November 2023

Skadden

# The Nucleus: Life Sciences Enforcement and Regulatory Updates

**In this issue:**



## Increased Focus on Cybersecurity Could Pose False Claims Act Exposure Risk for Life Sciences Companies

The False Claims Act (FCA) remains a familiar tool for litigants seeking to pursue civil liability against life sciences companies. The past decade has seen continued deployment of the FCA in the life sciences space under common theories such as causation of medically unnecessary claims, sales of defective products and so-called "fraud on the FDA" (Food and Drug Administration) theory. There can be little doubt that the Department of Justice (DOJ) and the relators' bar will continue to pursue and explore cases based on these theories of liability in the years to come.

The recent FDA and DOJ focus on cybersecurity issues, however, suggests the possibility of new theories of FCA liability, arising at the intersection of already established theories and concerns about cyberfraud. Life sciences companies should be aware of that intersection and take steps to minimize their exposure to potential FCA risk by evaluating their cybersecurity risks and implementing appropriate controls.

### DOJ and FDA Focus on Cybersecurity

In October 2021, Deputy Attorney General Lisa Monaco announced DOJ's launch of its Civil Cyber-Fraud Initiative. The Civil Division's Commercial Litigation Branch, which is responsible for evaluating and prosecuting FCA cases, leads this initiative. To date, DOJ has announced three resolutions of cases brought as part of the initiative, two of which relate to the cybersecurity of health information:

- In two cases brought by the U.S. Attorney's Office for the Eastern District of New York, DOJ alleged that Comprehensive Health Services LLC (CHS) submitted false claims to the State Department for payment for its secure electronic medical record (EMR) system for military, civilian and contractor personnel operating in Iraq. DOJ alleged that CHS failed to disclose to the State Department that it did not consistently store patients' medical records securely, at times saving scanned copies of EMR to a network drive that was accessible to nonclinical staff. In March 2022, CHS paid $930,000 to resolve the matter.

- In March 2023, Jelly Bean Communications Design LLC reached a settlement with DOJ resolving allegations that it submitted false invoices to a Medicaid-funded state-administered children's health and dental insurance program over the course of multiple years in which Jelly Bean designed, programmed and hosted the program's website and online application portal. DOJ alleged that, contrary to various representations Jelly Bean made throughout its contractual relationship with the program, the company failed to maintain updated and fully patched software supporting the website. DOJ alleged that this failure exposed patient data to vulnerability and, in at least one instance, a cyberattack that accessed over 500,000 patients' application data. Jelly Bean paid $293,000 to resolve the matter.

FDA's eye also is trained on cybersecurity. Our prior issue of *The Nucleus* discussed the Food and Drug Omnibus Reform Act (FDORA), enacted in late December 2022. Among other provisions we explore there, FDORA added the term "cyber devices" to the Food, Drug and Cosmetic Act (FDCA) and subjected those devices to specific regulation and enforcement mechanisms.

Pursuant to FDORA, a "cyber device" is a medical device that "(1) includes software validated, installed, or authorized by the sponsor as a device or in a device; (2) has the ability to connect to the internet; and (3) contains any such technological characteristics validated, installed, or authorized by the sponsor that could be vulnerable to cybersecurity threats."

Manufacturers seeking clearance or approval of cyber devices must:

- File a premarket submission that addresses cybersecurity concerns, including a "software bill of materials" (SBOM) and a plan to address cybersecurity vulnerabilities.
- Implement processes and procedures, including post-market updates and patches, that provide "reasonable assurance" that the device and any "related systems" are and remain "cybersecure."

FDORA directs that a failure to comply with these requirements is a prohibited act under the FDCA. As discussed below in "Final Guidance on Cybersecurity Considerations in Premarket Submissions for Medical Devices," FDA has issued final guidance regarding cybersecurity requirements in the premarket submission and has indicated that it will refuse to accept applications that do not comply with those requirements. These new FDA requirements, coupled with DOJ's cyber-fraud focus, suggest that FCA theories traditionally used in life sciences cases could soon be used to pursue cybersecurity-based FCA liability.

## Historic Theories of FCA Liability Against Life Sciences Companies

Three theories of FCA liability, among others, have recurred over the past decade of litigation in the life sciences sector.

### Fraud on the FDA

The theory of "fraud on the FDA" derives from common law fraudulent inducement theories, which courts have applied to the FCA in other contexts. Under this theory, a plaintiff claims that a manufacturer made materially false statements or omissions in its submissions to FDA to obtain approval or clearance to market and sell its product. The theory contends that all claims for reimbursement made to federal payors thereafter are false, because the product would not be on the market at all but for the alleged fraud in the manufacturer's original application materials.

Federal courts have given this theory a mixed reception. For instance:

- The U.S. Court of Appeals for the First Circuit rejected this theory in *U.S. ex rel. D'Agostino v. ev3, Inc*., 845 F.3d 1 (1st Cir. 2016), holding that no causal link connected the defendant's alleged false statements to the FDA and federal payors' later payment of the defendant's claims.
- However, the U.S. Court of Appeals for the Ninth Circuit has accepted "fraud on the FDA" theories in two instances.
  - In *U.S. ex rel. Campie v. Gilead Sciences, Inc*., 862 F.3d 890 (9th Cir. 2017), the court reversed a dismissal of an FCA complaint that alleged that a drug manufacturer failed to notify FDA of a change in active ingredient manufacturers, hid the change from FDA and used active ingredient from the unapproved manufacturer in its product.
  - In *U.S. ex rel. Dan Abrams Co. v. Medtronic Inc.*, 850 F. App'x 508 (9th Cir. 2021), the court permitted the theory to proceed only as to a manufacturer's products that, but for the allegedly fraudulently obtained approval, would have had no other medical use on the market.

DOJ recently expressed support for this theory, stating that in its view, FCA liability lies where, among other circumstances, FDA "never would have approved or cleared the affected products — or allowed them to remain on the market — if it had known the truth, and claims involving those devices never would have been eligible for federal healthcare program reimbursement[,]" as well as where "materially false or fraudulent statements [are] made to FDA regarding drugs or medical devices" during or after the FDA approval process. *United States ex rel. Crocano v. Trividia Health Inc*., No. 0:22-cv-60160 (S.D. Fla.), ECF No. 124 at 5–6 (June 3, 2022).[1]

### Sales of Defective Products

In this scenario, a plaintiff does not take issue with a product's approval by FDA but alleges that a manufacturer knowingly requests reimbursement from federal payors for products that in fact are materially defective, or that otherwise materially deviate from their approved specifications. These allegations mirror paradigm FCA product defect actions in other industries in which plaintiffs allege that defendants sell materially deficient goods or services to the government.

As we have discussed elsewhere, this theory has provided fertile ground for numerous recent resolutions of FCA matters. For example:[2]

- In July 2021, medical device manufacturers Alere Inc. and Alere San Diego Inc. paid $38.75 million to settle allegations that their blood coagulation monitors contained a software error that produced inaccurate results for some patients. The settlement followed a separate settlement against the two manufacturers in August 2018 in *United States ex rel. Wu v. Alere San Diego, Inc*., No. 1:11-cv-01808 (D. Md.), in which the Alere entities paid $33.2 million to settle allegations that some of their rapid point-of-care testing devices produced erroneous results that affected clinical decision-making.

[1] For additional discussion of this theory, see our November 2022 article in *Bloomberg Law*, "Circuit Split Doesn't Slow DOJ False Claims Act Settlements Based on FDCA Allegations."

[2] For more on recent resolutions involving alleged post-marketing failures to comply with the FDCA, see "Circuit Split Doesn't Slow DOJ False Claims Act Settlements Based on FDCA Allegations."

- In a resolution with the U.S. Attorney's Office for the Eastern District of New York, AmerisourceBergen Corp. and several of its subsidiaries collectively paid $625 million in October 2018 to settle allegations that they provided pre-filled syringes for several of their injectable cancer drugs by breaking the sterility of other manufacturers' products, pooling their contents at unapproved and sometimes nonsterile facilities, and repackaging them under the companies' own labeling.
- In *United States ex rel. Wall v. Baxter International, Inc*., No. 1:13-cv-00042 (W.D.N.C.), a pharmaceutical manufacturer executed a deferred prosecution agreement and civil settlement in which it agreed to pay a total of $18 million to resolve charges and allegations that its sterile intravenous solutions were adulterated because the air at the facility at which they were manufactured was continuously forced through a moldy particulate filter, in violation of FDA Current Good Manufacturing Practices.

### Causation of Medically Unnecessary Claims

This well-worn theory involves a product that is properly approved and not subject to any alleged defects, but as to which a plaintiff alleges the manufacturer causes the submission of claims for a medically unnecessary use. Because medical necessity is required for reimbursement by federal payors, this theory alleges that the claims caused by the manufacturer's conduct are false. As recent settlements have demonstrated, medical necessity theories can sustain sizeable claims for damages. For example:

- In *United States ex rel. Johnson v. Therakos, Inc*., No. 2:12-cv-01454 (E.D. Pa.), DOJ alleged that a manufacturer promoted its extracorporeal photopheresis treatment system for use with pediatric patients, which DOJ alleged was not a population in which FDA had approved those systems for use. The manufacturer's former owners settled the matter in November 2020 for a combined $11.5 million.
- In *United States ex rel. Chung v. DUSA Pharmaceuticals, Inc*., No. 2:16-cv-01614 (W.D. Wash.), DOJ alleged that a pharmaceutical company encouraged physicians who administered its skin lesion treatment drug to patients to use a shorter incubation period than FDA-approved instructions indicated, which DOJ alleged was unsupported by clinical evidence and reduced the drug's effectiveness. The company settled the matter in August 2020 for $20.75 million.

**DOJ has clearly signaled its intention to use the FCA as a tool to combat cybersecurity-related fraud and has been quick to pursue that approach in the health care sector.**

## Potential Implications for FCA Liability Based on Cybersecurity Issues

DOJ has clearly signaled its intention to use the FCA as a tool to combat cybersecurity-related fraud and has been quick to pursue that approach in the health care sector. As discussed above, FDA, meanwhile, is implementing requirements to ensure that device manufacturers consider and confront cybersecurity vulnerabilities in their products. These efforts may converge in the future in new theories of FCA liability. The first cases resolved in DOJ's Civil Cyber-Fraud Initiative may provide a road map to some of these potential developments.

Consider the CHS cases, in which DOJ alleged that the defendant made misrepresentations about the secure storage of patient data. In the FDA context, a plaintiff might assert that a manufacturer made similar misstatements about the cybersecurity of its cyber devices in its premarket submissions to FDA. This, in turn, could support a "fraud on the FDA" theory that FDA would never have cleared or approved the subject device if it had known the true cybersecurity vulnerabilities of the product.

Alternatively, the Jelly Bean case could suggest a new form of product defect theory. Similar to Jelly Bean's alleged concealment of its failure to keep its products reasonably up-to-date over time, a plaintiff might allege that a defendant's actual cyber device does not meet the specifications listed in its SBOM or cybersecurity plan submitted to FDA, or that a defendant failed to patch known cybersecurity vulnerabilities. This could support a theory that these deficiencies constitute material defects in the product, rendering the product inappropriate for reimbursement by federal payors and claims for the product correspondingly false.

These examples focus primarily on device manufacturers, because FDORA's new provisions relate to devices, but others in the life sciences sector may also be affected by new theories like these. For example, pharmaceutical manufacturers that develop software or apps that may be subject to regulation as medical devices may now be subject to further scrutiny as cyber devices, and manufacturers of lab-developed tests may face future compliance requirements to the extent that those products become subject to regulation as medical devices.

And, as the Civil Cyber-Fraud Initiative has already demonstrated, companies that manufacture EMR, electronic health records, or any similar systems sold to or used by the federal government are subject to potential enforcement action pursuant to the FCA.

**Pharmaceutical manufacturers that develop software or apps that may be subject to regulation as medical devices may now be subject to further scrutiny as cyber devices.**

## Practical Considerations for Life Sciences Companies

While we have yet to see the application of these potential FCA theories, it seems likely that they are on the horizon. As such, life sciences companies should consider assessing, and taking steps to implement controls that may help mitigate against, their potential exposure to these theories. For example, life sciences companies should consider:

- Assessing the extent to which their current and potential future product offerings — as well as their storage mechanisms for health-related data such as clinical trial and patient support program data — involve actual or potential cybersecurity risks.
- Undertaking comprehensive cross-functional assessments of those risks and implementing governance mechanisms to ensure potential vulnerabilities are evaluated and appropriately controlled for, actual or potential data breaches are promptly identified, and that such actual or potential breaches are addressed and reported as required under applicable regulations.
- Paying close attention to any representations — to FDA as well as to potential customers — regarding the cybersecurity of products and services, and retaining contemporaneous documentation that supports the accuracy of those representations.
- Staying abreast of cybersecurity regulatory developments and ensuring that company policies and procedures continue to meet regulatory requirements and industry best practices.

---


**Maya P. Florence**, **William Ridgway** and **John A.J. Barkmeyer**

# FDA Enforcement

## Promotional Enforcement Update

We have long kept tabs on activities by FDA's Office of Prescription Drug Promotion (OPDP) — both the warning and untitled letters it issues and the guidance documents it produces. For life sciences companies, these communications provide a helpful sense of FDA's priorities when it comes to the important topic of promotional communications.

However, there has been little to track in the past couple of years. OPDP issued only four letters in 2022 (one warning letter and three untitled letters) and none through the first five months of 2023. Activity picked up in June 2023, with OPDP since issuing one warning letter and two untitled letters relating to drug promotional activity.

Perhaps the most important takeaway from this burst of enforcement activity is that FDA appears to be focusing on situations where it believes companies are making unsupported efficacy claims. This reflects a departure from FDA's 2018 comments that it was intending to allow companies to "duke it out" when it came to efficacy claims that did not involve risks to human safety.

### Warning Letter: First Since February 2022

In its August 4, 2023, warning letter, FDA raised concerns about a brochure that OPDP asserted contained false or misleading efficacy claims. Most notably, OPDP took issue with a claim — "DIFFERENCE OBSERVED IN TIME TO ALL-CAUSE MORTALITY (OVER 52 WEEKS)" in chronic obstructive pulmonary disease (COPD) patients — that was based on a secondary endpoint from a study where the drug had failed to meet the primary endpoint.

FDA asserted that because the trial had failed to meet the primary endpoint, it was improper to make claims based on any secondary endpoints that might have been reached. FDA acknowledged that the promotional brochure contained the disclaimer, "These results are observational in nature, and any comparisons between treatment arms should be interpreted with caution." Nevertheless, FDA stated that the disclaimer did not mitigate the misleading impression and emphasized that, to date, no drug has been shown to improve all-cause mortality in COPD.

OPDP also took issue with claims that the same study showed a "significant reduction in severe exacerbations," asserting that the reduction in severe exacerbations was not statistically significant relative to comparator groups. Here again, FDA acknowledged that the promotional brochure included caveats in a footnote, but indicated that it did not correct the misleading impression made by the bolded statements in the piece.

As is often its practice when issuing a warning letter, OPDP requested that the company undertake corrective actions, including undertaking corrective communications.

### 2023 Untitled Letters: Internet Promotional Materials

In a June 2023 untitled letter, FDA took issue with claims made on the consumer page of a company's website, which had been submitted to FDA via 2253. According to FDA, the promotional communications created a misleading impression regarding the safety and effectiveness of the drug, which in fact has a number of serious and potentially life-threatening risks, including a boxed warning regarding its risks.

OPDP identified concerns with multiple claims on the website, including a claim that "67% of patients who moved on to the second part of the study had normal cortisol levels by the end of the study." According to FDA, this misleadingly overstated the drug's efficacy because although 67% of patients in the study had normal cortisol levels at the end of the titration phase, the titration phase was not the "end of the study." According to OPDP, suggesting that 67% of patients who "moved on to the second part of the study" had normal cortisol levels by the end of the study significantly overstates the efficacy of the product.

OPDP also claimed that the website omitted material information necessary for consumers to interpret the study. OPDP pointed to the "CLINICAL STUDIES" section of the drug's package insert, which states, "[b]ecause 51% of patients discontinued treatment prematurely due to adverse reaction, lack of efficacy, or other reasons, these results should be interpreted with caution." This information was not included on the company's website, and FDA asserted that the omission undermined the ability of the reader to understand and evaluate the study results presented, thereby creating a misleading impression about the drug's efficacy.

FDA issued a close-out letter on August 9, 2023, which represents a prompt resolution to this misstep for the company.[3]

The second untitled letter of 2023, issued on August 11, 2023, took issue with promotional material posted on social media regarding an oral contraceptive. OPDP asserted that the post had multiple infirmities, including making misrepresentations regarding the drug's efficacy and its risks. OPDP also pointed out that the material was not submitted to FDA at the time of initial dissemination or publication as required by 21 CFR 314.81(b)(3)(i). With respect to efficacy, the social media post claimed the ability to "[o]ffer your patients estrogen-free birth control with periods on a schedule." According to OPDP, this claim is misleading because it overstates the drug's efficacy by claiming patients will have predictable menstrual bleeding that is "on a schedule" when this has not been demonstrated.

**OPDP appears to be more actively monitoring promotional communication and has restarted "throwing the flag" when it believes there are inappropriate efficacy claims.**

With respect to risks, FDA asserts that while the post presents claims and representations about the benefits of the drug, it fails to communicate any risk information. According to FDA, failing to include any risk information creates a misleading impression about the drug's expected benefits and safety.

As corrective actions, FDA requested that the company submit a written response to the untitled letter within 15 working days from the date of receipt:

- addressing the concerns described in the letter;
- listing all other promotional communications (with the 2253 submission date) for the drug that contain representations such as those described in the letter; and
- explaining any plan for discontinuing use of such communications or for ceasing distribution of the drug.

As these three letters reflect, OPDP appears to be more actively monitoring promotional communication and has restarted "throwing the flag" when it believes there are inappropriate efficacy claims. We recommend that companies continue to make it a regular practice to review OPDP's warning and untitled letters, in addition to their guidance documents, in order to ensure that they are applying appropriate standards as part of their materials review processes.

[3] FDA may issue a close-out letter once the agency has completed an evaluation of corrective actions undertaken and has determined that the company in question has addressed the violations contained in the letter.

## FDA Issues Spate of Warning Letters Arising Out of Inspection Activities

In addition to the recent flurry of OPDP enforcement based on promotional activity, the past few months have also seen continued enforcement arising out of inspection-related activities.

### Warning Letter to iRhythm Technologies, Inc.

In June 2023, FDA's Center for Devices and Radiological Health (CDRH) released a warning letter issued to iRhythm Technologies, Inc. based on an inspection conducted in May 2022. The warning letter asserted that the company marketed its cardiac monitoring system for uses not covered by the cleared 510(k). More specifically, FDA explained that the relevant monitoring device was cleared "for long-term monitoring of arrhythmia events for non-critical care patients where real-time monitoring is not needed as reporting timeliness is not consistent with life-threatening arrhythmias," but marketing materials indicated that the device was intended for "'near real-time monitoring' as a 'mobile cardiac telemetry monitor,' [that] can provide notifications 'immediately,' and that it is intended for 'high-risk patients.'"

**FDA asserted that "this change could significantly affect the safety or effectiveness of the device because it suggests that the device is intended for a new patient population — high-risk patients," and therefore required submission of a new 510(k).**

FDA asserted that "this change could significantly affect the safety or effectiveness of the device because it suggests that the device is intended for a new patient population — high-risk patients," and therefore required submission of a new 510(k).

Separately, the warning letter asserted that the company's cardiac monitoring system was misbranded because it did not bear adequate directions for use for the physician related to transmission limits. To this end, FDA stated that the labeling did not identify that there was a limit on the number of arrhythmia events for which the system could transmit data, nor did it notify the patient when that limit was reached or indicate what to do about it. These aspects of the warning letter are particularly notable, as they involve the type of alleged violations often identified in OPDP warning letters but instead arise out of a facility inspection.

In addition to these promotion- and labeling-related findings, the warning letter also cited a number of additional deficiencies, of the types more frequently identified through inspections. These include:

- That the firm made hardware and firmware changes to its cleared device that also could affect its safety or effectiveness, and therefore required submission of a new 510(k).
- Failures to adequately establish and maintain procedures for implementing corrective and preventive action (CAPA).
- Failure to conduct a health hazard evaluation as required by the company's CAPA procedure.
- Failure to adequately establish procedures for receiving, reviewing and evaluating complaints by a formally designated unit.
- Various failures to file required medical device reports (MDRs).
- Failures to develop, implement and maintain written procedures relating to MDR reporting.

### Warning Letters Arising Out of Remote Regulatory Assessments

In August and September 2023, FDA issued a total of 15 warning letters to foreign facilities registered as over-the-counter (OTC) drug manufacturers arising out of requests for records issued under Section 704(a)(4) of the FDCA. Section 704(a)(4) authorizes FDA to request that any records relating to drug products that FDA would otherwise be authorized to inspect be provided to FDA remotely "in advance of or in lieu of an inspection."

FDA issued its first warning letter arising out of a remote regulatory assessment in January 2021. It issued another 12 such warning letters in 2021, followed by six more in 2022. To date in 2023, FDA has issued 23 such warning letters: 22 to OTC drug manufacturers and one to a manufacturer of active pharmaceutical ingredients. The majority of these manufacturers are located overseas. All of these 2023 warning letters assert either cGMP violations identified through the records reviewed or a failure to provide records in response to FDA's request. For the foreign firms receiving letters, this failure resulted in the firms being placed on FDA import alerts.

The notable uptick in 2023 in warning letters arising out of remote regulatory assessments likely follows from FDA's substantially increased use of the tool during the COVID-19 pandemic, when FDA found itself unable to conduct physical inspections. (FDA has had the authority to make remote records requests since 2012 but, as noted above, did not issue a warning letter based on such a request until 2021.)

While the warning letters issued to date generally appear to be directed to foreign manufacturers — and largely to OTC drug firms — FDA's authority to request records under Section 704(a)(4) extends to all establishments that engage in the manufacture, preparation, propagation, compounding or processing of a drug. As such, all drug manufacturers should be aware of this development and ensure that any Section 704(a)(4) requests are promptly and appropriately responded to, as it is clear they may give rise to enforcement in the same manner as physical inspections.

## Another Loss on Statutory Interpretation

Over the last 24 months, FDA has lost a number of cases in court — an atypical record for an agency that has historically benefited from judicial deference to its scientific expertise. Many of these cases, especially those in the tobacco vaping space, have held that FDA misapplied statutory standards in the premarket review context. Others, like *Catalyst Pharmaceuticals, Inc. v. Becerra*, 14 F.4th 1299 (11th Cir. 2021), which evaluated the orphan drug provisions of the FDCA, have held that FDA's actions have in some cases exceeded its statutory authority.

The mifepristone lawsuit in the U.S. Court of Appeals for the Fifth Circuit, *Alliance for Hippocratic Medicine v. FDA*, 78 F.4th 210 (5th Cir. 2023) — which stands alone for many reasons — is a mix of these, alleging FDA both misapplied the law and acted outside its statutory authority in rendering regulatory decisions.

In July 2023, FDA encountered another judicial setback in *United States v. Vepuri*, 74 F.4th 141 (3d. Cir. 2023), losing an appeal of a count in a criminal case on the grounds that the text of the FDCA did not support its cause of action.

The case arises from a 2019 government investigation into KVK-Tech, Inc., a generic drug manufacturer, over its distribution of the sedative drug hydroxyzine hydrochloride. In 2021, the government charged the company — as well as its de facto director, Murty Vepuri, and its director of quality, Ashvin Panchal — in a two-count indictment. The indictment charged KVK with one count of mail fraud under 18 U.S.C. Section 1341 and all three defendants with one count of conspiracy to defraud and commit offenses against the United States under 18 U.S.C. Section 371.

The conspiracy charge involved three alleged objects:

- Defrauding the government by impeding the lawful function of the FDA.
- Introducing "unapproved new drugs" into interstate commerce with the intent to defraud or mislead.
- Making false statements to FDA.

The charges stemmed from allegations that the defendants had sourced the active pharmaceutical ingredient (API) for the hydroxyzine from a facility that was not included in the abbreviated new drug application (ANDA) for their product and lied about it to the government. The government asserted that use of API from a source that had not been sanctioned by FDA in the ANDA rendered the finished products containing that API "unapproved new drugs" within the meaning of the FDCA, the approval of the ANDA notwithstanding.

The charge was grounded in FDA's long-standing policy that drugs that deviate from their respective new drug application (NDA) or ANDA approval are unapproved new drugs, and therefore illegal.

The defendants moved to dismiss the indictment on several grounds, and the district court granted the motion in part, dismissing the conspiracy count as to the unapproved new drug charge. The court parsed the language of the FDCA and concluded that the mere existence of a deviation from the ANDA does not make a drug an unapproved new drug. Rather, the court focused on the specific definition of "new drug" in the FDCA and explained that the statute defines the term by the product's composition and labeling, not the manner or place of its manufacture.

The court reasoned that, so long as the API used in the finished product had the same composition as the API approved in the ANDA, the product did not differ from the ANDA for purposes of the criminal charge. The court also explained that FDA had other remedies available to it to address concerns about drug quality, including adulteration charges and withdrawal of the ANDA under Section 505(e) of the FDCA.

The government appealed the district court opinion, but the U.S. Court of Appeals for the Third Circuit affirmed. Like the district court, the Court of Appeals engaged in a strict textual analysis and concluded that the language in the FDCA (or at least the language charged in the indictment) did not support the government's cause of action on the unapproved drug charge. "Because the Hydroxyzine at issue has the same composition and labeling as the Hydroxyzine for which an approval of an ANDA is effective," said the court, "the Government cannot rely in this case upon the premise that the two drugs are different."

In support of their holdings, both the district court and Court of Appeals invoked a 1970 precedent, *United States v Kaybel*, 430 F.2d 1346 (3d Cir. 1970), in which the Third Circuit rejected the government's argument that a company needs a separate NDA approval to repackage drugs manufactured by another company in compliance with that manufacturer's NDA. The court in *Kaybel* refused to accept that the repackaged drug was different from the "new drug" for which the company had already obtained approval.

The Court of Appeals in *Vepuri* cited the reasoning with favor and distinguished a 2007 U.S. Court of Appeals for the Seventh Circuit holding, *United States v. Genendo Pharmaceutical, N.V.*, 485 F.3d 958 (7th Cir. 2007), on the grounds that neither party in that case ever contested the assumption that a drug becomes an unapproved new drug when an NDA or ANDA is not followed exactly as written. Like the district court, the Court of Appeals also reasoned that FDA had other remedies under the FDCA to address its concerns about the API.

Portions of the indictment still survived the motion to dismiss, including the wire fraud charge and aspects of the conspiracy charge relating to false statements and impeding the lawful functions of FDA. Notably, the conspiracy charge still includes the allegation that the defendants were required to notify FDA about the new source of API as a "major manufacturing change" under Section 506A of the FDCA. The upshot is that FDA and DOJ still have myriad tools to enforce the FDCA when they believe that the quality of drugs is compromised or that applicants are deceiving the government or consumers.

**But the holding on the definition of "unapproved new drug" is significant in that it squarely rejects a long-standing FDA position based on a textual analysis of the FDCA.**

But the holding on the definition of "unapproved new drug" is significant in that it squarely rejects a long-standing FDA position based on a textual analysis of the FDCA. The Court of Appeals acknowledged that differences in labeling or composition could well render a drug unapproved, but it was not willing to assume that two drugs with the same composition were different for purposes of the criminal charge in the absence of explicit statutory support for the argument.

## Implications

This analysis could potentially impact the drug importation battle, where FDA has long relied on technical legal arguments under the FDCA and its implementing regulations to support its position that foreign versions of drugs made by the same manufacturer are illegal in the United States, even when they are chemically identical. To be sure, FDA's legal arguments in the importation context extend well beyond the unapproved new drug charge, but this holding strikes at the powerful notion that any failure to comply with any detail of an approved product application renders a product illegal.

We expect the government to seek *certiorari* on the *Vepuri* decision given its importance, but we recognize also that government concerns of the U.S. Supreme Court rejecting its argument may be a reason to cut losses. FDA has ample authority to fashion charges in drug cases, and we expect FDA may plead actions differently in the future to vindicate its interests in cases like this. Still, the loss is a reminder that, as courts devote ever more energy to parsing statutes, long-held assumptions about the scope of FDA's authority are poised for a fresh look.

# FDA Regulatory

## Long-Awaited Proposed Rule To Regulate Laboratory-Developed Tests Issued

On September 29, 2023, the FDA issued a proposed rule that would end its long-standing policy of enforcement discretion with respect to regulation of laboratory-developed tests (LDTs) (the Proposed Rule).[4] Under the Proposed Rule, FDA would add language to the definition of "in vitro diagnostic products" (IVDs) in 21 CFR Part 809.3(a) stating that IVDs are considered devices under the FDCA, "including when the manufacturer of these products is a laboratory."

Recognizing that treating LDTs as IVDs subject to regulation as medical devices will have profound impacts on clinical laboratories offering LDTs, the Proposed Rule provides for a phased end to FDA's policy of enforcement discretion with respect to LDTs. Under this approach, LDT manufacturers will be required to comply with various medical device regulatory requirements in stages beginning between one and four years after FDA publishes the final LDT rule, the preamble of which will include FDA's final policy regarding this "phaseout" process.

While it is therefore unclear when these regulatory requirements ultimately would become effective, laboratories offering LDTs should be aware of and continue to track developments relating to the Proposed Rule, particularly as it does not propose to "grandfather" any LDTs currently on the market.

### Background on LDT Regulation

FDA regulations define IVDs as "reagents, instruments, and systems intended for use in the diagnosis of disease or other conditions, including a determination of the state of health, in order to cure, mitigate, treat, or prevent disease or its sequelae and intended for use in the collection, preparation, and examination of specimens taken from the human body."

IVDs are medical devices, subject to the full range of premarket and postmarket controls, including requirements pertaining to:

- 510(k) premarket notification or premarket approval (PMA).
- Quality system (QS) regulation.
- Medical device reporting (MDR).
- Registration and listing.
- Labeling.

In addition, IVDs are also generally subject to regulation under the Clinical Laboratory Improvement Amendments of 1988 (CLIA).

LDTs are a subset of IVDs that are designed, manufactured and used within a single laboratory (*i.e.*, a clinical lab with a single CLIA certificate). Although FDA historically has maintained that it has the authority to regulate LDTs as medical devices, it generally has not enforced premarket review and other medical device regulatory requirements for LDTs. This policy of enforcement discretion arose because LDTs historically were perceived as low-risk due to their use in limited volumes primarily in rare diseases and generally with interpretation by a treating physician.

[4] The Proposed Rule was published in the Federal Register on October 3, 2023.

However, as FDA describes in the Proposed Rule, over the past 50 years, LDTs have become "used more widely, by a more diverse population, with an increasing reliance on high-tech instrumentation and software, and more frequently for the purpose of guiding critical healthcare decisions." The Proposed Rule therefore asserts that "today's LDTs are similar to other IVDs that have not been [subject to the Agency's] general enforcement discretion approach," such that "phasing out the general enforcement discretion approach for LDTs is important to protect the public health." For purposes of the rule, FDA is defining LDT broadly, asserting that many manufacturers of high complexity tests have cloaked themselves as LDT manufacturers when their tests do not technically qualify as such.

The Proposed Rule is not FDA's first attempt at regulating LDTs. Since at least 2006, both FDA and Congress have repeatedly revisited the approach to regulating LDTs. Congress has never taken action, while FDA has issued draft guidances asserting an intent to require premarket review of LDTs before reconsidering in response to strong pushback. Responses to FDA's proposals questioned whether LDTs are, in fact, subject to FDA jurisdiction, whether additional regulation is appropriate in light of CLIA's application to LDTs and whether additional regulation by FDA would inhibit innovation and restrict patient access.

In 2017, FDA published a white paper proposing enhanced medical device regulatory oversight and invited Congress to take up the issue. The Verifying Accurate, Leading-Edge IVCT Development (VALID) Act has been introduced in the past few Congresses and was expected to be included in the omnibus bill passed at the end of 2022 but ultimately stalled. Against this backdrop, earlier this year, the Biden administration announced that it would undertake LDT rulemaking, leaving industry observers watching closely for the release of the Proposed Rule.

**The Proposed Rule provides that FDA will phase out its general enforcement discretion policy with regard to LDTs in five stages over a four-year period.**

## Summary of Proposed Rule

As noted above, the actual changes included in the Proposed Rule are minimal, amounting to the addition of 10 words to the IVD definition, but the potential impacts of this change are significant. In recognition of this impact, and of industry comments received in response to past regulatory attempts, the Proposed Rule provides that FDA will phase out its general enforcement discretion policy with regard to LDTs in five stages over a four-year period:[5]

1. One year after FDA publishes a final phaseout policy in the preamble of the final rule, enforcement discretion would end with respect to both MDR and correction and removal reporting requirements.
2. Two years after publication of the final phaseout policy, enforcement discretion would end with respect to requirements other than MDR, correction and removal reporting, QS, and premarket review. At this stage, LDTs would be required to comply with FDA requirements relating to registration and listing, labeling, and investigational device exemptions.
3. Three years after publication of the final phaseout policy, enforcement discretion would end as to QS requirements (good manufacturing practice requirements applicable to medical devices).

[5] FDA proposes to apply this "phaseout policy to IVDs that are manufactured and offered as LDTs by laboratories that are certified under CLIA and that meet the regulatory requirements under CLIA to perform high complexity testing, even if those IVDs do not fall within FDA's traditional understanding of an LDT because they are not designed, manufactured, and used within a single laboratory."

4. Three and a half years after publication of the final phaseout policy (but not before October 1, 2027), enforcement discretion would end with respect to premarket review requirements for high-risk IVDs. At this point, Class III LDTs would be subject to full PMA requirements under the FDCA.
5. Finally, four years after publication of a final phaseout policy (but not before April 1, 2028), enforcement discretion would end with respect to premarket review requirements for moderate-risk and low-risk IVDs that require premarket review under applicable regulations. At this point, Class II LDTs (and those Class I LDTs requiring premarket review) would be subject to the full 510(k) premarket notification and *de novo* requirements under the FDCA. The Proposed Rule states that FDA generally would not intend to enforce against LDTs for which 510(k)s and *de novo* applications are submitted in the four-year time frame until FDA's review of the submission is completed.

FDA asserts in the Proposed Rule that "the phaseout of FDA's general enforcement discretion approach for LDTs is intended to help assure the safety and effectiveness of LDTs, and may also foster the manufacturing of innovative IVDs for which FDA has determined there is a reasonable assurance of safety and effectiveness."

Of particular note, the Proposed Rule's current approach of not "grandfathering" LDTs on the market at the time of the final rule is in contrast to the VALID Act and prior proposals by FDA, all of which have included grandfathering provisions. Such provisions are intended to preserve patient access and mitigate economic impact by allowing already marketed LDTs to remain on the market, subject to certain conditions, without the need for subsequent premarket review.

The Proposed Rule does identify certain classes of LDTs, such as forensic tests and human leukocyte antigen tests, that would expressly be exempted from the Proposed Rule's enhanced requirements. But all other LDTs on the market at the time of the final rule would be expected to come into compliance. FDA acknowledges that, under this approach, LDTs on the market may have to come off, but it estimates that nearly 50% of the LDTs on the market today would qualify as low-risk tests that, as Class I devices, would generally not be subject to premarket review even under the new regime.

The Proposed Rule asserts that FDA retains the right to take legal action against any LDT during the final phaseout period should such action be necessary, as well as to promulgate different policies of enforcement discretion for specific LDTs in the future if there is a public health need, as in the case of COVID-19. Finally, the Proposed Rule suggests that FDA may seek to outsource review of the IVD submissions, at least in part, through FDA's Third Party review program to help improve efficiencies.

### Impacts of Proposed Rule

With the repeated reintroduction of the VALID Act in recent years and the Biden administration's announcement this year of its intent to begin rulemaking, it has appeared all but certain that LDTs would become subject to greater regulation in the near future. If enacted as proposed, the Proposed Rule will have a profound impact on clinical labs that offer LDTs.

In the near term, clinical labs offering LDTs should consider beginning to develop systems to ensure that they can comply with MDR reporting requirements whenever the first phase of enforcement discretion ends.

Over the years to follow, in order to support premarket review, labs would have to develop evidence of both LDTs' (1) analytical validity (which is currently subject to review under CLIA); and (2) clinical validity (*i.e.*, the accuracy with which an LDT identifies, measures, or predicts the presence or absence of a clinical condition or predisposition in a patient).

Approaches to complying with all of these regulatory requirements, including developing the evidence required to support premarket review, are fairly well established and understood in light of FDA's historical regulation of other IVDs. Nevertheless, the volume of tests that would have to undergo new regulatory scrutiny, and the desire by some to preserve access to LDTs already in the marketplace, will likely result in calls for clarity and reform of clinical expectations.

We also expect judicial challenges to the final rule, as those most opposed to FDA's proposed oversight of LDTs question FDA's jurisdiction to regulate LDTs and may take issue with FDA's assertion of this jurisdiction through rulemaking rather than in response to legislation. To the extent such litigation ensues, it could significantly delay FDA's publication of a final rule and when the rule actually becomes effective.

Clinical laboratories and other stakeholders seeking to comment on the Proposed Rule must do so by the December 4, 2023, deadline.

## Enforcement Date Delayed for Use of Electronic Interoperable Systems To Track Prescription Drugs at Package Level

In August 2023, FDA announced that it will grant manufacturers and their trading partners a one-year reprieve from requirements in the Drug Supply Chain Security Act (DSCSA) mandating use of systemwide interoperable electronic systems for tracking prescription drugs sales at the package level. Under the DSCSA, the systems were supposed to be in use by November 27, 2023, but FDA announced it will not enforce the requirements until November 27, 2024.

Congress enacted the DSCSA in November 2013 as an amendment to the FDCA. The law was intended to replace the elaborate and outmoded drug pedigree and licensure requirements in the Prescription Drug Marketing Act of 1987. Among other things, the DSCSA:

- Outlines steps to achieve interoperable, electronic tracing of products at the package level as they are distributed in the United States.
- Directs FDA to establish national licensure standards for wholesale distributors and third-party logistics providers (3PLs).
- Requires these entities to report licensure and other information to FDA annually.

Congress established a 10-year timeline for DSCSA implementation, recognizing the need for an iterative implementation approach given the complexities and costs of compliance. Accordingly, FDA has approached implementation of the DSCSA in phases, focusing at first on lot-level management, serialization, electronic transfer of transaction history between actors, suspect product investigations and development of national licensure requirements for 3PLs.

More recently, FDA implemented a pilot project program to better understand the technical capabilities of the supply chain and to assist with identifying system attributes that are necessary to implement the DSCSA's track-and-trace requirements.

The announcement that FDA would exercise enforcement discretion with respect to the enhanced systemwide distribution security requirements that were scheduled to go into effect on November 27, 2023, was made in a guidance document on August 25, 2023. FDA said in this guidance that it will not take action to enforce the DSCSA requirement that transaction information be exchanged in a secure, interoperable, electronic manner for another year.

FDA also said the exercise of enforcement discretion will apply to the requirement that package-level product identifiers be included in transaction information for any product sold into interstate commerce before November 27, 2024. This announcement does not impact other verification and tracing requirements under the DSCSA, including requirements relating to serialization, which remain in effect.

The exercise of enforcement discretion is consistent with FDA's prior approach to implementing the DSCSA; the agency has delayed related enforcement dates on past occasions when it recognized stakeholders needed more time to come into compliance. The guidance document reminds industry, however, that the reprieve should not be viewed as a justification to delay efforts to achieve the interoperable distribution system.

To that end, FDA issued a separate guidance in September 2023 addressing the adoption of standards and technology to effectuate establishment of the interoperable system. This guidance explains that only electronic methods of product-tracing will be permitted, and, consistent with the July 2022 draft guidance on the topic, it recommends that stakeholders use the Electronic Product Code Information Services (EPCIS) standard, which is a global GS1 standard.

In terms of technology, the final guidance expressly allows trading partners to use platforms like web portals and emails to exchange transaction information, so long as the EPCIS standard is utilized. This flexibility had been a priority request from multiple trade groups across the supply chain.

## Compliance Corner

The extra year to establish an integrated electronic system is a welcome development, but it is not grounds to slow the effort. FDA has a history of measured implementation of the DSCSA, and it has postponed other enforcement dates to allow the industry time to comply with the complex requirements in the statute. But FDA has in prior instances pressed ahead after granting the short reprieve, and we expect the same will happen here. Accordingly, companies should continue to prioritize compliance with these requirements and engage trading partners, consistent with the terms of FDA's September 2023 Guidance, to achieve systemwide integration by November 2024.

## Final Guidance on Cybersecurity Considerations in Premarket Submissions for Medical Devices

On September 27, 2023, as part of its ongoing focus on cybersecurity risks, FDA issued the final version of the guidance document "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions" (the Guidance). This final document updated a draft version issued on April 8, 2022, and superseded a prior guidance issued on October 2, 2014, "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices."

With this lengthy, 53-page Guidance, FDA has provided a detailed set of recommendations and examples to inform device manufacturers about the agency's expectations for cybersecurity design, testing, labeling and management. It also provides recommendations for the corresponding documentation to be included in premarket submissions for applicable products, with the intention to "promote consistency, facilitate efficient premarket review, and help ensure that marketed medical devices are sufficiently resilient to cybersecurity threats."

In the Guidance, FDA makes clear that strong cybersecurity controls are an essential component of a device manufacturer's quality system and are a necessary consideration in assessing the overall safety and effectiveness of a medical device. In particular, the Guidance emphasizes the risks presented by:

- The expanding interconnectivity among devices and electronic systems.
- The growing frequency and severity of cyberattacks, particularly attacks on the health care sector that increasingly carry the threat of direct clinical consequences for patients.

**The Guidance broadly applies to any medical device with "cybersecurity considerations," including those that have a device software function or that contain software or programmable logic.**

### Cybersecurity Considerations for Device Premarket Submissions

The Guidance broadly applies to any medical device with "cybersecurity considerations," including those that have a device software function or that contain software or programmable logic. It is not limited to devices with networking or other interconnected capabilities. It also applies to devices that meet the definition of a biological product under Section 351 of the Public Health Service Act, whether or not they require a premarket submission, and to the device constituent parts of combination products.

The Guidance describes four general principles for device cybersecurity that FDA believes are relevant to device manufacturers:

1. **Cybersecurity is part of device safety and the Quality System Regulation.** FDA makes clear throughout the Guidance that management of cybersecurity risks is an integral part of a device manufacturer's broader Quality System Regulation (QSR) obligations, intended to ensure a device's safety and effectiveness. As a way to satisfy these requirements, the Guidance suggests that device manufacturers use a Secure Product Development Framework (SPDF) as a complement to their QSR compliance. FDA defines an SPDF as a "a set of processes that help identify and reduce the number and severity of vulnerabilities" throughout a product's entire life cycle.
2. **Designing for security.** FDA emphasizes that cybersecurity objectives must be addressed throughout a device's architecture and be integrated into its overall design, including with respect to its supply chain, third-party components, implementation, intended use (and foreseeable misuse), interconnectedness with other devices and systems, unique cybersecurity vulnerabilities and risk of patient harm.

3. **Transparency.** A device's safety and effectiveness may be impacted by a lack of cybersecurity information, including how to integrate the device into its use environment and how users should maintain cybersecurity throughout its life cycle. To mitigate this risk, users must be able to access relevant information about a device's cybersecurity controls, potential risks, and methods for updating the device and otherwise preventing cyber threats. Manufacturers must develop a plan for monitoring, remediating and communicating with users about a device's vulnerabilities in the postmarket environment.
4. **Submission documentation.** The Guidance indicates that the volume and complexity of submission documentation relating to cybersecurity should correspond to the relative cybersecurity risks associated with the device. FDA also notes that cybersecurity risks addressed in submission materials should be treated separately from other types of risks or criteria relevant to a device, such as software risks.

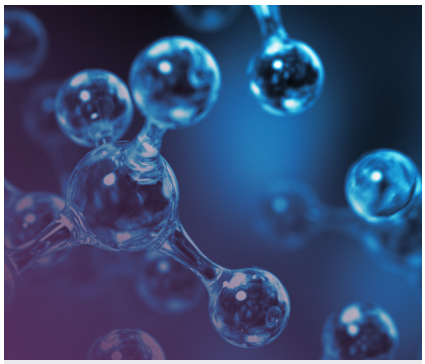
Much of the Guidance is devoted to detailed recommendations and examples regarding how manufacturers should use and design SPDFs to manage cybersecurity risks. SPDFs should incorporate a security risk management plan, which should be included in premarket submissions to help demonstrate a device's safety and effectiveness. A security risk management plan should contain documentation for:

- Threat modeling.
- Interoperability considerations.
- Cybersecurity risk and vulnerability assessments.
- Software bill of materials.
- Component support information.
- Unresolved anomaly assessments.

In addition, a manufacturer's SPDF should address a device's security architecture — covering the entire system in which it is expected to operate — and the manufacturer's cybersecurity testing procedures, which are intended to demonstrate and verify the device's cybersecurity design controls.

Among the key points manufacturers should consider in their SPDF and cybersecurity management, and document in their premarket submissions, are:

- Cybersecurity risks along all points of a product's development and life cycle, including plans for addressing postmarket vulnerabilities.
- Cybersecurity considerations presented by third-party software components or cloud-based services utilized by a device.
- Cybersecurity risks raised by the use of artificial intelligence and machine learning in a device.
- Cybersecurity considerations in the context of how a device will interact with other devices, networks and systems.
- Whether the device's labeling is sufficiently tailored to the "average user," presenting information about a device's cybersecurity risks in a way that is both accurate and easy to understand. If a manufacturer fails to adequately label a device with respect to cybersecurity considerations, it could be deemed misbranded under Section 502(f) of the FDCA.



## Strategy Considerations

The entry into force of FDCA Section 524B, together with the final Guidance on "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions" and FDA's other energetic activity in this space, serve as ample reminders to medical device manufacturers that they must take cybersecurity as seriously as any other quality system requirements when designing, producing, marketing and monitoring their products.

Accordingly, sponsors should ensure that their premarket submissions for medical devices with cybersecurity considerations fulsomely address the concerns and principles that FDA has laid out in the Guidance.

### FDA's Expanding Cybersecurity Authority and Oversight

FDA observers are well aware of the agency's current focus on cybersecurity issues, and the Guidance should be viewed in the context of several recent, related measures. In particular, as discussed above in "Increased Focus on Cybersecurity Could Pose False Claims Act Exposure Risk for Life Sciences Companies," the final Guidance references new cybersecurity authority granted to FDA under FDORA, which went into effect on December 29, 2022. (For more on this topic, see our article "Spotlight on FDORA: Key Provisions for Life Science Enforcement and Regulation Industry Participants" in the June 2023 issue of this newsletter.)

FDORA amended the FDCA by adding Section 524B, "Ensuring Cybersecurity of Devices," which established new cybersecurity requirements applicable to premarket submissions for cyber devices, including 510(k) premarket notifications, premarket approval applications, product development protocols, *de novo* requests and Humanitarian Device Exemption applications. FDORA further amended the FDCA by making a failure to comply with Section 524B a prohibited act under FDCA Section 301, which may result in criminal prosecution or injunctive relief.

FDA released the Guidance around the same time it began to enforce a "refuse-to-accept" policy for medical device premarket submissions that lack the cybersecurity information required under Section 524B. Under FDORA, Section 524B cybersecurity requirements were slated to go into effect on March 29, 2023, but FDA guidance provided a six-month grace period that ended on October 1, 2023. Issuing the final Guidance shortly before that date may be viewed as a complimentary measure that provides device sponsors with information that aids premarket submissions in meeting these newly effective requirements.

However, it should be noted that although the Guidance references Section 524B, it applies much more broadly because its scope is not limited to "cyber devices"; rather, the Guidance applies to any device with "cybersecurity considerations," as described above.

In addition to building on FDA's new cybersecurity authorities under FDORA, it is clear that FDA intends the Guidance to enhance and complement existing cybersecurity guidance materials. Specifically, the Guidance supplements two other FDA cybersecurity-related guidance documents:

- "Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software," issued in 2005.
- "Content of Premarket Submissions for Device Software Functions," issued earlier in 2023.

FDA also noted that the Guidance's recommendations align with or expand on the premarket cybersecurity considerations in the International Medical Device Regulators Forum's 2020 guidance, "Principles and Practices for Medical Device Cybersecurity."

# Other Enforcement

## DOJ-Led Enforcement Actions Against Life Sciences Companies Continue on a Downward Trend

The number of DOJ-led enforcement actions against life sciences companies has continued to trend downward during 2023. Year to date, DOJ has announced negotiated resolutions with just two life sciences companies. That tally is four fewer settlements than in 2022, which was the previous low-mark year for DOJ-led settlements.

While it is not unusual to see an uptick in enforcement actions announced in the last few months of the year, it seems unlikely that this year will match even last year's low number of resolutions, as DOJ had announced twice as many settlements by this time last year.

The two resolutions announced so far this year reflect common themes: distribution of knowingly defective products and kickbacks to prescribers.

In January 2023, a medical device manufacturer paid close to $10 million to resolve allegations that, over the course of five years, company sales representatives provided approximately $100,000 in free spinal implants and tools for use in surgeries performed outside the United States to induce a surgeon to use the manufacturer's products in surgeries performed in the U.S.

In March 2023, another medical device company entered a nonprosecution agreement to address claims that the company conspired to commit health care fraud and wire fraud in connection with the design and manufacture of an implantable — but inert, nonfunctioning — medical device component that according to DOJ "served no medical purpose."

As detailed in the nonprosecution agreement, although the company did not voluntarily disclose the misconduct, the government determined that a nonprosecution agreement and discounted monetary penalty was appropriate because the company replaced prior senior management, fully cooperated with DOJ's investigation and implemented extensive remedial actions. (The reduced fine also reflected an ability-to-pay discount.) The company also agreed to pay $8.6 million to resolve a federal False Claims Act *qui tam* suit based on the same set of facts.

Prosecution of the company's former CEO is ongoing.

## Another Claim Against Product Support Services: If at First You Don't Succeed, Try State Court

On August 8, 2023, Takeda Pharmaceutical Company Limited and certain subsidiaries entered a $42.7 million civil settlement to resolve allegations that Shire[6] utilized product support programs as "marketing" tools to induce physicians to prescribe certain "exorbitant[ly]" priced drugs used to treat chronically ill patients. The relator's petition also alleged that Shire paid clinical nurse educators to recommend one of its drugs to providers, all in violation of the Texas Medicaid Fraud Prevention Act (TMFPA).

[6] The defendants identified in the original petition include Shire PLC, Baxter International Inc., Baxalta Inc. and ViroPharma Inc. (collectively, "Shire"). As set forth in the pleadings, Takeda acquired Shire in January 2019, approximately three years after the alleged misconduct ended.

The settlement stems from a lawsuit filed by Health Choice Advisory, LLC (HCA), a purported health care research organization, under the *qui tam* provisions of the TMFPA. Similar to other lawsuits filed by HCA and its affiliates in federal and state courts against other pharmaceutical companies,[7] HCA alleged in this action that Shire used two product support programs as "selling" tools to induce physicians to prescribe Shire's products.

The first program, free nurse educator services, allegedly relieved physicians of their "duty to monitor" chronically ill patients. Although the relator's petition provides little in the way of details, the petition indicates that nurse educators "help[ed] professionally manage the wellness of patients" by answering patient questions regarding covered drugs and teaching patients how to administer them.

The second program offered free reimbursement support — benefits verification, prior authorization assistance and appeals of coverage denials — to physicians who prescribed Shire's products. The relator alleged that the two programs constituted illegal kickbacks because the services reduced physicians' administrative expenses, thereby increasing their profit margins for prescribing the covered products. According to the relator, the product support programs were allegedly distinguishable from benign post-prescription interactions between pharmaceutical companies and patients because Shire's alleged schemes were designed to "impact [p]rescriber-level behavior that occurs *prior to* the writing of prescriptions."

Relator HCA originally pursued claims against Shire in federal court but voluntarily dismissed that action in March 2020, after the U.S. government moved to dismiss a number of similar lawsuits filed by entities affiliated with HCA against other pharmaceutical companies. Two months later, in May 2020, HCA filed a petition in state court against Shire asserting claims under Texas law. According to the underlying pleadings, the Texas attorney general declined to intervene, yet HCA proceeded and secured a denial of Shire's dismissal motion before the parties ultimately reached a negotiated settlement.

Of note, in denying Shire's petition for a writ of *mandamus*, the Texas appellate court analyzed a recent Fifth Circuit case that had affirmed a trial court's decision to grant DOJ's request to dismiss a similar nurse educator case filed in federal court by an affiliate of relator HCA. In so doing, the court concluded that the Fifth Circuit ruling was insufficient to establish that HCA's claims were foreclosed as a matter of Texas law — *i.e.*, legally impossible.[8]

The Texas appellate court also rejected Shire's argument that the 2003 HHS-OIG (Health and Human Services Office of Inspector General) compliance program guidance established, as a matter of law, that Shire's product support programs are not

[7] As set forth in the pleadings, HCA is an affiliate of the National Healthcare Analysis Group, a self-described "healthcare industry watchdog" that has established affiliated entities to pursue federal and state *qui tam* litigation against several pharmaceutical companies premised on alleged kickback schemes involving the inappropriate provision of free nurse and reimbursement support services.

[8] *See In re Shire PLC*, 633 S.W.3d 1, 31 (Tex. App. 2021) ("Shire's reading of [the federal case] carries that court's holding too far. The Fifth Circuit did not hold that the government had established that "the allegations … lack[ed] sufficient merit to justify the cost of investigation and prosecution" or that "further litigation … [would] undermine practices that benefit federal healthcare programs by providing patients with greater access to product education and support." *Id.* Rather, the Fifth Circuit held that the government's conclusions that the allegations lacked sufficient merit and would undermine beneficial practices were valid reasons to move for dismissal. In other words, the Fifth Circuit merely held that the government's reasons for dismissing the *qui tam* lawsuit in [the federal case] were "plausible, or arguable, reasons supporting the [decision to dismiss].") (citations omitted).

kickbacks. In reaching this conclusion, the court observed that Shire had not identified case law interpreting the nonbinding HHS-OIG compliance guidance, the parties disagreed as to whether the product support programs confer independent value and such a fact-specific inquiry would be premature.

In response to an argument that certain HHS-OIG advisory opinions foreclosed the relator's claims as a matter of law, the court noted that the cited advisory opinions specifically state that HHS-OIG expresses no opinion with respect to the application of any state law. Accordingly, the court concluded that the advisory opinions had limited persuasive value with respect to the legality of the product support program under Texas state law.

### Practice Takeaways

The Takeda settlement is an important reminder that there are no statutory exceptions or regulatory safe harbors that directly apply to product support activities, and that state analogues to the federal Anti-Kickback Statute offer yet another tool for relators and prosecutors to attack product support programs and the perceived high-priced drugs such programs purportedly prop up.

The settlement also brings back to the fore the question of whether the federal nurse educator cases that preceded the state action against Shire would have been dismissed under the current Biden administration, further reducing the "comfort" one can take from those dismissals. Accordingly, a company's analytical framework for assessing product support activities should include not only a robust legal analysis under both federal and state fraud and abuse laws, but also consider the political landscape in which the nurse educator cases have been built.

## In Joint Letters to Hospitals and Telehealth Providers, FTC and OCR Warn of Online Tracking Technology Risks

On July 20, 2023, the Federal Trade Commission (FTC) and the Department of Health and Human Services' Office for Civil Rights (OCR) jointly issued a letter to 130 hospital systems and telehealth providers, warning them about their use of online tracking technologies, which may place consumers' sensitive personal health information at risk of unauthorized disclosure.

This unusual joint outreach put the spotlight on risks associated with technologies that may be incorporated into websites or mobile apps and are capable of collecting users' information without their knowledge or consent.

### Letters Caution Against Inadvertent Disclosures From Third-Party Tracking Technologies

In the letters, the agencies cautioned the recipients about the risks of third-party tracking technologies that may be integrated into a health care organization's website or mobile app and are able to track a consumer's online activities. These technologies are capable of gathering sensitive, identifiable information about a user, often without their knowledge or consent and in ways that are unavoidable and undetectable to them.

As a result, health care organizations may be disclosing — perhaps even inadvertently — their users' personal health information to the third-party companies that operate these tracking technologies. The letters note that the user information potentially at risk of such impermissible disclosures includes "health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more."

Potential consequences may include "identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others."

Highlighting the recipients' potential obligations under both the Health Insurance Portability and Accountability Act (HIPAA) as well as the FTC Act and the FTC Health Breach Notification Rule (the Rule), the letters clarified that health care organizations must:

- Monitor how health information is transmitted to third parties through their online platforms.
- Guard against impermissible disclosures of personal health information, even if they relied on third parties to develop their websites or apps and even if they do not use the information collected through tracking technology.

In a press release issued concurrent with the letters on July 20, 2023, Samuel Levine, director of the FTC's Bureau of Consumer Protection, cautioned that the FTC "is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect consumers' health information from potential misuse and exploitation" because consumers "should not have to worry that their most private and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties."

### Letters Consistent With Recent FTC Enforcement Activity Under the Health Breach Notification Rule

Although the letters focused specifically on tracking technologies employed by health care organizations, this action by the FTC and OCR should be viewed as consistent with recent government efforts — particularly by the FTC pursuant to the Rule — to step up their oversight and enforcement over technologies and practices that expose consumers' personal health information to improper disclosure and misuse.

Under the Rule, "vendors of personal health records" are subject to notification requirements and [penalties] for such "unauthorized disclosures," which include not only data breaches that result from third-party cyberattacks but also a company's disclosure of sensitive data without proper consent.

While the Rule was first adopted in 2009, the FTC's focus in this area has greatly expanded since 2021, when it began engaging in a series of increasingly assertive and specific policy statements, followed by the FTC's first enforcement actions under the Rule in 2023.[9] Taken together, this uptick in activity places health care and life sciences participants on notice that they are responsible for both:

- understanding and monitoring how their digital platforms and online interaction with consumers may place individuals' health information at risk, and
- taking meaningful steps to prevent unauthorized access, disclosure and abuse of their users' data.

In addition, companies are expected to clearly and accurately disclose their data use practices to consumers.

These developments are especially relevant for companies such as medical device and wearable health technology manufacturers that are not subject to HIPAA and, until recently, may not have understood themselves as being held to similarly high standards for the privacy and security of consumer health data under their control.

FTC enforcement actions under the Rule have resulted in meaningful consequences for the companies involved, including:

- Compliance obligations with independent oversight requirements.
- Strict bans on the companies' ability to use and profit from their customers' health data in the future.
- Multimillion-dollar penalties.
- Consumer refunds.

Considering that the FTC has obtained these results in less than a year since it first began enforcing the Rule, the recipients of the July 2023 FTC-OCR joint letters and other companies operating in the health care space should make it a priority to understand how they — and the third parties whose technology they rely on — are using and disclosing their consumers' health data, and take appropriate steps to protect that data against misuse.

[9] The FTC's messaging since 2021 has ranged from generally educating industry about the Rule's applicability, to providing granular guidance about highly specific technologies that place consumer data at risk. For example, on March 16, 2023, the FTC's Technology Blog published a post, "Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking," which explained the concept of pixel tracking, how it is being used to monetize consumer data and the concerns it poses for consumer data. Similarly, FTC took its first enforcement actions under the Rule beginning in 2023, and the settlements it has reached with companies such as GoodRx, BetterHelp and Premom have included detailed allegations about ways those companies intentionally or unwittingly allowed third parties to access and commercialize their users' sensitive health data, such as through technologies like ad trackers.

# The Nucleus: Life Sciences Enforcement and Regulatory Updates

November 2023

## Contacts


**Jennifer L. Bragg**
Partner / Washington, D.C.
202.371.7980
jennifer.bragg@skadden.com

**Avia M. Dunn**
Partner / Washington, D.C.
202.371.7174
avia.dunn@skadden.com

**Maya P. Florence**
Partner / Boston
617.573.4805
maya.florence@skadden.com

**Bradley A. Klein**
Partner / Washington, D.C.
202.371.7320
bradley.klein@skadden.com

**Michael K. Loucks**
Partner / Boston
617.573.4840
michael.loucks@skadden.com

**William (Bill) McConagha**
Partner / Washington, D.C.
202.371.7350
william.mcconagha@skadden.com

**John A.J. Barkmeyer**
Counsel / Washington, D.C.
202.371.7306
john.barkmeyer@skadden.com

**Nicole L. Grimm**
Counsel / Washington, D.C.
202.371.7834
nicole.grimm@skadden.com





One Manhattan West / New York, NY 10001 / 212.735.3000

skadden.com