CLIENT ALERT | WHITE COLLAR INVESTIGATIONS, RISK & INTEGRITY

Accelerating Data-Driven & AI-Enabled Enforcement in Healthcare & the Importance of an Integrated Risk Management Framework

AUGUST 10, 2026

BY RALPH DADO AND KATE MCCLELLAND

In late July, the Department of Justice's (DOJ's) National Fraud Enforcement Division announced the first declination of a healthcare company under the new Department-wide corporate enforcement policy. In explaining its decision to decline charges, the government specifically noted that the organization proactively cooperated by, among other things, retrieving and analyzing its own historical data.[1]

Roughly forty-five days since the DOJ's announcement of its sweeping June National Health Care Fraud Takedown, it is critical to understand the declination, the June Fraud Takedown, and other developments this year as connected parts of a wider, accelerating enforcement trend in the healthcare sector involving the rapid scaling of investigations through advanced data analysis and artificial intelligence (AI) integration. This, in turn, signals the need for thoughtfully designed compliance and risk mitigation strategies that account for the shift in enforcement through an integrated risk management strategy for company data.

Takeaways

- DOJ is leveraging advanced data analytics and artificial intelligence to emerge as a leader in a "whole of government" data-driven approach to investigation and enforcement in the healthcare sector alongside other agencies.
- This expanded analytical power complements, but does not replace, traditional enforcement measures.
- The current trend should be expected to accelerate and, in this environment, companies must apply an integrated, proactive risk management approach to their data to match DOJ and other agency capabilities; it is not sufficient to regard data as an "after-the-fact" issue in compliance and enforcement.

Data-Driven Trends in DOJ's Approach to the Healthcare Sector

The July 2026 declination by DOJ is an example of how healthcare companies can leverage advanced data analysis techniques, progressively augmented with AI, to respond effectively to government investigations that increasingly rely on these tools. As investigators expand their ability to meaningfully analyze healthcare data, target companies can use advanced tools to determine the patterns revealed by their own data, giving them a broader range of options when confronted by the possibility of an investigation. Within government, the administration's new Task Force to Eliminate Fraud, supported by DOJ's National Fraud Enforcement Division, seeks to capitalize on government experts' growing ability to share data across federal agencies in a "whole of government" approach to data analysis, investigation, and enforcement.[2] The government has spent 2026 showcasing its ability to deploy AI and advanced data analytics tools against healthcare targets, including:

- Implementing the new National Fraud Enforcement Division;[3]
- Coordinating the June Fraud Takedown led by that Division;[4]
- Streamlining receipt of data-mined information from potential relators in *qui tam* actions;[5] and
- Stopping payments in real time through the Centers for Medicare & Medicaid Services' (CMS) Medicaid Fraud War Room.[6]

Today the government's focus is advancing through the trove of data generated by federal health benefits systems—and, just as one example, mining every layer of those systems contributed to a substantial increase in the number of defendants charged in DOJ's 2026 healthcare takedown versus the 2025 enforcement.[7] We are in the *beginning* stages of synchronized government enforcement efforts driven by data analytics and AI, which will accelerate as the "whole of government" becomes increasingly coordinated around this objective.

For companies across the healthcare and life-sciences sectors, including pharmaceutical and medical-device manufacturers, healthcare providers at scale, and insurers, this is the moment to proactively prepare for upcoming data-powered advances in investigations. Companies need to take a close look at their own data to identify problematic patterns to mitigate future risks. Scrutinizing internal data also expands companies' available options when confronted with an investigation, as seen in the recent declination.

It is vital that these, and other, data activities occur not in an *ad hoc* or reactive manner but through an integrated risk management approach, which systematically identifies key data, organizes and pools it within internal systems through established processes,

assesses it to identify risks, develops effective mitigations to those risks, and creates governance around these efforts. Such an approach aligns with DOJ's own guidance in its latest Evaluation of Corporate Compliance Programs (2024), which instructs prosecutors to evaluate company capabilities, including access to operational data, use and validation of analytics, and integration of emerging-technology risk into broader risk-management systems.[8]

Treating data like this, as a critical input to the company's overall risk management framework, is important both because of data's rising significance for purposes of regulatory, legal, and enforcement exposure and because the government on the other side is applying this level of sophistication to its own enforcement efforts. Effective analytics, including appropriately governed AI tools, should enable healthcare companies to answer practical questions such as:

- What is our response when a whistleblower has provided investigators with our clinical trial data paired with an AI-written program enabling them to examine it as efficiently as an internal company subject-matter expert?
- Can we identify outliers in claims and utilization data (billing, coding, prior authorization, referral, etc.) before DOJ, CMS, a state regulator, or a relator does, and distinguish legitimate variation patterns from issues requiring escalation?
- How can we effectively gather and analyze data from our manufacturing processes to explain and defend them concisely, particularly as seasoned experts continue leaving regulatory bodies like the Food and Drug Administration (FDA)?
- Does our support and outreach program data (speakers, consulting, copay assistance, free samples, reimbursement support, etc.) show patterns or correlations that an investigator or relator could characterize as improper and, if they are in fact legitimate, do we have documentation to support that counter-characterization?
- Where do we face the most regulatory and enforcement risk from a product market and pricing strategy (price reporting, rebates, discounting, contracting, channel strategy, etc.) and what are the most risk-spend-efficient means to reduce that risk?
- Can we connect adverse events, product complaints, and clinical, service, warranty, and manufacturing data across systems quickly enough to detect an emerging safety signal, make a defensible reporting decision, and demonstrate that escalation was timely?

Companies in the healthcare sector are at varying levels of systems and process maturity when it comes to this type of risk-based data integration and assessment. Not all elements of a framework need to be implemented to full maturity immediately, and various elements can be enhanced over time (for example, enhancing the linkage with the company's Enterprise Risk Management approach; shifting toward leading versus lagging indicators; and enhancing predictive capabilities).

But the challenge in 2026 is to ensure that the basic pillars of this approach are in place promptly given the Department's already-demonstrated ability to leverage data for enforcement purposes at a scale that was not being contemplated even a few years ago. Healthcare companies of all stripes that effectively manage risk will know their own data and use it creatively to design compliance programs that will withstand intense government scrutiny and drive better outcomes when enforcement does occur.

Data-Driven & AI-Enabled Enforcement Trends Will Deepen Traditional Areas of Risk

Even as the government expands its approach with advanced data analysis, it continues to prioritize traditional areas of healthcare enforcement. The current regime should not be thought of as substitutive (data-driven enforcement replacing traditional enforcement methods and priorities) but rather as "enforcement plus"—data-driven enforcement deepening the government's existing enforcement footprint and priorities.

In this context, DOJ's statements regarding recent settlements and deferred prosecution agreements have highlighted its continued scrutiny of the healthcare sector, including pharmaceutical companies. This includes two recent civil settlements in False Claims Act cases against pharmaceutical companies, with one case involving payments to physicians in the form of speakers' fees and the other case involving reimbursements and free samples to providers, both topics of long-standing focus for the Department.[9] In the settlement announcements, the new National Fraud Enforcement Division was mentioned, demonstrating the alignment between the administration's ongoing anti-fraud push and healthcare sector scrutiny. Prosecutors also reached a deferred prosecution agreement with a medical technology company, which acknowledged that it failed to file adverse event reports with the intent to defraud or mislead the FDA.[10]

On that note, the FDA, particularly through its Center for Drug Evaluation and Research (CDER), continues to pursue perennial approaches to investigations while signaling gradual updates to its risk management evaluations. In the area of current good manufacturing practice (CGMP), FDA's March 2026 draft guidance offered insight into current expectations about drug manufacturers' responses to receiving a Form 483.[11] The draft guidance suggests that investigators are paying particular attention to whether

manufacturers' responses demonstrate not only management's thorough understanding of the problems identified, but also that management is substantively addressing root causes with appropriate remediations.[12] Further, CDER announced in early 2026 that it was accepting a fresh round of applicants for its voluntary Quality Management Maturity Program, indicating a continuing commitment to supporting practices that advance beyond the bounds of CGMP.[13] CDER also appears to be paying close attention to the use of AI in drug manufacturing, having counseled against "overreliance" on AI and stressed the importance of "human accountability" in public statements and an April 2026 warning letter to a manufacturer.[14]

The interaction between the government's rising data-driven focus and its ongoing emphasis on traditional areas of enforcement provides opportunities now for thoughtful planning. *First*, companies should be thinking *now* about how a data-driven (and AI-enabled) enforcement approach will affect their potential exposure within the various areas of traditional DOJ, FDA, and other agency focus, including speaker programs; off-label marketing; reimbursement programs; pricing activity; and patient support efforts. To the extent there are identifiable issues within the associated data for these activities, companies must be able to spot them, because the government is rapidly moving toward an equivalent capability. Indeed, the Department in its June Fraud Takedown press release stated:

> To enhance the deployment of advanced analytics to target health care fraud, the Fraud Division and CMS announced today that they have entered an agreement whereby the Fraud Division will be provided cloud computing space in the CMS Integrated Data Repository environment in which to deploy advanced data analytics algorithms and artificial intelligence tools. In addition, the Fraud Division entered into agreements with the Department of Homeland Security and the Federal Trade Commission aimed at breaking down data silos and improving access to information critical to identifying and combatting health care fraud. CMS also is announcing today that it is developing a Claims Core processing with electronic attestation, identify verification, and IP address log-in, and working to get pledges that all Medicaid, Managed Care, and other plans report the same standardized data fields used for Medicare Part B claims data.[15]

Second, companies should be considering how the government's current enforcement guidance and policies interact with its expansion into data-driven enforcement, which can create a complex calculus and require weighing considerations that were not in play even just a couple of years ago.

For example, as described above, the DOJ's 2024 refinements to its policy on evaluating corporate compliance programs ask prosecutors to consider a target company's own data

analytics processes and use of AI to effectively respond to emerging risks and monitor compliance.[16] The new Department-wide corporate enforcement policy, which was applied in the July 2026 declination, formalizes and standardizes prosecutors' responses to disclosures and encourages prompt, voluntary self-disclosure of misconduct.[17]

The incentive is therefore present for companies under enforcement scrutiny both to demonstrate significant data analytics capability and to self-disclose, including in the form of company data. But this must be balanced against the fact of the Department's own enhanced data analytics capability, which could expose issues that the company itself is not aware of (particularly if it lacks a robust risk management framework). Disclosure now turns on not merely identifying data responsive to the issue at hand but understanding the extent to which that data, when exposed to sophisticated government analytics, could reveal additional issues. In such a situation, where is the right line for strategic self-disclosure and how can a company's own data analytics assist with this judgment call?

This and other issues at the new intersection of advanced healthcare data analysis and DOJ policy will inform prosecutorial decision-making and enforcement mitigation and defense. Companies will be better able to plan, mitigate risk, and, in the event of an enforcement scenario, defend themselves by carefully considering these topics now.

Implications

The key high-level question to ask now is: do we know what story our own data is telling? The government's aggressive scaling of its data analytics capabilities demands corresponding internal capabilities that can proactively identify patterns and mitigate risks.[18] Investigators and prosecutors are incorporating advanced data tools into the frameworks that they use to evaluate every stage of a case, and successfully navigating any enforcement action (or proactively avoiding such an action) requires preparation for this new reality. Problems that might once have gone unidentified may now be unearthed, necessitating strengthened internal controls and compliance resources directed through an overall risk management framework. Doing this enables a company to understand the data it has and the potential issues that data reveals and to escalate and act upon those issues.

Companies will reduce their exposure through this thoughtful management of data. This should be coupled with careful monitoring of investigators' ongoing enforcement activities and messaging to keep a finger on the pulse of ongoing growth in the data and AI-driven enforcement trend.

We continue to monitor these and other developments. Please contact the White Collar Investigations, Risk & Integrity group with any questions or for further guidance.

Authors

Ralph Dado
Partner, Aronberg Goldgehn

Kate McClelland
Partner, Aronberg Goldgehn

[1] Letter from Darren C. Halvorsen et al. to Ben Curtis et al., at 2 (July 28, 2026), https://www.justice.gov/opa/media/1454681/dl?inline; *see also* U.S. Dept. of Justice, Fraud Division Resolves Fraud Investigation of Eye Care Group Under New Corporate Enforcement Policy; Health Care Executive Charged for Alleged Fraud and Kickbacks (July 29, 2026), https://www.justice.gov/opa/pr/fraud-division-resolves-fraud-investigation-eye-care-group-under-new-corporate-enforcement.

[2] U.S. Dept. of Justice, National Health Care Fraud Takedown Results in 455 Defendants Charged in Connection with Over $6.5 Billion in Alleged Fraud (June 23, 2026), https://www.justice.gov/opa/pr/national-health-care-fraud-takedown-results-455-defendants-charged-connection-over-65.

[3] U.S. Dept. of Justice, About the National Fraud Enforcement Division (Apr. 29, 2026), https://www.justice.gov/fraud/about-national-fraud-enforcement-division.

[4] *See* note 2.

[5] U.S. Dept. of Justice, Civil Division Announces FOCUS Initiative for Data Miners Filing *Qui Tam* Complaints (Apr. 30, 2026), https://www.justice.gov/opa/pr/civil-division-announces-focus-initiative-data-miners-filing-qui-tam-complaints.

[6] Ctrs. for Medicare & Medicaid Servs., CMS Medicaid Fraud War Room Stops More Than $203 Million in Improper Payments During First 88 Days (July 28, 2026), https://www.cms.gov/newsroom/press-releases/cms-medicaid-fraud-war-room-stops-more-203-million-improper-payments-during-first-88-days.

[7] *Compare* note 2 *with* U.S. Dept. of Justice, National Health Care Fraud Takedown Results in 324 Defendants Charged in Connection with Over $14.6 Billion in Alleged Fraud (June 30, 2025), https://www.justice.gov/opa/pr/national-health-care-fraud-takedown-results-324-defendants-charged-connection-over-146.

[8] U.S. Dept. of Justice, Crim. Div., Evaluation of Corporate Compliance Programs (Sept. 2024), at 3-4, 13, https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl?inline.

[9] U.S. Dept. of Justice, Takeda Agrees to Pay $13.6M to Resolve False Claims Allegations Relating to Improper Payments to Physicians (May 14, 2026), https://www.justice.gov/opa/pr/takeda-agrees-pay-136m-resolve-false-claims-allegations-relating-improper-payments; U.S. Dept. of Justice, EyePoint Pharmaceuticals to Pay $4.6 Million to Resolve False Claims Act Allegations (July 17, 2026), https://www.justice.gov/opa/pr/eyepoint-pharmaceuticals-pay-46-million-resolve-false-claims-act-allegations.

[10] U.S. Dept. of Justice, Former ExThera Medical Corporation Executive Admits to Concealing Patient Deaths from FDA and Company Enters Deferred Prosecution Agreement (Mar. 5, 2026), https://www.justice.gov/opa/pr/former-exthera-medical-corporation-executive-admits-concealing-patient-deaths-fda-and.

[11] U.S. Food & Drug Admin., Responding to FDA Form 483 Observations at the Conclusion of a Drug CGMP Inspection: Guidance for Industry (Mar. 2026), https://www.fda.gov/media/191427/download.

[12] *See* note 11 at 8-9.

[13] Voluntary Quality Management Maturity Prototype Assessment Protocol Evaluation Program, 91 Fed. Reg. 6229 (Feb. 11, 2026).

[14] James Jarvis & Jessica Karins, Acting CDER Director Stresses Human Accountability As Use of AI Expands, Inside Health Policy (May 22, 2026), https://insidehealthpolicy.com/daily-news/acting-cder-director-stresses-human-accountability-use-ai-expands; Letter from Francis Godwin, et al., to Maria Mattina (Apr. 2, 2026), https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/purolea-cosmetics-lab-722591-04022026.

[15] *See* note 2.

[16] *See* note 8 at 3-4, 13.

[17] U.S. Dept. of Justice, Corporate Enforcement and Voluntary Self-Disclosure Policy (Mar. 10, 2026), https://www.justice.gov/dag/media/1430731/dl?inline; *see also* U.S. Dept. of Justice, Department of Justice Releases First-Ever Corporate Enforcement Policy for All Criminal Cases (Mar. 10, 2026), https://www.justice.gov/opa/pr/department-justice-releases-first-ever-corporate-enforcement-policy-all-criminal-cases; *see also* note 1.

[18] *See* note 2.