

What Healthcare Providers and Life Sciences Companies Can Expect for Enforcement in 2022

February 1, 2022

After a relative lull in white-collar enforcement during the last U.S. administration, many anticipated resurgent healthcare enforcement activity in 2021, particularly given Department of Health and Human Services (HHS) Secretary Xavier Becerra's background as the former attorney general of California.¹ But amidst the challenges of a pandemic that has yet to fully recede, enforcement efforts by the Biden administration got off to a slow start; for example, by the end of 2021, two-thirds of the U.S. Attorney slots were yet to be filled with Senate-confirmed prosecutors. Over the past few months, though, the Department of Justice (DOJ) has shown signs of increased activity, turning its attention back to one of its favorite targets, the healthcare and life sciences industry. After more than a year of responding to the pandemic, HHS, too, is likely to increase its focus on affirmative projects, both independently and in partnership with DOJ. As but one example, a recent [letter](#) sent by nearly 200 House of Representatives members to the White House urging the executive branch to investigate allegedly inflated pricing by nurse staffing agencies presents the type of consumer-protection-oriented project that HHS may embrace.

Below are areas the government is likely to view as particularly attractive targets in the coming year, focused on healthcare providers, life sciences companies, and the industry at large.

Healthcare Providers

Pandemic Regulatory Flexibilities, Especially Telehealth

HHS offered healthcare providers unprecedented regulatory flexibility during the COVID-19 public health emergency (PHE). Many of these regulatory flexibilities are tethered to the pendency of the PHE and as a result continue to remain available to providers. The most significant shifts arose through HHS's power under Social Security Act Section 1135 to waive or modify certain federal healthcare requirements during declared PHEs. Through waivers, the Centers for Medicare & Medicaid Services (CMS) has, among many other flexibilities, significantly altered the scope of Medicare-payable telehealth services, exempted certain financial relationships from otherwise-applicable sanctions under the Stark Law, and broadly expanded the circumstances qualifying a patient for skilled nursing facility coverage under Medicare Part A.

DOJ has reiterated that combatting and preventing COVID-19-related fraud is a priority for law enforcement, but so far, there have been relatively few announced enforcement actions relating to abuse of pandemic regulatory flexibilities. For example, last year DOJ Criminal Division announced two prosecutions for abuse of the CMS telehealth waivers as part of broader schemes to bill for medically unnecessary cancer and cardiovascular genetic testing, but DOJ Civil Division has not yet publicly pursued any enforcement actions under the False Claims Act (FCA) solely relating to more nuanced abuse of the telehealth waivers. Nonetheless, there are reasons to believe that increased enforcement actions in this space, especially on the civil side, remain pending in the pipeline, particularly with respect to telehealth, which experienced one of the most dramatic pandemic alterations in billing practices. Over the past two years, DOJ's pace of investigating and resolving FCA cases has slowed significantly, but as DOJ begins to return to a new normal, and new leadership at Main Justice and the U.S. Attorneys' Offices is confirmed, we expect to see additional scrutiny — likely driven by data-mining and the finding of pending HHS Office of the Inspector General (HHS-OIG) reports on telehealth billing integrity — of how providers have used pandemic billing flexibilities.

Remote Patient Monitoring (RPM)

The COVID-19 pandemic also served as an accelerant for the growing area of RPM. RPM leverages devices such as continuous glucose monitors and digital blood pressure monitors to allow healthcare providers to monitor patient health remotely. Patients and providers looking for virtual care options during the pandemic increasingly turned to RPM. Providers have reported successful RPM programs to manage at-home recoveries from COVID-19 in addition to better managing chronic conditions such as diabetes.

Even as providers continue to experiment with RPM, CMS, too, is gaining its footing from a billing and coding perspective. Effective January 1, 2018, CMS first introduced separate Medicare reimbursement for generic RPM codes and in each year since has expanded the reimbursement opportunities for RPM, sometimes temporarily during the pandemic but often permanently. Complicating the challenges inherent in a new billing area, CMS has provided multiple midstream clarifications around RPM billing rules. Many are expecting that RPM will continue to expand postpandemic, and as with telehealth, the infusion of additional reimbursement over the past couple of years will draw enforcement scrutiny. HHS-OIG has already announced that it will be auditing RPM billing, and the publication of that report — expected later this year — will likely attract further whistleblower attention as well.

Use of Antitrust Violations as a Basis for FCA Liability

The Biden administration has expressed its intention to tighten up antitrust enforcement to promote competition, and the healthcare industry is one of a handful of target industries identified in the July 9, 2021 Executive Order on Promoting Competition in the American Economy.³ Even prior to the executive order, DOJ had begun using antitrust violations in the drug pricing context as the predicate for FCA liability. For example, on October 1, 2021, DOJ announced that a trio of pharmaceutical companies paid, in the aggregate, nearly half a billion dollars to resolve allegations that they conspired to fix the prices of generic drugs.⁴ Although framed in part as Anti-Kickback Statute (AKS) violations, the proposition that anticompetitive conduct can “artificially inflate prices” and result in false claims may be raised by DOJ as a standalone theory separate from kickbacks.

OIG, too, seems to have recently embraced the notion that fraud and abuse can be inextricably linked

with competition concerns. In an AKS advisory opinion issued late last year to a provider of therapy and rehabilitation services, OIG concluded that it may impose sanctions on a proposed joint venture between the therapy provider and the owner of long-term care facilities.⁵ OIG concluded that the proposed arrangement presented “significant” fraud and abuse concerns for both traditional reasons — it seems “designed to permit Requestor to do indirectly what it cannot do directly: pay the JV Partner a share of the profits from the JV Partner’s referrals ... to Requestor for therapy services” — and nontraditional ones — it may “block out potential competitor therapy services providers.” OIG has historically not focused on competition concerns in its AKS advisory opinions, and this shift may portend a keener interest across law enforcement in the intersection between antitrust and fraud and abuse.

No Surprises Act Enforcement and Litigation

On January 1, 2022, federal surprise billing legislation known as the No Surprises Act (NSA) went into effect. The law’s principal feature is to bar healthcare providers from balance billing patients for certain services provided out-of-network and instead channel disputes between providers and insurance companies over out-of-network reimbursement through an independent dispute resolution (IDR) process. The NSA imposes additional requirements on providers, including that they must furnish patients with a good faith estimate of expected charges, with further restrictions on billing beyond that initial estimate.

Enforcement of the NSA as to both payors and providers is split between states and the federal government. For example, states have primary responsibility for enforcing the good faith estimate requirement, and HHS will enforce only in states that have notified HHS that they are unable or unwilling to do so themselves. A number of states have informed HHS that they lack authority to enforce this provision, and therefore HHS will be taking up the role of enforcer.⁶ HHS has opened a portal soliciting complaints from patients about violations of this and other provisions of the NSA.⁷ HHS can impose civil monetary penalties of up to \$10,000 per violation. We expect that HHS will prioritize enforcement of the good faith estimate provision in particular, and providers should take steps to ensure compliance with this new requirement.

In addition to government-initiated enforcement actions against providers, the government can expect to be on the receiving end of provider-initiated lawsuits. The federal agencies responsible for implementing the NSA have generally been applauded by health insurance companies and criticized by healthcare providers for choices they have made that benefit payors at the expense of providers. At the forefront of these contentious decisions is the choice to give almost outcome-determinative weight in the IDR process to a particular metric relating to contracted rates that payors calculate. This feature of the agencies’ rulemaking has been the subject of six lawsuits, and whatever the outcome, further litigation is likely in 2022 over other aspects of the government’s implementation of the NSA.

Life Sciences Companies

Off-Label Enforcement and the Food and Drug Administration’s (FDA) New Definition of “Intended Use”

In the fall of 2021, FDA issued a final rule⁸ amending the regulatory definitions of “intended use” to significantly expand the types of evidence FDA will consider when determining whether a manufacturer intends its drug or device to be used off-label, i.e., for a new intended use. As discussed further [here](#), under the prior definition, “intended use” generally turned on the manufacturer’s promotional claims. But

the new definition, according to accompanying preamble language, purports to authorize FDA to “look to any relevant source of evidence, including a variety of direct and circumstantial evidence.” 86 Fed. Reg. at 41,386, 41,388. Such evidence may include safe-harbored communications, for example, distribution of scientific and medical publications. According to the new codified definition, it may also include the product’s “design or composition.” Depending on the circumstances, even the manufacturer’s knowledge of off-label use may be cited as evidence of a new intended use in a particular investigation. Though the preamble accompanying the final rule indicates that the intent behind the amendments was to provide “clarity and direction” to manufacturers, 86 Fed. Reg. at 41,384, FDA’s new definition sows confusion by shifting from an objective standard focused on external claims to a standardless, unpredictable inquiry into “all relevant sources of evidence.” Manufacturers should assess the operational effects of FDA’s revised definition, particularly any historical reliance on policies defining safe-harbored communications, and remain aware of enforcement actions that are based in part on the revised definition.

Intersection Between Rebates and the AKS

In the waning days of the prior administration, HHS issued a rule (Rebate Rule) that would have revised the AKS discount safe harbor to remove protection for rebates from drug manufacturers to Part D plan sponsors, either directly or indirectly through a pharmacy benefit manager (PBM), unless required by law. The Rebate Rule also created two new safe harbors: one for certain point-of-sale price reductions on drugs and another for certain fixed fees that manufacturers pay to PBMs for services rendered to the manufacturers. In the face of litigation from industry, early last year the Biden administration delayed the effective date of the rule to January 2023. Congress then further delayed the implementation of the rule to 2026 through the Infrastructure Investment and Jobs Act, which was signed into law on November 15, 2021. The Rebate Rule has been contentious, particularly because of controversial positions articulated by HHS-OIG in the rule’s preamble. For example, OIG stated that it was “confirm[ing] our position, as stated in the preamble to the Proposed Rule, that any portion of a payment (whether it is called a ‘rebate’ or something else) that a manufacturer pays to a PBM that is retained by the PBM and not passed through to the buyer never was protected under the discount safe harbor. ... [because a] PBM is not a buyer, and the portion of a payment from a manufacturer to a payor that is retained by a PBM is not a reduction in price.” Even though the Rebate Rule has been delayed and may ultimately be invalidated to offset the costs of other legislation, this interpretive statement was set forth in the preamble and should be considered further in assessing the potential risks of certain Part D rebate arrangements. HHS continues to assess its position on moving price concessions to the point of sale, as evidenced by its recent proposal to require Part D plans to apply all price concessions they receive from network pharmacies to the point of sale. Manufacturers, PBMs, and Part D plans should continue to assess their rebate arrangements in light of evolving federal and state government developments and continue proactively to engage with government stakeholders.

Compensation Arrangements With Independent Contractor Sales Forces

DOJ has increasingly targeted commission-based arrangements with independent contractors under the AKS. In March 2021, as discussed further [here](#), DOJ issued a press release announcing a recent U.S. Court of Appeals for the Fourth Circuit victory, which DOJ broadly characterized as holding that commission-based sales force compensation arrangements unprotected by a safe harbor, including those with nonemployee contract sales forces — standard in some sectors of the healthcare and life

sciences industries — are unlawful remuneration given to “recommend” products. This pronouncement is inconsistent with the historically nuanced, fact-intensive analysis OIG engages in to assess the legality of compensation arrangements and lies in tension with the First Amendment’s protections for truthful, nonmisleading commercial speech (which notably were not raised to the Fourth Circuit). The case is part of a larger trend, as DOJ continued to enter into settlements over the past year involving arrangements where “the amount of the kickback was based either on a percentage or fixed amount of Medicare’s reimbursement for each test”¹⁰ or “illegal remuneration [was offered] ... in the form of volume-based commissions paid to independent contractor recruiters.”¹¹ DOJ’s newfound focus on these types of financial arrangements highlights the importance of companies’ structuring their contracts where possible to comply with the AKS’s employee or personal services safe harbors and otherwise to minimize contextual risks that could draw enforcement scrutiny.

Issues of Cross-Cutting Concern to the Healthcare and Life Sciences Industry

Private Equity (PE) Investors and FCA Risk

PE investors in the healthcare industry have increasingly been the subject of FCA enforcement actions relating to the alleged misconduct of their portfolio companies. DOJ has historically focused only on majority PE investors actively involved in the management of their portfolio companies, but last year, DOJ for the first time entered into a settlement with a minority PE investor. While this particular investor also had a management services agreement with the portfolio company at issue, certain of DOJ’s comments in the press release announcing the settlement suggest that DOJ may not always limit FCA liability to PE investors that also actively manage portfolio companies. In the press release, DOJ explained that the minority PE investor allegedly “learned of ... kickbacks based on due diligence” it performed prior to investing in the company and then failed to remedy the fraud postclosing. DOJ’s criticism of PE investors gaining knowledge during due diligence and then not halting the known noncompliance suggests that DOJ expects PE investors with authority to impose compliance adjustments postclosing to do so.

This position is consistent with a broader expectation DOJ began articulating last year that companies profiting from business relationships involving misconduct have an obligation to take steps to cease profiting from that misconduct. For example, in a November 2021 press release announcing an FCA settlement with a pharmaceutical manufacturer, DOJ criticized the manufacturer for directing physicians to send prescriptions to particular specialty pharmacies engaging in misconduct, such as falsifying prior authorization requests.¹² The manufacturer allegedly “knew of or deliberately ignored this pharmacy misconduct, but nevertheless kept directing business to these pharmacies,” and this continued profiting off of a business partner’s misconduct was part of the alleged misconduct resolved by the settlement. Taken together, these cases demonstrate that DOJ expects highly sophisticated healthcare industry actors — whether they directly provide healthcare items or services to government payors or merely invest in healthcare companies — to take a broad view of their compliance obligations.

Cybersecurity and FCA Risk

In fall 2021, DOJ announced a Civil Cyber-Fraud Initiative,¹³ through which DOJ uses the FCA to prosecute cybersecurity-related fraud. Though the initiative is not focused on any particular industry and in many ways appears aimed at government contractors and grant recipients, hospitals, health systems, and medical device and health technology companies can expect to face risk. The initiative is designed

to attract whistleblowers, and the healthcare industry has historically been whistleblowers' prime target under the FCA. Furthermore, cyberattacks across the healthcare industry have been on the rise, and the issue has attracted the attention of both OIG and FDA.

Last summer, OIG completed a review of the extent to which CMS and its contracted accrediting organizations impose and police cybersecurity standards for hospital networked devices, which include devices that monitor patient activity or obtain and communicate imaging.¹⁴ In the report, OIG noted that the conditions of participation applicable to hospitals are silent as to cybersecurity obligations, and OIG urged CMS "to address cybersecurity of networked medical devices in its quality oversight of hospitals." However, CMS would commit only to "considering additional ways to appropriately highlight the importance of cybersecurity of networked medical devices for providers in consultation with its HHS partners that have specific oversight authority regarding cybersecurity." It is not uncommon for DOJ, either directly or through *qui tam* suits, to prioritize for enforcement areas in which it believes HHS is failing to provide adequate supervision, and the Civil Cyber-Fraud Initiative provides a ready vehicle for targeting cybersecurity at hospitals.

In addition, last year FDA initiated medical device recalls and alerts based on cybersecurity flaws and released a discussion paper titled "Strengthening Cybersecurity Practices Associated with Servicing of Medical Devices: Challenges and Opportunities" that solicited comments from stakeholders about cybersecurity issues unique to medical devices.¹⁵ Life sciences companies should stay apprised of FDA guidance in this space and take steps to control cybersecurity risks. While FDA recognized in its discussion paper that "it is not possible to completely eliminate all cybersecurity vulnerabilities from medical devices," this acknowledgment will not stop whistleblowers and the government from applying 20/20 hindsight to cybersecurity incidents.

¹Press Release, Cal. Dep't of Justice, California State Assembly Advances AG-Sponsored Legislation to Strengthen the False Claims Act and Protect California Taxpayers from Fraud (June 10, 2020), available at <https://oag.ca.gov/news/press-releases/california-state-assembly-advances-ag-sponsored-legislation-strengthen-false>.

²HHS-OIG, Audits of Medicare Part B Telehealth Services During the COVID-19 Public Health Emergency, <https://oig.hhs.gov/reports-and-publications/workplan/summary/wp-summary-0000556.asp>.

³<https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/09/fact-sheet-executive-order-on-promoting-competition-in-the-american-economy/>

⁴Press Release, DOJ, Pharmaceutical Companies Pay Over \$400 Million to Resolve Alleged False Claims Act Liability for Price-Fixing of Generic Drugs (Oct. 1, 2021), <https://www.justice.gov/opa/pr/pharmaceutical-companies-pay-over-400-million-resolve-alleged-false-claims-act-liability>

⁵OIG, Adv. Op. No. 21-18 (Nov. 17, 2021), <https://oig.hhs.gov/compliance/advisory-opinions/21-18/>.

⁶<https://www.cms.gov/CCIIO/Programs-and-Initiatives/Other-Insurance-Protections/CAA>.

⁷<https://www.cms.gov/nosurprises/consumers/complaints-about-medical-billing>.

⁸86 Fed. Reg. 41,383 (August 2, 2021).

⁹85 Fed. Reg. 76,666 (Nov. 30, 2020).

¹⁰Press Release, DOJ, AutoGenomics, Inc. Agrees to Pay Over \$2.5 Million for Allegedly Paying Kickbacks (Jan. 11, 2021), <https://www.justice.gov/usao-wdwi/pr/autogenomics-inc-agrees-pay-over-25-million-allegedly-paying-kickbacks>.

¹¹Press Release, DOJ, Seven Texas Doctors and a Hospital CEO Agree to Pay over \$1.1 Million to

Settle Kickback Allegations (Jan. 20, 2022), <https://www.justice.gov/usao-edtx/pr/seven-texas-doctors-and-hospital-ceo-agree-pay-over-11-million-settle-kickback>.

¹²Press Release, DOJ, Kaléo Inc. Agrees to Pay \$12.7 Million to Resolve Allegations of False Claims for Anti-Overdose Drug (Nov. 9, 2021), <https://www.justice.gov/opa/pr/kal-o-inc-agrees-pay-127-million-resolve-allegations-false-claims-anti-overdose-drug>.

¹³Press Release, DOJ, Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative (Oct. 6, 2021), <https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative>.

¹⁴HHS-OIG, Medicare Lacks Consistent Oversight of Cybersecurity for Networked Medical Devices in Hospitals (June 2021), <https://oig.hhs.gov/oei/reports/OEI-01-20-00220.pdf>.

¹⁵https://www.fda.gov/medical-devices/quality-and-compliance-medical-devices/discussion-paper-strengthening-cybersecurity-practices-associated-servicing-medical-devices?utm_medium=email&utm_source=govdelivery.

CONTACTS

Jaime L.M. Jones , Partner	+1 312 853 0751, jaime.jones@sidley.com
Raj D. Pai , Partner	+1 202 736 8089, rpai@sidley.com
Matt Bergs , Senior Managing Associate	+1 312 853 9443, mbergs@sidley.com

Attorney Advertising—Sidley Austin LLP is a global law firm. Our addresses and contact information can be found at www.sidley.com/en/locations/offices.

Sidley provides this information as a service to clients and other friends for educational purposes only. It should not be construed or relied on as legal advice or to create a lawyer-client relationship. Readers should not act upon this information without seeking advice from professional advisers. Sidley and Sidley Austin refer to Sidley Austin LLP and affiliated partnerships as explained at www.sidley.com/disclaimer.

© Sidley Austin LLP