

# The Nucleus: Life Sciences Enforcement and Regulatory Updates

## In this issue:

- 01 What Life Sciences Companies Need To Know About Recent Changes to DOJ Policies
- 07 FDA Enforcement
- 11 FDA Regulatory
- 15 HHS Compliance
- 17 FCA Enforcement



## What Life Sciences Companies Need To Know About Recent Changes to DOJ Policies

In the first quarter of 2023, the Department of Justice (DOJ) announced a series of updates to existing policies, as well as some entirely new policies, relating to the prosecution of corporate crime and the corresponding evaluation of corporate compliance programs.

These DOJ policies apply across industries, but certain aspects of the new DOJ policies are particularly notable — and may pose particular challenges — for life sciences companies, which have long looked to the Department of Health and Human Services Office of Inspector General (HHS-OIG) at least as much as the DOJ in designing and benchmarking their compliance programs.

### Key Points

- Since the beginning of January 2023, the DOJ has announced a number of updates to its Corporate Enforcement Policy (CEP) and Evaluation of Corporate Compliance Programs (ECCP), and launched a pilot program on Compensation Incentives and Clawbacks (the Pilot Program).
- Most notably for life sciences companies, the DOJ has:
  - Refined the circumstances under which a company can receive credit for self-disclosing identified violations of criminal law.
  - Implemented corresponding voluntary self-disclosure policies across DOJ prosecutorial components.
  - Announced the Pilot Program.
  - Clarified its expectations regarding both incentive-based compensation measures and the preservation of and access to electronic communications.<sup>1</sup>

<sup>1</sup> For more on the DOJ's policy updates, see our client alerts "[DOJ Focus on Corporate Enforcement Continues With Updated Policies Related to Corporate Crime and Compliance Programs](#)" (March 10, 2023), "[DOJ Implements Voluntary Self-Disclosure Policy for US Attorneys' Offices](#)" (March 3, 2023) and "[DOJ Doubles Down on Efforts To Incentivize Early Self-Reporting and Cooperation](#)" (January 19, 2023).

# The Nucleus: Life Sciences Enforcement and Regulatory Updates

June 2023

---

- Taken together, these updates make clear that the DOJ believes effective, well-integrated compliance programs should include, among other things:
  - Compensation structures that tie compensation to compliance.
  - Serious consideration of whether self-disclosure is warranted when misconduct or mistakes are identified.
  - A tailored, risk-based approach to the use of personal devices and messaging applications.
- The DOJ's policies regarding incentive-based compensation measures and clawbacks relate to topics that have been addressed in HHS-OIG corporate integrity agreements (CIAs) for more than a decade, but appear to require greater input from senior leadership and lower the threshold for when compensation may be at risk.
- The DOJ's new self-disclosure policies also differ from HHS-OIG's long-standing Health Care Fraud Self-Disclosure Protocol in that they are less prescriptive regarding the content required to be self-disclosed, and favor prompt self-reporting over completing an internal investigation.
- Finally, the DOJ's pronouncements regarding preservation of and access to electronic communication systems may pose particular monitoring and compliance challenges for life sciences companies, which frequently have a substantial portion of their workforce based in the field.

## Pilot Program and ECCP: New Compensation Considerations

Since 2012, certain life sciences industry CIAs have included incentive compensation and clawback provisions. For example, recent CIAs have provided:

- That employees or executives may not be eligible or may have limited eligibility for incentive compensation where they have been found to have committed or directed significant or nonminor violations of company policies and procedures, have not completed compliance training or have unsatisfactory job performance.
- That employees or executives who are determined to have violated the law, the company's code of conduct or a significant or nonminor provision of any company policy will be ineligible to receive future incentive payments for a period of time from the date of such determination.
- That employees or executives determined to have engaged in "significant misconduct" will have current incentive grants suspended and past grants rescinded for any period in which the violations occurred or were discovered.
- For detailed "executive compensation recoupment programs," pursuant to which "significant misconduct" puts at risk cash and equity-based awards.

The revised ECCP similarly directs prosecutors making charging and resolution decisions to assess, among other things:

- Whether a company's compensation systems defer or escrow compensation based on compliance measures and/or permit the company to recoup compensation for identified misconduct.
- Whether the company, in fact, maintains and enforces its compliance-based compensation provisions.

# The Nucleus: Life Sciences Enforcement and Regulatory Updates

June 2023

---

**Every company entering a corporate resolution with the DOJ Criminal Division will be required to develop and implement compliance-related criteria in its compensation and bonus system, and report annually to the Criminal Division about that implementation.**

---

**Further, the Pilot Program**, which will run until March 2026, includes two components:

- Every company entering a corporate resolution with the DOJ Criminal Division will be **required** to develop and implement compliance-related criteria in its compensation and bonus system, and report annually to the Criminal Division about that implementation.
- Criminal Division prosecutors may accord a 100% reduction of criminal fines for any compensation that a company is able to recoup during the period of the resolution, as well as provide a reduction of up to 25% for good faith attempts to recoup compensation that are ultimately unsuccessful, provided the company fully cooperates, timely and appropriately remediates the misconduct and seeks recoupment through a preestablished recoupment program.

In describing the Pilot Program, the DOJ advised that compliance-related compensation and bonus criteria may include, for example:

- A prohibition on bonuses for employees who do not satisfy compliance performance requirements.
- Disciplinary measures for employees who violate applicable law and/or those who have supervisory authority over such employees or involved business areas who knew of or were willfully blind to the misconduct.
- Incentives for employees who demonstrate a commitment to compliance.

The ECCP and Pilot Program represent the DOJ's first significant foray into incentivizing compliance through compensation measures. While these topics have been addressed in CIAs for more than a decade, the DOJ's recent pronouncements take a different tack than that previously seen in CIAs in several regards.

First, the ECCP and Pilot Program are less formulaic and prescriptive than life sciences CIAs. Second, the DOJ policies (particularly the ECCP) appear to lower the threshold of conduct that is potentially subject to compensation-based consequences to "breaches of compliance" and "ethical lapses" (compared to CIAs, which focus on significant or nonminor compliance violations).

Finally, while CIAs require that companies implement compliance-related criteria in their compensation and bonus systems, the ECCP adds an expectation that senior leadership work in partnership to design and implement a compliance-oriented compensation structure. Specifically, prosecutors are instructed to ask about:

- The role compliance plays in "designing and awarding financial incentives at senior levels of the organization."
- If a company has "evaluated whether commercial targets are achievable if the business operates within a compliant and ethical manner."
- Whether compliance is a "significant metric" in management bonuses.

These types of inquiries presuppose close collaboration among senior compliance, business, legal and human resource leaders, which historically has not been required in CIAs.

# The Nucleus: Life Sciences Enforcement and Regulatory Updates

June 2023

---

## Challenges of Taking Advantage of Self-Disclosure Policies

Since January 2023, the DOJ has announced updates to the CEP designed to incentivize self-disclosure as well as separate self-disclosure policies for the Criminal Division, U.S. Attorneys' Offices (USAO) and the Consumer Protection Branch (CPB), which sits within the Civil Division but is charged with prosecution and oversight of all criminal matters arising under the Food, Drug and Cosmetic Act (FDCA).

**Similarities.** Each of the policies describes similar requirements to receive credit for self-disclosure of a criminal violation:

- Disclosure must be made “directly” to the DOJ component on whose self-disclosure policy the company seeks to rely.
- There can be no preexisting obligation to disclose.
- Disclosure must be made “within a reasonably prompt time” after becoming aware of the misconduct.
- Disclosure must be prior to an “imminent threat” of disclosure or government investigation, and before the violation is publicly disclosed or otherwise known to the government.
- Disclosure must include all relevant facts concerning the misconduct known to the company, including identifying individuals who were involved in the misconduct.
- A company must timely preserve, collect and produce relevant documents.

**Differences.** In addition to these similarities, the self-disclosure policies include some notable variations.<sup>2</sup>

- The Criminal Division's policy reflects a presumption that a company will receive a declination absent aggravating circumstances, whereas the CPB and USAO self-disclosure policies state that those respective DOJ components will not pursue a guilty plea absent aggravating circumstances. Each component also identifies distinct factors that it will consider to be aggravating.
- In addition, the Criminal Division's self-disclosure policy provides for an explicit “additional avenue” for companies to receive a declination notwithstanding the presence of aggravating factors, provided the voluntary self-disclosure is “immediate,” the company provides “extraordinary” cooperation and remediation, and the company has in place a fully functioning compliance program at the time of the misconduct and the disclosure.

Although the issuance of self-disclosure policies by the various DOJ components creates strong incentives for companies to consider self-disclosing identified violations of criminal law, deciding whether and, if so, how to do so may prove especially challenging for life sciences companies.

---

<sup>2</sup>For prior Skadden analysis of these distinctions, see “[Practical Implications of New DOJ Criminal Self-Disclosure Policies](#)” (*Insights – April 2023*) and “[DOJ Doubles Down on Efforts To Incentivize Early Self-Reporting and Cooperation](#)” (January 19, 2023).



# The Nucleus: Life Sciences Enforcement and Regulatory Updates

June 2023

---

For example, life sciences companies that identify a violation of the FDCA may have historically considered disclosing to the Food and Drug Administration (FDA) in the first instance, as FDA has primary responsibility for enforcing the FDCA. While such disclosure is explicitly encouraged in the CPB self-disclosure policy,<sup>3</sup> it also cautions that “if a company identifies potentially intentional or willful conduct, but chooses to self-report only to a regulatory agency and not to the CPB, the company will not qualify for the benefits of a voluntary self-disclosure under this policy in any subsequent CPB investigation.”

This pronouncement leaves open substantial questions regarding how life sciences companies should evaluate whether to self-disclose to the CPB potential violations of the FDCA that fall short of “potentially intentional or willful conduct” given that the CPB can, and has, pursued strict liability misdemeanor criminal charges under the FDCA.

The DOJ’s self-disclosure policies also put a premium on getting a handle on key facts, and assessing potential liability, very quickly. As noted above, the USAO and CPB policies both require disclosure “within a reasonably prompt time” after becoming aware of the misconduct; the Criminal Division policy goes further, encouraging self-disclosure “at the earliest possible time,” even where a company has not completed an internal investigation.

Meeting these expectations may be particularly challenging for life sciences companies assessing highly fact-specific questions, such as whether an arrangement involving remuneration to a referral source fits within a regulatory or statutory safe harbor, or is accompanied by the intent to induce required to violate the Anti-Kickback Statute (AKS).

---

**“If a company identifies potentially intentional or willful conduct, but chooses to self-report only to a regulatory agency and not to the CPB, the company will not qualify for the benefits of a voluntary self-disclosure under this policy in any subsequent CPB investigation.”**

---

The time pressures imposed by the DOJ policies stand in stark contrast to HHS-OIG’s voluntary self-disclosure protocol (HHS-OIG SDP), which has been in place since 1998. The HHS-OIG SDP permits a disclosing company to make an initial disclosure, complete its internal investigation and associated damages analysis, and finalize its disclosure within 90 days of the initial submission.

The HHS-OIG SDP also offers a number of other benefits<sup>4</sup> but notably only provides a path to resolving HHS-OIG authority to impose civil monetary penalties, not necessarily associated criminal or civil liability.<sup>5</sup> As such, life sciences companies that identify violations for which the primary exposure appears to be under the FCA, Stark Law or other civil law may be

---

<sup>3</sup>The CPB policy encourages companies to “continue to make voluntary self-disclosures to appropriate regulatory agencies under existing regulations and procedures.”

<sup>4</sup>These include specific instructions regarding the information that must be included in a self-disclosure submission and the fact that HHS-OIG generally resolves matters disclosed through the SDP without imposing a CIA, and applies a lower multiplier on single damages than would normally be required in resolving a government-initiated investigation. In addition, in cases involving potential AKS violations, the HHS-OIG SDP indicates that HHS-OIG may be willing to resolve matters based on a multiplier of the remuneration provided rather than claims at issue.

<sup>5</sup>HHS-OIG may refer matters disclosed through the SDP to the DOJ to investigate civil or criminal violations, or disclosing parties may seek a False Claims Act release and request that the DOJ participate.

# The Nucleus: Life Sciences Enforcement and Regulatory Updates

June 2023

---

in the challenging position of deciding whether to disclose to HHS-OIG in the first instance and request the DOJ's participation, or disclose in the first instance to a DOJ civil component, for which self-disclosure policies do not currently exist.

## Use of Personal Devices and Communication Platforms

The ECCP revisions issued in mid-March 2023 also contain new guidance on the DOJ's expectations regarding the use of personal devices, communications platforms and messaging apps. Under the revised ECCP, prosecutors are instructed to evaluate, in both charging and resolution decisions, whether:

- A company's policies on the use of personal devices and messaging apps are tailored to the corporation's risk profile and specific business needs, and communicated consistently to employees.
- Those policies ensure that, as appropriate, the company can preserve and access business-related electronic data and communications.
- The company enforces its preservation and access policies consistently (*e.g.*, imposes consequences on employees who refuse to grant the company access, or has exercised its rights to enforce its policies or disciplined employees who fail to comply with them).
- Employees use electronic communication channels to conduct business and whether those channels have archival and preservation settings.
- The company has a "bring your own device" (BYOD) program and, if so, how it works to ensure data preservation, including for example:
  - The company's policies governing preservation of and access to corporate data and communications stored on personal devices — including data on messaging platforms — and the rationale behind those policies.
  - If policies permit the company to review business communications on BYOD or messaging apps.
  - What exceptions or limitations to these policies have been permitted.
  - If the company's approach seems reasonable given its business needs and risk profile.

The ECCP revisions also provide that during an investigation, if a company has not produced communications from third-party messaging apps, prosecutors will ask about the company's ability to access such communications, whether they are stored on corporate devices or servers, as well as applicable privacy and local laws. In announcing the changes to the ECCP, Criminal Division Assistant Attorney General Kenneth Polite noted that a company's answers "or lack of answers" to these questions "may well affect the offer it receives to resolve criminal liability."

# The Nucleus: Life Sciences Enforcement and Regulatory Updates

June 2023

The DOJ's remarks make clear that the Criminal Division will take seriously the thoroughness of efforts to assess the existence of and secure access to business-related communications and data stored on personal devices, communications platforms and messaging apps.

Life sciences companies, in particular, may face challenges in this regard given that they frequently employ large field-based work forces that often do not communicate over centralized communication platforms. In light of the DOJ's revised pronouncements, companies may wish to consider evaluating their policies regarding business-related communications.<sup>6</sup>



## Practice Takeaways

In a May 2023 speech, [Criminal Division Deputy Assistant Attorney General Lisa Miller](#) observed that "in determining whether a compliance program is effective, it's all about what systems are in place that enable a company to successfully respond when misconduct does occur." In this regard, the DOJ's recent policy updates make clear that its expectations around the systems necessary to demonstrate an effective, well-integrated compliance program have evolved significantly.

HHS-OIG officials have also announced that they will be issuing revised, modernized compliance program guidelines by the end of 2023.<sup>6</sup> Life sciences companies, in particular, should continue to monitor both agencies' guidance and consider new developments as they look to benchmark and update their compliance programs.

<sup>6</sup> See [88 Fed. Reg. 25000](#) (April 25, 2023). See also "[Inspector General Grimm HCCA 27th Annual Compliance Institute Keynote](#)" (April 24, 2023).



## FDA Enforcement

### Olympus Faces FDA Warning Letters for Endoscope Quality Issues

On March 15, 2023, Olympus Medical Systems Corporation received its third FDA warning letter in five months, following a November 2022 inspection that determined endoscope accessories manufactured by the firm were adulterated under the FDCA because they were not produced in conformity with FDA's current good manufacturing practice (GMP) requirements of the Quality System Regulation.

The warning letter cited Olympus' inadequate response to inspection observations in several categories, including failing to:

- Adequately establish and maintain corrective and preventative action procedures, including failing to analyze complaint trends, complaint investigations, nonconformances and other sources of quality data to identify causes of nonconforming product and other quality problems.
- Review, evaluate and revalidate processes in the event of changes or deviations.
- Adequately establish and maintain complaint evaluation procedures, including delayed compliant investigations.

# The Nucleus: Life Sciences Enforcement and Regulatory Updates

June 2023

---

Other endoscope accessories were deemed misbranded as a result of Olympus' failure to furnish Medical Device Reporting (MDR) materials required under the FDCA, including its failure to adequately implement written MDR procedures and to report device malfunctions to FDA.

Several of the issues presented in the March 2023 warning letter echoed two other recent warning letters issued to Olympus and its subsidiaries that identified similar deficiencies related to the firm's endoscope products.

Warning letters sent to Olympus' Fukushima and Tokyo facilities in November 2022 and December 2022, respectively, asserted multiple deficiencies related to the design and quality control of its endoscope devices, as well as deficient MDR procedures. FDA cited problems including inadequate validation of device designs and manufacturing processes, failure to maintain Design History Records and failure to implement written MDR procedures and timely make MDR submissions to FDA.

FDA described the March 2023 warning letter as the "latest step" in its "extensive and ongoing efforts" to address Olympus' endoscope-related compliance issues. Jeff Shuren, director of FDA's Center for Devices and Radiological Health, commented on Olympus' ongoing issues in a [March 2023 news release](#): "Olympus' continued failure to meet FDA requirements demonstrates a troubling disregard for patient safety." FDA noted that it would "continue to ensure" that the company "fully addresses" the issues identified in the warning letters.

## Spotlight on FDORA: Key Provisions for Life Science Enforcement and Regulation Industry Participants

As many industry participants are aware, on December 29, 2022, President Joe Biden signed FDORA into law as part of the Consolidated Appropriations Act. FDORA amended the FDCA and the Public Health Service Act (PHS Act) and included significant expansions to FDA enforcement powers.

Although many of these provisions will be rolling out over the next year and FDA is still in the process of developing corresponding regulations and guidance, some of them have already come into effect, most notably new cybersecurity requirements for medical devices. Accordingly, regulated companies should already be evaluating their policies, procedures and compliance measures that may be affected by this new law and preparing to make necessary updates.

To assist companies with this planning, some of the most significant changes are summarized below.

### Accelerated Approval Program

FDORA makes several important changes to FDA's accelerated approval process for drugs and biologics, including enhanced enforcement authorities for this program.

- FDORA grants FDA the authority to require, "as appropriate," that studies must already be underway prior to granting accelerated approval, or to mandate that sponsors begin post-approval studies within a specified time from the date of approval.
- Sponsors must submit progress reports regarding the progress of any post-approval study every 180 days (in comparison to annually under the previous law), and FDA must publish the sponsor's progress reports on its website.



# The Nucleus: Life Sciences Enforcement and Regulatory Updates

June 2023

---

**As a result of changes to the accelerated approval process included in FDORA, FDA is authorized to initiate enforcement actions if a sponsor fails to conduct a required post-approval study with due diligence, including a failure to meet any required conditions specified by FDA or submit timely reports.**

---

- FDORA imposes additional transparency requirements on FDA's decisions to not require post-approval studies for accelerated approval products. If the agency determines that a post-approval study is not required, it must publish the rationale on its website explaining why.
- FDA is authorized to initiate enforcement actions if a sponsor fails to conduct a required post-approval study with due diligence, including a failure to meet any required conditions specified by FDA or submit timely reports.
- FDORA enhances FDA's expedited withdrawal authority for products approved under the accelerated approval pathway and increases the transparency of those decisions. Specifically, FDORA authorizes FDA to use expedited procedures if a sponsor fails to diligently conduct any required post-approval study, including with respect to "conditions specified by the Secretary." FDA must, however, provide clarity regarding proposed withdrawals by providing sponsors with notice and an explanation. The sponsor will then have an opportunity to meet with and file a written appeal to FDA commissioner. At the request of the sponsor, an advisory committee may be convened and consulted on issues related to the proposed withdrawal, if no such committee had previously advised FDA on the matter. Further, the agency must publish the withdrawal proposal for public comments on its website. This is a stark change from previous accelerated approval withdrawal procedures, which only required an opportunity for an informal hearing.

## Bioresearch Monitoring Inspections

FDORA resolves questions regarding FDA's authority to conduct bioresearch monitoring inspections, which monitor the conduct and reporting of FDA-regulated research (commonly referred to as BIMO inspections), and it expands the agency's authority to perform those inspections.

The statute states that the purpose of BIMO inspections is to ensure the accuracy and reliability of clinical and nonclinical studies submitted to FDA or otherwise conducted under the FDCA or PHS Act, as well as to assess compliance with applicable requirements under those laws.

- FDORA expressly permits FDA to inspect facilities involved in the preparation, conduct or analysis of clinical and nonclinical studies submitted to FDA, as well as to inspect other persons holding study records or involved in the study process.
- FDORA clarifies that the scope of BIMO inspections includes records and other information related to studies and submissions.
- FDA is required to issue draft guidance to describe its processes and practices for BIMO inspections of sites and facilities no later than 18 months after the date of FDORA's enactment.

## Expansion of Medical Device Inspection Authority

FDORA authorizes FDA to request records and other information before or instead of an inspection of a medical device manufacturing facility, paralleling authority that FDA received for pharmaceutical facility inspections in 2012 under the FDA Safety and Innovation Act.

In practical terms, this new authority enhances FDA's ability to conduct remote inspections of medical device manufacturers. To exercise this authority, FDORA requires FDA to provide a "rationale" for doing so, and the agency must issue draft guidance on these provisions within one year of FDORA's enactment.

# The Nucleus: Life Sciences Enforcement and Regulatory Updates

June 2023

---

## Medical Device Cybersecurity Requirements

FDORA gives FDA important new cybersecurity enforcement authority by amending the definition of “prohibited acts” in the FDCA to include the failure to comply with newly established device cybersecurity requirements.

- FDORA adds the term “cyber devices” to the FDCA, defined as 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.”
- If a device meets this definition, FDORA requires a premarket submission seeking FDA clearance or approval to include cybersecurity information, such as a software bill of materials, and a plan to address cybersecurity vulnerabilities (discussed below, in the “Digital Health Technologies and Cybersecurity” section).
- The sponsor also must design, develop, and maintain processes and procedures that provide “reasonable assurance” that the device and “related systems” are “cybersecure,” including making post-market updates and patches available to address “vulnerabilities.” Failure to comply with these requirements now constitutes a prohibited act under the FDCA.
- These provisions took effect 90 days after the enactment of FDORA, on March 29, 2023.

## Modernization of Cosmetics Regulation Act of 2022

Although not directly relevant to drug and device manufacturers, it is notable that among the most significant expansions of FDA enforcement authority in FDORA is the Modernization of Cosmetics Regulation Act of 2022 (MOCRA), which amends Chapter VI of the FDCA and significantly augments FDA’s oversight and regulation of the cosmetic industry and cosmetic products.

FDA has stated that MOCRA is “the most significant expansion of FDA’s authority to regulate cosmetics since the Food, Drug and Cosmetic Act was passed in 1938.”

- FDORA requires, among other things, cosmetic facility registration, product and ingredient listing with FDA, serious adverse event reporting to FDA, compliance with certain labeling requirements and maintenance of records that adequately substantiate product safety.
- MOCRA grants FDA new enforcement authority over cosmetics, in the form of mandatory recall authority. FDA may order a recall of a cosmetic product if it determines that there is a “reasonable probability that a cosmetic is adulterated or misbranded and the use of or exposure to the cosmetic will cause serious adverse health consequences or death.” In such cases, FDA has the authority to order a mandatory recall if the responsible person refuses to do so voluntarily.
- The new requirements under MOCRA will take effect one year after FDORA’s enactment.

# The Nucleus: Life Sciences Enforcement and Regulatory Updates

June 2023

## FDA Regulatory

---

### End of COVID-19 Public Health Emergency – Implications for Medical Products

The COVID-19 Public Health Emergency (PHE) expired on May 11, 2023, more than three years after HHS first declared the PHE. Importantly, expiration of the COVID-19 PHE does not impact existing emergency use authorizations (EUAs) for applicable medical products or FDA’s continuing ability to authorize medical products for emergency use.

FDA’s EUA authority is based on declarations by HHS under Section 564 of the FDCA that circumstances exist justifying the authorization of emergency use of certain medical products. These EUA declarations under the FDCA are distinct from the PHE declaration under the Public Health Service Act, although both types of declarations involve a determination by HHS that a public health emergency exists.

HHS issued its first COVID-19-related EUA declaration on February 7, 2020, which stated that EUAs for in vitro diagnostic products for the detection and/or diagnosis of COVID-19 were justified based on HHS’ determination that COVID-19 constituted a “public health emergency that ha[d] a significant potential to affect national security or the health and security of United States citizens living abroad.”

HHS published additional EUA declarations for “personal respiratory protective devices,” “medical devices, including alternative products used as medical devices,” and “drugs and biological products” in the spring of 2020 based on that same determination. In March 2023, HHS amended the February 2020 determination to recognize the existence of a “public health emergency, or a significant potential for a public health emergency,” in order to “avoid the need to issue a new determination under [FDCA Section] 564 where there is no longer a ‘public health emergency,’ but there is still a ‘significant potential for a public health emergency’” involving COVID-19.

As such, an EUA issued under one of the four 2020 EUA declarations will remain in effect until the termination of the relevant declaration or revocation of the EUA. FDA has committed to providing advance notice of any EUA termination and allowing for a reasonable transition period to enable proper disposition of relevant products.

### FDA Continues Efforts To Address Impact of Artificial Intelligence and Machine Learning on Medical Devices

Over the past decade, FDA has been actively attempting to evaluate and address the impact of software on medical devices. This includes the evaluation of fundamental jurisdictional questions relating to software as a medical device (SaMD) as well as how new software applications impact the safety and effectiveness of long-standing device technologies. As part of this effort, FDA has devoted considerable attention to the specific promise — and risks — associated with artificial intelligence (AI) and machine learning (ML).

In April 2019, FDA proposed a regulatory framework for addressing AI and ML in medical devices. The agency introduced the concept of a Predetermined Change Control Plan (PCCP) that would allow for the evaluation of AI and ML “improvements” to the device as part of the premarket review process.

The proposal represented a laudable effort to streamline the medical device approval process. The goal was to reconcile the inherent tension between use of AI software functions that continually update and improve a device and the traditional review framework, in which

# The Nucleus: Life Sciences Enforcement and Regulatory Updates

June 2023

---

updates to devices are reviewed by FDA on a case-by-case basis before they are cleared or approved for use. The PCCP would allow for the one-time approval of AI/ML-related improvements without the need for a new review and clearance with each change.

FDA issued the PCCP proposal as a discussion paper and sought feedback from stakeholders on the merits of the approach. It also initiated a series of public meetings and workshops on AI/ML.

In January 2021, FDA issued an Action Plan on AI/ML-based software in medical devices in response to the feedback it received. The Action Plan retained and elaborated the concept of the PCCP, focusing on distinctions between AI/ML modifications related to inputs, performance and intended use. The Action Plan also proposed a series of next steps, including issuance of a guidance on PCCPs. In late December 2022, Congress passed the Food and Drug Omnibus Reform Act (FDORA), which expressly authorized FDA to approve PCCPs in premarket approval applications of 510(k)s under Section 515C of the FDCA.

Most recently, in April 2023, FDA issued draft guidance titled “Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence/ Machine Learning (AI/ML)-Enabled Device Software Functions.” The draft guidance sets forth a detailed approach to the PCCP concept, attempting to support iterative AI/ML improvements to medical devices through the least burdensome approach while continuing to provide a reasonable assurance of safety and effectiveness.

The draft guidance covers automatic AI/ML-based modifications to a device as well as those changes that are implemented manually. It defines a PCCP as the documentation describing what modifications will be made to an AI/ML-enabled software function and how the modifications will be assessed.

The PCCP components include:

- A Description of the Modifications associated with the AI/ML.
- A Modification Protocol.
- An Impact Assessment.

The draft guidance contains an extensive discussion of data management and sections that discuss each of the PCCP components in detail. FDA has opened a docket to solicit comment on the draft guidance, and we expect it will be refined moving forward. But the draft as written is already a major step forward in FDA’s attempt to address AI/ML as part of the initial premarket review process, and it signals FDA’s continued commitment to avoiding the need for serial re-review and approval/clearance where possible.

These specific efforts are just one part of FDA’s broader aim to address the regulatory challenges and potential associated with digital health, which are also discussed in the “[Spotlight on FDORA](#)” article above.

## Digital Health Technologies and Cybersecurity

FDA recently issued multiple policies on digital health and software, including:

- A framework for using digital health technologies (DHTs) in clinical trials.
- Final guidance regarding cybersecurity requirements for medical device premarket submissions.

---

**FDA is continuing its efforts to reconcile the inherent tension between use of AI software functions that continually update and improve a device and the traditional FDA review framework.**

---



# The Nucleus: Life Sciences Enforcement and Regulatory Updates

June 2023

---

**DHT framework.** On March 23, 2023, FDA published a framework for the use of DHTs in drug and biological product development. Although the framework is not an official guidance document, it provides insight into FDA's plans to regulate technologies such as wearable, implantable, ingestible and environmental sensors that allow for the ability to remotely obtain clinically relevant information.

The framework outlines internal programs intended to build FDA's review capacity and expertise on DHTs, including establishing a DHT steering committee and enhancing FDA's IT capabilities to support the review of DHT-generated data. The framework also describes a range of external programs and workshops to engage industry stakeholders in the development and use of DHTs.

**Medical device cybersecurity requirements.** As noted above, FDORA added provisions that required newly defined "cyber devices" to meet requirements that took effect on March 29, 2023. On March 30, 2023, FDA issued final guidance on cybersecurity requirements for cyber device premarket submissions, which sets forth the agency's implementation of FDORA's requirements. As detailed in the final guidance, cyber device manufacturers will be required to:

- Submit a plan to monitor, identify and address post-market cybersecurity vulnerabilities.
- Implement processes to help ensure the device and related systems are cybersecure, including using updates and patches that address device vulnerabilities.
- Provide a "software bill of materials" that includes commercial, open source and off-the-shelf software components.

Failure to comply with these requirements will result in a "refuse to accept" decision in the future. However, the final guidance establishes a preliminary period through October 1, 2023, for cyber device sponsors to prepare to meet the new FDORA requirements, during which FDA generally plans not to issue "refuse to accept" decisions based solely on these cybersecurity requirements.

## New Clinical Trial Requirements

In addition to those discussed above, FDORA included a number of new provisions of relevance to clinical trial sponsors. Since FDORA's enactment, FDA has released a flurry of guidance that clinical trial sponsors should be aware of, and additional clinical trial-related guidance is anticipated.

**Externally controlled trials.** First, as part of its ongoing effort to address the use of real world evidence in drug development, on February 1, 2023, [FDA issued draft guidance regarding externally controlled trials](#) (ECTs). FDA described ECTs as those that would compare patients receiving an investigational treatment within the trial to patients outside of the trial who have not received the same treatment. The draft guidance notes that FDA has long "recognized the potential value of" external controls but stresses that the "suitability of an externally controlled trial design warrants a case-by-case assessment."

In particular, the draft guidance instructs that "reducing the potential for bias in externally controlled trials is best addressed in the design phase" to reduce errors that lead to incorrect assessments of a treatment's effect. As such, the draft guidance encourages sponsors to select an external control arm prior to initiating the trial, rather than making the selection after the completion of a single-arm trial.

# The Nucleus: Life Sciences Enforcement and Regulatory Updates

June 2023

---

**Decentralized clinical trials.** In accordance with FDORA requirements, FDA released a second draft guidance on May 2, 2023, containing recommendations for decentralized clinical trials (DCTs) involving drugs, biological products and medical devices. A DCT is one in which “trial-related activities occur at locations other than traditional clinical trial sites,” such as a participant’s home, a health care provider’s facility or a clinical laboratory.

DCTs may be fully decentralized — with all activities taking place outside of traditional clinical trial sites — or hybrid, in which some activities occur at traditional clinical trial sites and some do not. As the draft guidance notes, “bringing trial-related activities to participants’ homes, including through the use of DHTs,” may improve clinical trial diversity by reducing both “the need for travel and improv[ing] engagement, recruitment, and retention amongst potential participants with challenges accessing traditional clinical trial sites” and the impact of linguistic barriers on clinical trials.

The draft guidance provides examples of approaches that may be available to conduct a DCT, such as telehealth visits and visits conducted by a local health care provider at the participants’ home. As with the ECT draft guidance, the DCT draft guidance stresses that issues related to the design of a DCT “should be discussed early with the relevant FDA review divisions.”

The draft guidance also addresses the use of digital health technologies in DCTs to remotely capture and transmit health care information, such as software or mobile applications that can serve as communication tools between DCT personnel and trial participants.

**Diversity action plans.** FDORA provides that clinical trial sponsors will be required to submit these two at the same time as they submit other key study documents:

- A Diversity Action Plan for “a clinical investigation of a new drug that is a phase 3 study” or “another pivotal study of a new drug (other than bioavailability or bioequivalence studies).”
- Device studies, which FDA had previously recommended in an April 2022 draft guidance.

A Diversity Action Plan must include “the sponsor’s goals for enrollment in the clinical study; the sponsor’s rationale for such goals; and an explanation of how the sponsor intends to meet such goals.”

FDORA directs the secretary of the U.S. Department of Health and Human Services to consult with stakeholders — such as drug sponsors, clinical research organizations and patients — to receive input on the enrollment of historically underrepresented populations in these trials, and it encourages participation from these populations in order to understand the “prevalence of the disease or condition among demographic subgroups.”

FDORA requires FDA to issue or update guidance on the format and content of Diversity Action Plans by the end of 2023. The requirement to submit Diversity Action Plans will take effect 180 days after FDA finalizes its guidance.

# The Nucleus: Life Sciences Enforcement and Regulatory Updates

June 2023

## HHS Compliance

### Recent HHS-OIG Presentation Underscores Evolving Compliance Program Expectations

In 2022, HHS-OIG entered into 31 new corporate integrity agreements with companies and individuals in lieu of exercising its permissive exclusion authority to bar entities and individuals from participating in federally funded health care programs because of fraud.<sup>7</sup> Of the 31 CIAs entered in 2022, five were made with drug or device manufacturers.<sup>8</sup>

During a recent compliance forum, senior HHS-OIG counsel Laura Ellis discussed key takeaways from some of the latest CIAs, which together underscore HHS-OIG's heightened expectations regarding the role and prominence of compliance officers and compliance committees.<sup>9</sup> These expectations signal an enhanced focus by HHS-OIG on ensuring that companies dedicate the resources and oversight necessary to maintain enduring compliance programs that adapt and evolve over time:

- **HHS-OIG has discretion to limit noncompliance responsibilities of compliance officers.** Several CIAs negotiated in 2022 require that compliance officers “shall not have any noncompliance job responsibilities that, in HHS-OIG’s discretion, may interfere or conflict” with the duties required of them in the CIAs. Senior HHS-OIG officials have explained that they introduced this change to ensure that compliance officers are independent and have the authority and stature to engage as a peer with other executives.
  - HHS-OIG acknowledged that privacy and audit responsibilities, under certain circumstances, are “complementary” to and can be assumed by compliance officers, but HHS-OIG has cautioned against “job creep,” advising that compliance officers should remain objective, provide guidance and oversight and avoid performing business operation roles or supervising legal functions.
- **Compliance committees are expected to play an active oversight role.** CIAs negotiated in 2022 shifted the role of the compliance committee from “supporting” the compliance officer to actively overseeing specific compliance-related activities.
  - For example, recent CIAs task the compliance committee with, among other things, annually reviewing CIA-mandated policies, procedures and training plan as well as overseeing the risk assessment process and the transition plan.
  - Such oversight is a significant departure from earlier CIAs, which simply required management-level compliance committees to “support” the compliance officer in fulfilling his or her responsibilities, and reflects HHS-OIG’s heightened expectations of an active and engaged compliance committee.
  - During the compliance forum, HHS-OIG noted that the current list of compliance committee activities is not exhaustive.
- **Annual risk assessments are a priority.** During the compliance forum, HHS-OIG emphasized the need for compliance personnel to conduct annual risk assessments.

<sup>7</sup> For an in-depth review of HHS CIAs companies entered into in 2022, see Skadden’s April 10, 2023, client alert “[HHS Corporate Integrity Agreements: A Year in Review.](#)”

<sup>8</sup> These figures include the CIAs posted to HHS-OIG’s website as of May 31, 2023. All five CIAs entered into in 2022 were tied to False Claims Act (FCA) settlements. Two CIAs were premised on alleged kickbacks to physicians; one was based on the submission of claims to federal health care programs for tests improperly performed by unqualified personnel; one involved alleged false representations made to the Food and Drug Administration during the pre-market approval (PMA) application process for a medical device; and one stemmed from alleged drug pricing violations and kickbacks to patients through alleged improper donations to a copay charity.

<sup>9</sup> See the Health Care Compliance Association’s live broadcast: “HHS Current OIG Concerns, Revisions to the CIA, and What Can Be Learned From Them,” delivered by Laura Ellis, senior counsel at the Office of Inspector General, HHS (April 24, 2023).

# The Nucleus: Life Sciences Enforcement and Regulatory Updates

June 2023

---

In recent remarks, an HHS-OIG official noted that even if a company is not operating under a CIA, company officers should be thinking strategically about maintaining and bolstering ongoing and evolving compliance plans.

---

- HHS-OIG explained that routine risk assessment enables compliance programs to proactively identify and manage risk and to do so in coordination with key stakeholders, including IT and audit functions.
- According to HHS-OIG, an effective risk assessment begins with a well-defined framework that specifically defines: (i) the scope of the risk assessment; (ii) how risks will be identified (*e.g.*, via surveys, data analysis, etc.); (iii) a scoring methodology; and (iv) the organization's risk tolerance.
- **Novel "transition plans" are now a standard provision of CIAs.** During the compliance forum, HHS-OIG stated that a company subject to a CIA is now required in the fourth year of the CIA to develop a strategic plan for how the company will continue to ensure it maintains an effective compliance program after the expiration of the CIA.
- HHS-OIG noted that even if a company is not operating under a CIA, company officers should be thinking strategically about maintaining and bolstering ongoing and evolving compliance plans.
- **State Medicaid screening is expected.** CIA provisions regarding exclusion screening routinely define "ineligible persons" broadly to include a person who is "currently excluded from participation in any Federal health care program," which would presumably include individuals excluded from a state Medicaid program.
- Notably, however, several recent CIAs explicitly state that ineligible person screening should include publicly available state Medicaid program exclusion lists.

## HHS-OIG Announces Modernization Changes to Its Compliance Program Guidelines

HHS-OIG announced that it will issue revised, modernized Compliance Program Guidelines (CPGs) by the end of this calendar year.<sup>10</sup> The CPGs were part of a major initiative launched by HHS-OIG in 1998 to engage the private health care community in combatting fraud, waste and abuse, and were designed to provide voluntary, nonbinding guidance to encourage the development and use of internal controls and compliance programs for the health care industry. HHS-OIG's announcement emphasized that "the goal of [CPGs] has been, and will continue to be, to set forth a voluntary set of guidelines and identified risk areas that HHS-OIG believes individuals and entities engaged in the health care industry should consider when developing and implementing a new compliance program or evaluating an existing one." As set forth in the Federal Register notice:

- HHS-OIG intends to update CPGs periodically as changes in practices or legal requirements warrant.
- HHS-OIG is amending the format of CPGs by creating a general CPG and industry-specific CPGs.
  - The general CPG, which will apply to all individuals and entities in the health care industry, will cover topics including federal fraud and abuse laws, compliance basics, operating effective compliance programs, and HHS-OIG processes and resources.
  - Industry-specific CPGs will be tailored to fraud and abuse risk areas particular to the industry sector. HHS-OIG anticipates publishing the first two industry-specific CPGs in calendar year 2024 for (i) nursing homes and (ii) Medicare Advantage.<sup>11</sup>

---

<sup>10</sup> See 88 Fed. Reg. 25000 (April 25, 2023).

<sup>11</sup> See Inspector General Grimm HCCA 27th Annual Compliance Institute Keynote (April 24, 2023).



# The Nucleus: Life Sciences Regulation and Enforcement Updates

June 2023

---

## FCA Enforcement

---

### Scienter for Ambiguous Regulatory Provisions Under the False Claims Act

Courts continue to consider whether and to what extent the scienter standard articulated in the context of the Fair Credit Reporting Act in *Safeco Insurance Co. of America v. Burr*, 551 U.S. 47 (2007), applies to the False Claims Act.

In *Safeco*, the U.S. Supreme Court held that a plaintiff could not establish scienter where:

- The case relied on allegations of noncompliance with an ambiguous requirement.
- The defendant offered an objectively reasonable interpretation of that requirement.
- The evidence did not reflect “authoritative guidance” that “warned [the defendant] away” from its interpretation.

Courts across several circuits have applied the *Safeco* framework to determine whether a defendant acted “knowingly” under the FCA. Most recently, in April 2023, the Supreme Court heard argument in two cases out of the U.S. Court of Appeals for the Seventh Circuit applying that framework to FCA claims involving ambiguous Medicaid regulations: *United States ex rel. Schutte v. SuperValu Inc.* and *United States ex rel. Proctor v. Safeway, Inc.* (consolidated at Supreme Court Docket No. 21-1326). A decision in those cases is expected later this term.

Beyond the global question of whether the *Safeco* standard applies to the FCA, questions regarding the precise application of the standard may remain even if the Supreme Court upholds its application in FCA cases. For example, courts may need to determine what regulations are ambiguous, what interpretations are reasonable and whether a defendant must hold its proffered interpretation at the time of the events leading to liability instead of merely advancing the interpretation in later litigation.

# The Nucleus: Life Sciences Enforcement and Regulatory Updates

June 2023



**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

**Alexandra M. Gorman**

Counsel / Boston  
617.573.4852  
alexandra.gorman@skadden.com

**Nicole L. Grimm**

Counsel / Washington, D.C.  
202.371.7834  
nicole.grimm@skadden.com

---

Special thanks to **Elizabeth J. Perkins** and **Sophie Rebeil** for their contributions to this newsletter.

---

This communication is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This communication is considered advertising under applicable state laws.

One Manhattan West  
New York, NY 10001  
212.735.3000

skadden.com