insurers Have Denied Patients Access to Post-Acute Care* (Oct. 17, 2024), https://www.hsgac.senate.gov/wp-content/uploads/2024.10.17-PSI-Majority-Staff-Report-on-Medicare-Advantage.pdf; Nat'l Health Law Program, *Federal AI Policy Threatens Prior Authorization Reform*, https://healthlaw.org/federal-ai-policy-threatens-prior-authorization-reform/; Ctrs. for Medicare & Medicaid Servs., CMS Artificial Intelligence (AI) Resources, https://ai.cms.gov/ (last visited Mar. 20, 2026).

3 Ctrs. for Medicare & Medicaid Servs., *Medicare Advantage Final Rule (2024): Frequently Asked Questions* (Feb. 6, 2024) ("An algorithm or software tool can be used to assist MA plans in ' making coverage determinations, but it is the responsibility of the MA organization to ensure that the algorithm or artificial intelligence complies with all applicable rules for how coverage determinations by MA organizations are made.").

4 *See, e.g.*, HealthEdge, *How Can AI-Powered DRG Editing Improve Claims Accuracy?* (Jan. 15, 2026), https://healthedge.com/resources/blog/src-how-can-ai-powered-drg-editing-improve-claims-accuracy; Optum, Claims Edit System (Healthcare Operations: Payment Integrity), https://business.optum.com/en/operations-technology/payment-integrity/claim-editing.html; Lewis & Ellis, Inc., *Health Insurance Predictive Modeling* (Oct. 28, 2022), https://lewisellis.com/industries/health-care-health-insurance/health-insurance-predictive-modeling/.

5 Notable Health, *Getting Started with Prior Authorization Automation* (May 22, 2025), https://www.notablehealth.com/blog/getting-started-with-prior-authorization-automation; Mizzeto, *SmartAuth: AI-Powered Prior Authorization Automation for Health Plans*, https://www.mizzeto.com/smart-auth.

6 *See, e.g.*, *Kisting-Leung v. Cigna Corp.*, No. 3:23-cv-00654 (E.D. Cal. Filed July 24, 2023); *Barrows, v. Humana, Inc.*, No. 3:23-cv-00654 (W.D. Ky. filed Dec. 12, 2023); *Lokken v. UnitedHealth Group, Inc.*, No. 0:23-cv-03514, (D. Minn. filed Nov. 14, 2023).

bodies have raised concerns about inappropriate denials stemming from the application of undisclosed criteria, excessive documentation demands, or system-driven errors. [7] Litigation challenging algorithmic denials often reframes the dispute away from clinical disagreement and toward procedural compliance, arguing that the process itself violates plan documents, provider agreements, or governing law.[8] These claims are commonly framed as breach of contract claims, breaches of the implied covenant of good faith and fair dealing, statutory violations, and, in some cases, consumer protection or bad faith insurance theories—each premised on the assertion that the decision making architecture failed to deliver the physician led review and fair process promised to beneficiaries and providers. [9]

Recent cases illustrate this trend. Plaintiffs have alleged that algorithmic tools were used to generate large volumes of denials with minimal individualized review, contrary to plan language requiring determinations by licensed medical professionals.[10] Courts evaluating these claims have shown increasing willingness to scrutinize whether clinician involvement was meaningful or merely superficial, and whether algorithmic, semi-automated, or machine-learning systems operated within the bounds promised in contracts and required by statute. [11]

## Discovery Fights Over Algorithmic Decision-Making

Once claims challenging algorithm-driven denials survive the pleading stage, discovery frequently becomes the focal point of the litigation. Providers and members increasingly seek information beyond the individual claim file, including documentation explaining how algorithmic or machine-learning tools functioned at the time of the denial. Requested materials often include model documentation, decision logic, version histories, audit logs, and records reflecting human overrides or approvals. For example, in Lokken v. UnitedHealth Group, Inc., the court compelled broad discovery into the insurer's use of an AI-based post-acute care tool, requiring production of materials concerning the tool's design, deployment, oversight, incentives, and interaction with clinician review—well beyond the confines of the named plaintiffs' claim files.[12]

Providers may contend that, absent transparency into the decision making process, they are unable to meaningfully test the rationale for a denial or identify potential systemic errors. Payors, in turn, may assert confidentiality and trade secret objections, arguing that proprietary algorithms or source materials need not be disclosed where they maintain that clinicians ultimately reviewed the determinations. In resolving such disputes, courts may be called upon to balance these competing interests, in some instances permitting some discovery while still imposing protective measures

7 Office of Inspector Gen., U.S. Dep't of Health & Human Servs., *Some Medicare Advantage Organization Denials of Prior Authorization Requests Raise Concerns About Beneficiary Access to Medically Necessary Care*, OEI-09-18-00260 (Apr. 2022), https://oig.hhs.gov/documents/evaluation/3150/OEI-09-18-00260-Complete%20Report.pdf.

8 *Lokken,* No. 23-cv-3514, 2026 WL 658883, at *1, 4 (D. Minn. Mar. 9, 2026) (holding that claims challenging allegedly algorithmic denials turned on whether the insurer's use of AI complied with evidence of coverage terms requiring physician-made determinations, rather than on individualized medical judgment); *Kisting-Leung v. Cigna Corp*., 780 F. Supp. 3d 985, 995–96 (E.D. Cal. 2025) (alleging that defendants wrongfully denied medically necessary benefit claims pursuant to an algorithmic system (PxDx), despite plan language promising coverage determinations by medical directors, and reframing the dispute as a failure of the claims-review process itself, rather than a clinical disagreement, based on defendants' alleged lack of physician involvement and noncompliance with plan requirements).

9 *Kisting-Leung*, 780 F. Supp. 3d at 995 (discussing the plaintiffs' ERISA and state-law claims for wrongful denial of benefits and breach of plan obligations, including the plaintiffs' allegations that defendants failed to provide the physician-directed medical necessity review promised in coverage documents by instead relying on an automated algorithm); *Barrows*, No. 3:23-cv-00654, Dkt. No. 37 at 234-48 (bringing claims for breach of contract; breach of the implied covenant of good faith and fair dealing; unjust enrichment; violations of state unfair-claims-settlement and unfair-competition statutes; insurance bad faith; unfair and deceptive insurance practices; and common-law fraud, and seeking compensatory, consequential, statutory, and punitive damages; restitution and disgorgement; attorneys' fees and costs; prejudgment interest; emotional-distress damages; and declaratory and injunctive relief enjoining defendants' claim-handling practices).

10 *Kisting-Leung*, 780 F. Supp. 3d at 995 (discussing the plaintiffs' allegations that the defendants relied on an algorithm to enable physicians to batch-deny hundreds of thousands of claims automatically based on preset criteria, with doctors spending an average of 1.2 seconds per claim and often not reviewing patient files, and asserting that this process generated large volumes of denials with minimal individualized review, contrary to plan language requiring determinations by licensed medical professionals).

11 *See Lokkien*, 2026 WL 658883, at *4.

12 *See id.* ("This Court agrees that Plaintiffs are entitled to discovery of documents regarding how nH Predict works, its development goals and anticipated benefit, and whether it was designed to supplant physician decision-making. This includes not only documents and communications regarding nH Predict's development, design, creation, approval, implementation, and use, but also the identities of the individuals involved in nH Predict's development, design, creation, implementation, and approval.").

to address relevancy concerns.[13] As algorithmic systems become more central to utilization management, discovery disputes resembling those in intellectual property litigation may become more common in healthcare reimbursement cases.

### Contract Language and Compliance Considerations

For payors, managing litigation risk associated with automation begins with clear contract drafting. Provider agreements and plan documents should expressly address the use of algorithmic or machine-learning tools, define the hierarchy of medical necessity criteria, and clearly describe dispute-resolution processes. Equally important are documented workflows that preserve meaningful clinician involvement where required by law or contract, and internal auditing mechanisms designed to identify bias or systemic error in algorithmic or machine-learning systems.

Providers, meanwhile, are increasingly focused on negotiating contractual protections that limit or condition the use of automation. These may include requirements for licensed clinician review of adverse determinations, advance notice of changes to utilization management tools or criteria, and access to the standards applied in algorithmic or machine-learning decisions. Some providers also seek remedies tied to systemic automation-driven underpayment, such as audit rights, corrective action obligations, or fee-shifting provisions.

### Conclusion

Automation, algorithms, and artificial intelligence are now embedded in utilization management, driven by scale, efficiency, and cost pressures. For healthcare lawyers advising payors and providers, the critical question is no longer whether algorithmic tools may be used, but how they are implemented, documented, and defended.

As litigation increasingly focuses on process rather than outcome, organizations should assume that algorithmic or machine learning systems will be examined as evidentiary mechanisms as much as operational ones. In that context, disputes involving automated decision making may increasingly turn on whether parties can demonstrate transparent processes, compliance with contractual and regulatory requirements, and meaningful human oversight, all factors that are likely to shape future legislative approaches to the use of these tools.

13 *Id.* (permitting discovery into how the disputed artificial intelligence program "works," including its design, creation, approval, implementation and use, but not requiring discovery into the artificial intelligence program's "data, rules, source code, and medical guidelines").

# Managed Care Fraud Enforcement: The New Frontier Has Arrived

Scott R. Grubman, Grubman Warner Berry LLP

When the Department of Justice (DOJ) released its annual False Claims Act (FCA) statistics for fiscal year 2025, announcing that it had recovered a record-breaking $5.7 billion in healthcare-related settlements and judgments, it highlighted an area of healthcare fraud enforcement that has quickly emerged as the one of the government's top priorities: managed care fraud and, in particular, fraud affecting the Medicare Advantage (or Part C) program.[1] The government's focus on managed care fraud makes sense, considering that, as noted in the DOJ's January 2026 press release, "Medicare Part C is now the largest component of Medicare, both in terms of federal dollars spent and the number of beneficiaries impacted."

The DOJ has since made clear that it is not backing off of this priority in 2026. Barely two weeks into the new year, the DOJ announced that Kaiser Permanente affiliates had agreed to pay $556 million to resolve allegations that they violated the FCA by "submitting invalid diagnosis codes for their Medicare Advantage Plan enrollees in order to receive higher payments from the government.[2] Less than two months later, the DOJ announced that another large Medicare Advantage Organization, Aetna, had agreed to pay over $117 million to resolve similar allegations. [3]

**What is Medicare Advantage?**

The Medicare Advantage (MA) Program–also known as Medicare Part C–allows Medicare beneficiaries to opt out of traditional Medicare and enroll in a health plan administered by a private company, known as a Medicare Advantage Organization (MAO). Unlike the traditional fee-for-service payment model, the Centers for Medicare & Medicaid Services (CMS) pays MAOs a fixed amount per enrollee and adjusts that payment using diagnosis codes that are submitted by the MAO, generally paying more for sicker beneficiaries expected to incur higher costs. CMS's Managed Care Manual[4] requires that diagnoses used for risk adjustment be documented in the medical record and result from a face-to-face visit.

**Risk Adjustment Data Manipulation**

The most common alleged fraud scheme affecting MA plans is risk adjustment data manipulation. In the January 2026 Kaiser settlement, for example, the government alleged that Kaiser engaged in a scheme "to improperly increase its risk adjustment payments" by pressuring "its physicians to alter medical records after patient visits to add diagnoses that the physicians had not considered or addressed at those visits." Specifically, the DOJ alleged that Kaiser "developed various mechanisms to mine a patient's past medical history to identify potential diagnoses that had not been submitted to CMS for risk adjustment" and then would send "queries" to its providers "urging them to add these diagnoses to medical records via addenda, often months and sometimes over a year after visits." The government also alleged that Kaiser set "aggressive physician- and facility-specific goals for adding risk adjustment diagnoses."

The March 2026 Aetna settlement contained similar allegations of risk adjustment data manipulation. Specifically, the government alleged that Aetna operated a "chart review program in which it paid diagnosis coders to review medical records . . . and identify all medical conditions that the charts supported." Aetna would then rely on the results of those reviews to submit additional diagnoses codes to CMS, thereby increasing its reimbursement. The government also alleged that although Aetna's chart reviews did not substantiate some of its previously reported diagnoses codes, Aetna "did not delete or withdraw those diagnoses codes, which would have required Aetna to reimburse CMS."

In addition to MA plans themselves, providers that submit diagnosis codes to such plans are also on the hook for potential FCA liability, as the FCA prohibits not only directly submitting a false claim or statement to a federal healthcare program, but also causing such a submission. See 31 U.S.C. § 3729(a)(1)(A). In March 2025, for example, Medicare Advantage provider Seoul Medical Group, along with related entities and its former owner Dr. Min

1 https://www.justice.gov/opa/media/1424126/dl

2 https://www.justice.gov/opa/pr/kaiser-permanente-affiliates-pay-556m-resolve-false-claims-act-allegations.

3 https://www.justice.gov/opa/pr/aetna-agrees-pay-1177-million-resolve-false-claims-act-allegations.

4 https://www.cms.gov/regulations-and-guidance/guidance/manuals/downloads/mc86c07.pdf.

Young Cha, agreed to pay a combined $60 million to resolve allegations that they violated the FCA by "causing the submission of false diagnoses codes for two spinal conditions to increase payments from the Medicare Advantage program."[5] According to the DOJ, for a six year period, Seoul Medical Group and Dr. Cha submitted diagnoses for spinal enthesopathy and sacroiliitis for patients who did not suffer from these conditions. "When Seoul Medical Group was questioned by an MA Plan about its use of spinal enthesopathy, [Seoul] enlisted the assistance of Renaissance Imaging Medical Associates to create radiology reports that appeared to support" the diagnosis, resulting in increased payments to Seoul. For its part, Renaissance agreed to pay an additional $2.35 million.

### Kickbacks Affecting MA Plans

In addition to allegations of risk adjustment data manipulation, the government is also actively pursuing cases involving allegations of kickbacks. In May 2025, for example, the DOJ intervened in an FCA qui tam case against Aetna, Elevance Health (formerly known as Anthem), and Humana, along with several large insurance broker organizations, alleging that the defendant insurers "paid hundreds of millions of dollars in illegal kickbacks to the defendant brokers in exchange for enrollments into the insurers' Medicare Advantage plans."[6] According to the government's press release, "rather than acting as unbiased stewards, the defendant brokers allegedly directed Medicare beneficiaries to the plans offered by insurers that paid brokers the most in kickbacks, regardless of the suitability of the MA plans for the beneficiaries."[7] In March 2026, the district court denied the defendants' motions to dismiss, moving the case towards discovery. [8]

### Conclusion

As with so many areas of FCA fraud enforcement, "success breeds success." As Medicare Part C spending continues to increase, and as the DOJ continues to obtain massive recoveries in managed care FCA matters, it is certain that private whistleblowers and their counsel will take note, likely resulting in even more MA-related qui tam complaints being filed moving forward. Accordingly, MA Plans and providers must continue to develop and implement strong policies and procedures to ensure compliance with Medicare Advantage rules and regulations before they become the subject of the government's next press release.

5 https://www.justice.gov/opa/pr/medicare-advantage-provider-seoul-medical-group-and-related-parties-pay-over-62m-settle.

6 https://www.justice.gov/opa/media/1398796/dl.

7 https://www.justice.gov/opa/pr/united-states-files-false-claims-act-complaint-against-three-national-health-insurance.

8 https://litigationtracker.law.georgetown.edu/wp-content/uploads/2025/05/United-States-et-al-v.-eHealth-Inc.-et-al-Docket-No.-1_21-cv-11777-D.-Mass.-Nov-02-2021-Court-Docket-3.pdf.