Stay Current

PAUL HASTINGS

September 2026

Follow us on LinkedIn

Regulatory Update

Healthcare Enforcement Q3 Highlights: What Providers Need to Know

By Jane H. Yoon, Dhara Satija, Jessica Montes, Hari Pillai, Jeni Griffin, Anita Hanlon and Tully Saunders

In the third quarter of 2026, U.S. federal agencies continued to advance the administration's healthcare fraud enforcement and prevention priorities. This reflects sustained regulatory scrutiny of fraud, waste and abuse, as well as increasing use of data analytics and artificial intelligence to identify potential fraud and strengthen healthcare program integrity.

Here is a summary of key activities from the third quarter:

- **Federal enforcement is increasingly data-driven and centralized**. DOJ launched the National Fraud Detection Center, issued the McDonald memorandum outlining Fraud Division priorities and is developing AI-enabled anomaly detection across Medicare and Medicaid claims data, all signaling that providers should ensure their own compliance programs leverage data analytics to identify risks proactively.

- **DOJ revised the Justice Manual to clarify which False Claims Act cases to pursue and to instruct prosecutors to continually assess whether *qui tam* actions should be dismissed for lack of factual or legal merit or failure to advance the interests of the United States**. The revisions provide that enforcement should be based on violations of legally binding rules, not sub-regulatory guidance (e.g., agency FAQs, internal memos or training materials), and prosecutors should continue to assess, after declining to intervene, whether *qui tam* actions lack factual or legal merit, or otherwise fail to advance the interests of the United States, and move to dismiss such cases to ensure resources are dedicated to meritorious investigations.

- **DOJ secured significant healthcare fraud recoveries, with *qui tam* relators playing a key role**. Civil settlements this quarter ranged from $2.4 million to $541.5 million across laboratories, eye care and Medicare Advantage.

- **DOJ is using RICO to prosecute healthcare fraud with aggravating factors**. The Southern District of New York (SDNY) indictment of a Bronx-based organization for Medicaid fraud, charged under RICO alongside healthcare fraud and Anti-Kickback Statute (AKS) violations, signals a willingness to layer racketeering charges onto schemes involving kickbacks, multi-entity collusion or intimidation.

- **HHS-OIG issued three unfavorable advisory opinions on arrangements with software vendors that are designed to facilitate the referral or ordering of federally reimbursable items and services**. While software platforms may be marketed and designed to bolster efficiency in a strained healthcare delivery system, these opinions stand as a warning to software sellers and subscribers that HHS-OIG is concerned by the anticompetitive, steering and kickback risks associated with certain software arrangements.

- **HHS-OIG's updated Corporate Integrity Agreement (CIA) template sets a new compliance benchmark**. Key additions include independent board member requirements, a prescribed risk assessment methodology and the first-ever CIA provisions addressing generative AI disclosure and verification in compliance activities.

- **CMS is achieving record program integrity results through prepayment interdiction**. Using AI and large-scale data analytics, CMS is focusing on fraud prevention with over 1,000 hospices removed and more than $1 billion in Medicaid payments deferred.

- **Privacy, cybersecurity and data governance obligations continue to expand**. Four new state privacy laws went into effect, underscoring the need for proactive data governance and preparedness for investigative demands.

- **Massachusetts Sen. Elizabeth Warren introduced the Stop Corporate Takeovers of Physicians Act** to prohibit private equity, insurers and other for-profit corporate entities from owning and controlling physician practices. Announced on Sept. 16, the proposed legislation would establish a national ban on the corporate practice of medicine, including preventing management service organizations (MSOs) from controlling practices. Hospitals and nonprofit providers would remain exempt.

- **Federal crackdown on ACA enrollment fraud**. On Sept. 22, the Trump administration announced that CMS had canceled Affordable Care Act (ACA) coverage for approximately 750,000 individuals, citing suspected fraudulent or improper enrollments. The administration also announced a six-month suspension of new ACA broker registrations. These actions are another example of federal scrutiny of healthcare program integrity and may cause coverage disruptions, increased uncompensated care and reimbursement risks for hospitals and healthcare providers, underscoring the importance of timely insurance eligibility verification.

Healthcare providers should respond by taking a targeted, risk-based approach to compliance, with greater emphasis on pre-claim submission reviews and the use of data to identify potential issues in coding and billing practices. Although regulatory risk cannot be eliminated, organizations can mitigate that risk through proactive monitoring, targeted risk assessments, effective internal controls, and timely investigation and remediation of identified issues. Providers should also consider responsible use of AI to enhance compliance capabilities, while maintaining appropriate accountability for its use. These developments, explained in detail below, reinforce the need for healthcare organizations to maintain compliance programs that are responsive to evolving regulatory priorities and approaches, capable of identifying and addressing potential risks before they result in enforcement exposure.

Enforcement

DOJ Fraud Enforcement Involving Providers

In the third quarter of 2026, DOJ secured civil settlements and resolutions ranging from $2.4 million to $541.5 million against laboratory, eye care and Medicare Advantage providers. Below is an overview of actions in these areas. Notably, *qui tam* relators remained a critical enforcement catalyst, and a federal appellate decision recently confirmed their constitutionality. On Sept. 1, a unanimous 11th Circuit panel held in *United States ex rel. Zafirov v. Florida Medical Associates* that the False Claims Act (FCA)'s *qui tam* provisions do not violate the Appointments Clause — reversing a closely watched District Court ruling that had threatened to curtail private whistleblower suits. The DOJ also issued its first healthcare fraud declination under the new Corporate Enforcement and Voluntary Self-Disclosure Policy, which can provide a roadmap for providers weighing voluntary self-disclosure. Providers would be well served to invest in a proactive compliance infrastructure, conduct regular internal audits of billing and coding practices, and establish clear self-disclosure protocols.

- **Laboratories and Diagnostics**. DOJ secured multiple resolutions with laboratories, diagnostic companies and related individuals alleged to have engaged in kickback schemes or submitted false claims for medically unnecessary testing. In one notable action, a national laboratory company accepted responsibility for and agreed to pay $14.5 million to resolve allegations that it billed Medicare for medically unnecessary urine drug testing. Separately, a skin cancer testing company agreed to pay up to $5 million to resolve allegations under the FCA's *qui tam* provisions for knowingly submitting false claims to Medicare for unreliable diagnostic tests. In a parallel civil and criminal action, a Florida-based genetic testing company and its former CEO agreed to pay a combined $36.4 million to resolve allegations that they funneled kickbacks to marketers in exchange for patient referrals, resulting in the submission of false claims to Medicare and Medicaid for medically unnecessary genetic tests. In connection with the settlement, the company entered into a five-year CIA with HHS-OIG, and the CEO pleaded guilty to conspiracy to defraud the United States. An Arkansas-based laboratory company and its former owners also agreed to pay $30 million and enter into a CIA to resolve allegations that they provided unlawful kickbacks and ordered medically unnecessary testing services. Relatedly, at the agency level, on Aug. 28, CMS announced that it has prevented more than $1.6 billion in fraudulent Medicare laboratory payments since the start of the Trump administration — revoking 157 fraudulent lab providers from Medicare and deploying AI-driven analytics to flag suspicious billing patterns before payments are released.

- **Eye Care**. The eye care sector also drew multiple DOJ settlements this quarter. For instance, a Massachusetts ophthalmology practice paid approximately $3.9 million to resolve FCA allegations that it falsely billed federal healthcare programs for office visits using an elevated billing code without performing the services to justify the higher reimbursement. Two additional ophthalmology practices paid a combined $2.3 million to settle allegations that they submitted fraudulent claims for cranial ultrasounds through a kickback arrangement with a third-party testing company, and a Florida ophthalmology practice and its physician owner paid $350,000 to resolve allegations that they submitted false claims for transcranial doppler tests through a kickback arrangement with an independent diagnostics company. Notably, the DOJ also announced its first declination under the new Corporate Enforcement Policy to a New Jersey-based management services organization for an optometry practice and ambulatory surgical center. The underlying misconduct concerned allegedly unnecessary diagnostic eye tests and kickbacks to ophthalmologists disguised as "consulting fees." In declining to prosecute, the DOJ emphasized the practice's voluntary self-disclosure, full cooperation with the investigation and timely remediation. Separately, the DOJ prosecuted the founder of the optometry practice and ambulatory surgical center for his role in the schemes.

- **Medicare Advantage**. The DOJ also resolved numerous FCA civil investigations against provider groups and management services organizations for submitting false diagnosis codes to inflate payments from the Medicare Advantage program. In one of the largest Medicare Advantage fraud recoveries to date, a Florida-based healthcare provider group agreed to pay $541.5 million to resolve self-disclosed allegations that it caused the submission of false diagnosis codes designed to inflate risk adjustment scores and increase capitated payments. Two additional settlements, both arising from FCA *qui tam* actions, addressed similar schemes in which provider organizations directed physicians to add unsubstantiated diagnosis codes. Specifically, a Florida-based management services organization that manages, owns or otherwise operates provider groups agreed to pay $14.1 million to resolve allegations that it prompted physicians to add clinically unjustified diagnosis, and a Tennessee-based chronic in-home care provider paid $2.4 million to settle allegations that it submitted diagnosis codes that were neither clinically accurate nor supported by documentation.

DOJ Initiatives and Organizational Changes

Amidst continued healthcare enforcement activity, the third quarter of 2026 included several key DOJ organizational shifts. On Aug. 8, the Senate confirmed the attorney general appointment of Todd Blanche, who as acting attorney general directed the creation of the National Fraud Enforcement Division in April. Shortly thereafter, on Aug. 13, Assistant Attorney General Colin M. McDonald issued a memorandum outlining the Fraud Division's enforcement priorities across five areas: (1) public trust and financial integrity; (2) healthcare; (3) internal revenue; (4) global trade and commerce; and (5) corporate misconduct.

The McDonald memorandum identifies substantive priorities — with healthcare as a centerpiece of the division's mandate — and details how the division intends to pursue cases. The memo states that the Fraud Division is "building the most sophisticated, innovative, and data-driven white-collar law enforcement component in the world," with prosecutors supported by a "cross-disciplinary team of experts in data science, and cutting-edge technology and resources." This builds on the Health Care Fraud Section's longstanding use of advanced data analytics to generate cases — an approach that has already yielded significant results, including a recent $45 million Medicare fraud conviction that originated from the Section's Data Analytics Team flagging a physician as an extreme outlier in Medicare payments. On Aug. 24, DOJ further operationalized its data-driven approach by launching the National Fraud Detection Center, a prosecutor-led, multi-agency team designed to use data analytics to proactively identify fraud against taxpayer-funded programs. Looking ahead, DOJ is also developing AI-enabled tools to apply anomaly detection across Medicare and Medicaid claims data, producing fraud risk scores and pattern classifications that could accelerate case generation at scale.

These developments reinforce the federal government's broader shift toward centralized, analytics-led enforcement. Healthcare providers should take note of this trend and consider whether their own compliance programs are leveraging data analytics to identify and mitigate risks before prosecutors do. For more information, read our client alert here.

Most recently, the DOJ announced revisions to the Justice Manual to clarify two aspects of False Claims Act enforcement for prosecutors. First, enforcement should focus on alleged violations of binding legal obligations by a party and not on violations of sub-regulatory guidance such as agency FAQs, internal memoranda or training materials. The DOJ emphasized that as a matter of fair notice to parties, subjects could be investigated for violations of law, but not guidance or other materials that do not constitute legally binding authority. Second, the DOJ clarified that, even as it declines to intervene in various *qui tam* actions, prosecutors should continue to assess, as these cases progress, whether the matters lack factual or legal merit, or fail to advance the interests of the United States. Prosecutors are encouraged to move to dismiss cases that meet these criteria in order to ensure that appropriate DOJ resources are allocated to pursuing meritorious False Claims Act investigations and enforcement matters. The DOJ

announcement regarding these revisions, with links to the actual Justice Manual revisions, can be found here.

OIG Advisory Opinion 26-15 (Referral Software Fees)

On June 30, HHS-OIG posted an unfavorable advisory opinion issued to a home health agency (HHA) seeking to pay subscription fees to a software vendor to access an online referral management platform used by hospitals. With this opinion, HHS-OIG has now released its third unfavorable advisory opinion addressing arrangements in which a seller of federally reimbursable items or services pays to access software utilized by referral sources in order to preserve or generate business with the referral source. We wrote about the other advisory opinions here. Across all three opinions, HHS-OIG has consistently emphasized the anti-competitive effects of such arrangements, finding that referral sources may favor sellers that pay for the software over those that do not. In-house counsel at healthcare companies should treat the opinion as a clear signal that HHS-OIG views pay-to-play software arrangements with significant skepticism.

In the arrangement at issue in Advisory Opinion No. 26-15, the software provides hospitals with a list of all available HHAs in a region for post-discharge patient referrals, but only HHAs that paid for a subscription could receive and respond to referral requests electronically through the platform. Where a hospital has subscribed to the software and an HHA has not, the hospital would be required to send the referral outside of the platform (e.g., via telephone or fax), and the non-paying HHA would be required to contact the hospital directly to accept the referral. Critically, the requestor certified that the speed with which an HHA responds to a hospital's request for home health services post-discharge is determinative of securing the referral. HHS-OIG found that the arrangement did not qualify for protection under the referral services safe harbor, in part because subscription fees were not assessed uniformly against all participants, and HHS-OIG concluded that the arrangement posed more than a minimal risk of fraud and abuse. In particular, HHS-OIG emphasized the risk of inappropriate steering and unfair competition, noting that, because hospitals often assign referrals on a first-come, first-served basis, subscribing HHAs enjoyed a significant competitive advantage. HHS-OIG also identified a risk of over utilization given that participating HHA could face pressure to recoup subscription costs by billing for medically unnecessary services.

Enforcement of Gender-Affirming Care Subpoenas

The DOJ secured a significant victory this quarter in its efforts to enforce gender-affirming care subpoenas. On Aug. 14, the 9th Circuit reversed a federal District Court's decision to quash a HIPAA administrative subpoena seeking information from a telehealth provider related to the provision of gender-affirming care. In reversing the order, the 9th Circuit held that the telehealth provider had not met its "heavy burden" of showing the subpoena was issued for an improper purpose. The majority emphasized that the Executive Branch's public opposition to gender-affirming care was insufficient to establish bad faith, that DOJ's actions are entitled to a presumption of regularity and that the president may direct DOJ to exercise its statutory authority in a manner consistent with his broader policy goals. The case was remanded for the District Court to address, in the first instance, arguments related to overbreadth, undue burden and patient privacy — which the 9th Circuit expressly acknowledged as viable bases for relief. You can find the 9th Circuit's opinion here.

However, on Aug. 26, the 2nd Circuit issued a procedural order denying the DOJ's motion to stay a preliminary injunction blocking federal prosecutors from obtaining gender-affirming care records from a New York hospital; it did not reach the merits of the underlying dispute. A federal district judge issued the injunction on July 6 following a temporary restraining order entered in June. Notably, this case arose from grand jury subpoenas — rather than administrative subpoenas — issued by the U.S. Attorney's Office in the Northern District of Texas, reflecting an escalation in DOJ's enforcement strategy following its string of losses at the District Court level in the administrative subpoena context.

Taken together, these appellate developments present a mixed picture for healthcare providers, although they reflect different procedural postures. The 9th Circuit's decision signals that courts may be reluctant to find improper purpose based solely on administration policy statements, while the 2nd Circuit's refusal to lift the New York hospital's injunction demonstrates that providers retain meaningful avenues to challenge DOJ's investigative demands, including in the grand jury context. Providers who receive similar subpoenas should continue to evaluate all available grounds for challenge, including overbreadth, undue burden and patient privacy. They also may take note that several New York City-based hospitals have entered into False Claims Act settlements. As part of these civil settlement agreements, the hospitals did not make any admissions of wrongdoing or liability. For more information about these settlements, see here and here.

RICO Charges Involving Healthcare Fraud Schemes

On Aug. 20, the U.S. Attorney's Office for SDNY and the Fraud Division unsealed a nine-count indictment charging four members of a Bronx-based criminal organization known as the "War Room" with racketeering conspiracy, healthcare fraud and AKS violations, among other criminal offenses, in connection with a scheme that generated over $12 million in fraudulent Medicaid claims. As alleged in the indictment, the defendants fabricated transportation data by using GPS "spoofing" applications to falsify pickup and drop-off locations for rides that never occurred. The defendants recruited patients from addiction treatment clinics and paid them kickbacks in cash and drugs in exchange for their enrollment information, operating under the guise of a sham charity.

The case is notable for DOJ's use of the Racketeer Influenced and Corrupt Organizations (RICO) Act to prosecute what is fundamentally a Medicaid fraud scheme. RICO, originally enacted in 1970 to combat organized crime, renders it unlawful to conduct the affairs of an enterprise through a pattern of racketeering activity, which can include healthcare fraud, wire fraud and AKS violations as predicate acts. While uncommon, prosecutors' use of RICO to charge healthcare fraud is not new. Indeed, in March 2026, the owners of the Savani Group — a multi-state network of dental practices — were convicted in the Eastern District of Pennsylvania of RICO conspiracy, among other charges, in connection with a $30 million scheme to obtain Medicaid contracts and fraudulently bill Medicaid using nominee-owned dental practices after managed care companies terminated the group's existing agreements.

For healthcare providers and their counsel, the case is a reminder that DOJ continues to view healthcare fraud through an increasingly expansive enforcement lens. The use of RICO here — in a case brought jointly by the SDNY and the Fraud Division — signals that prosecutors may be more willing to layer racketeering charges onto fraud schemes that involve aggravating factors such as kickbacks to vulnerable patients, collusion among multiple entities, and the use of violence or intimidation to protect illicit revenue streams. Providers should be aware that participation in or proximity to schemes exhibiting these characteristics may elevate their exposure well beyond traditional fraud and abuse penalties.

For more information, see the DOJ's press release here.

CMS Campaigns to 'Crush Fraud'

At the September 2026 Boston Regional Health Care Compliance Association Conference, featured presenter CMS Deputy Administrator and COO Kim Brandt signaled that the agency's two overarching priorities are (1) drug pricing and affordability and (2) an aggressive campaign to "crush fraud." CMS reported $41.9 billion in Medicare program integrity savings in FY 2025, a 59% increase over the prior year and the highest return on investment the agency has ever recorded at over $22 saved for every dollar invested. This reflects a fundamental shift from the traditional "pay-and-chase" recovery model to prepayment interdiction: 68% of savings now come from cost avoidance through revocations, automated claim denials and other actions taken before money leaves the program. The Fraud Defense Operations Center suspended more than $2.1 billion in potentially fraudulent payments across 453 providers in a single year, and CMS has revoked over 1,400 providers and suppliers from Medicare, a 40% increase

over last year. For Medicaid, CMS is applying this level of scrutiny for the first time, deferring more than $1 billion in federal payments and directing all 50 states to develop revalidation strategies for high-risk providers. Brandt also cited the recently lifted six-month DME moratorium as a continued area of focus for the agency.

Healthcare organizations should take note of technology and policy developments by CMS and the other government agencies highlighted in Brandt's presentation. CMS deploys AI and machine-learning tools at scale and uses risk-scoring algorithms that screen new enrollees against historical bad-actor patterns. Similar to the DOJ's efforts, CMS's use of proactive, large-scale analyses can inform when and how compliance officers use their own data to identify, prioritize and manage risks.

HHS Updated Corporate Integrity Agreement

Introduced earlier this year, the updated HHS-OIG CIA template was discussed at the American Health Law Association Annual Meeting and reflects OIG's most current compliance expectations. As reflected in recently published CIAs, the template maintains OIG's established compliance elements while adding new requirements that reflect the agency's evolving expectations.

Key additions appear in sections concerning compliance officer role and responsibilities, such as a requirement that compliance officers have direct and independent access to the board; board oversight, including requirements that boards include at least one independent (e.g., non-owner, non-employee and non-executive) member and retain an independent compliance expert; compliance committees, including a requirement that compliance committees include a member with IT expertise; arrangements with healthcare providers and organizations, including requirements that establish greater rigor around tracking and verifying arrangements and maintaining continuous fair market value documentation throughout an arrangement's life cycle; risk assessments, with the template outlining a prescribed five-step risk assessment methodology; and training, including broadened annual training requirements that go beyond the seven elements of an effective compliance program to cover all requirements under federal healthcare programs. Notably, for the first time, OIG expressly addressed generative AI in a CIA, requiring organizations to disclose whether they use AI in their compliance programs or in preparing reports, explain how it was used and provide assurance that AI-generated content was verified for accuracy.

Healthcare organizations, regardless of whether they currently operate under a CIA, should closely review the updated template, as these changes may inform how OIG evaluates compliance programs in future investigations, audits and enforcement actions.

OIG Semiannual Report

HHS-OIG's Spring 2026 Semiannual Report to Congress, issued on July 10 and covering Oct. 1, 2025 through March 31, 2026, reflects continued federal attention to healthcare fraud, improper payments, program integrity, and weaknesses in documentation and oversight. OIG reported approximately $5.56 billion in expected recoveries and projected savings, along with 604 criminal and civil enforcement actions and 1,212 exclusions from participation in federal healthcare programs. Significant matters included enforcement involving Medicare Advantage billing as well as OIG reviews identifying improper or potentially improper Medicaid payments, including payments associated with applied behavior analysis services.

For hospitals, health systems and providers, the report reinforces that OIG scrutiny extends beyond traditional fraud investigations to the underlying compliance processes that support accurate billing and appropriate use of federal healthcare dollars. Documentation deficiencies, payment accuracy, provider qualifications and lapses in organizational oversight continue to generate significant findings even where intentional misconduct is not alleged. Compliance leaders should consider these findings when

developing risk assessments, audit and monitoring plans, and data-analytic initiatives, with a particular focus on high-dollar or rapidly expanding services.

Privacy

This quarter saw continued developments in state privacy laws and protections for sensitive data, alongside growing attention to cybersecurity and data governance through new federal initiatives addressing AI-driven vulnerabilities and upcoming compliance obligations under the DOJ's Bulk Data Transfer Rule.

New State Privacy Rules Require Businesses to Assess High-Risk Activities and Regulate Disclosures of Sensitive Data

Businesses will need to take a closer look at upgrading their privacy programs as states consider more stringent laws on the collection and processing of personal data. In 2026, four states — Oklahoma, Louisiana, Alabama and Vermont — passed comprehensive new state privacy laws. Additionally, three states — Virginia, Maryland and Connecticut — have passed significant amendments to their privacy laws. While the new state laws may take effect in 2027, some of these amendments took effect this past July or will take effect in October.

This legislation is similar to past state frameworks, albeit with a greater emphasis on data protection impact assessment requirements, protections around the sale of data, and disclosures on the use of automated decision-making and large language models. With a national privacy law still unlikely, healthcare organizations will need to determine whether and how they need to comply with these requirements and take further steps to operationalize their privacy programs.

For more information, read our client alert here.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Boston

Dhara Satija
+1-617-912-1616
dharasatija@paulhastings.com

Hari Pillai
+1-617-912-1617
haripillai@paulhastings.com

Los Angeles

Jeni Griffin
+1-213-683-6159
jenigriffin@paulhastings.com

New York

Jane H. Yoon
+1-212-318-6006
janeyoon@paulhastings.com

Jessica Montes
+1-212-318-6657
jessicamontes@paulhastings.com