# The Role of Compliance in Government Enforcement

## Introduction

As reflected in recent remarks by Deputy Attorney General Rod Rosenstein, the United States Department of Justice (DOJ) is "reinforcing its relationship with good corporate citizens" by coordinating with, and considering, the fines and penalties other authorities are seeking in enforcement actions against corporations. This increased coordination among enforcement bodies also is meant to "help to identify culpable individuals and hold them accountable."

This white paper will explore recent governmental enforcement activity including the evolution of settlement agreements (Corporate Integrity Agreements [CIA] and Deferred-Prosecution Agreements [DPA]), which provide a perspective on the Department of Health & Human Services (HHS) Office of Inspector General's (OIG) and DOJ's priorities for healthcare compliance program structure and content. The resulting impacts from a mandated CIA or DPA can be mitigated if entities have a clear understanding of the government's current enforcement efforts and use that knowledge to implement and maintain effective compliance programs.

## Government's Perspectives on Corporate Enforcement

### *Recent Developments*

This year has witnessed several notable developments in corporate enforcement. The year began with the issuance of a DOJ memorandum related to dismissal of *qui tam* False Claims Act (FCA) cases. The FCA—an important statute that protects the U.S. government against fraud—imposes liability on any person who knowingly submits a false claim seeking government funds. Both the DOJ and private citizens, known as "relators," are allowed to bring actions on behalf of the United States asserting FCA violations. Under the statute, however, the government is empowered to dismiss the relator's complaint over the relator's objection.[1] For many years, the FCA defense bar has urged the DOJ to exercise its dismissal authority in weak cases, so that frivolous relator-filed cases do not clog the courts and impose needless costs. But over the years, the government has rarely exercised this power, leaving dismissal of frivolous and burdensome claims to the corporate defendants and the courts.

But change may be in the wind. On January 10, 2018, the head of the DOJ's FCA Unit issued an internal memorandum instructing all DOJ attorneys handling FCA cases to consider whether the government should move to dismiss cases where certain criteria are met.[2] The memorandum, dubbed the "Granston Memo," provides defense counsel and relators' counsel guidance on which cases are candidates for a government motion and a basis to argue the government should (or should not) move to dismiss.[3]


1 The only conditions on the government's authority are (1) notice to the relator and (2) a hearing on the motion. 31 U.S.C. § 3730(c)(2)(A).

2 The memorandum, available here, is marked "Privileged and Confidential; For Internal Government Use Only." The National Law Journal published it January 24, 2017. *See* Cogan Schneier, *DOJ Memo Urges Government Lawyers to Dismiss 'Meritless' FCA Cases*, National Law Journal (Jan. 24, 2017).

3 *See* WilmerHale, *Justice Department Issues Guidance on Dismissing Qui Tam False Claims Act Cases over Relators' Objections* (Jan. 25, 2018), https://www.wilmerhale.com/en/insights/client-alerts/2018-01-25-justice- department-issues-guidance-on-dismissing-qui-tam-false-claims-act-cases-over-relators-objections.

Shortly thereafter, on January 25, 2018, then-Associate Attorney General Rachel Brand issued a memorandum on "Limiting the Use of Agency Guidance Documents in Affirmative Civil Enforcement Cases,"[4] another development that is potentially helpful to corporate defendants in a range of enforcement matters. The memorandum makes clear that guidance documents "lack the force of the law,"[5] and emphasizes that DOJ lawyers should not treat them as though they are mandatory. The memorandum implemented sentiments former Attorney General Jeff Sessions articulated in a November 2017 memorandum.[6]

Both memos suggest that senior levels at the DOJ wish to manage their important law enforcement tools to avoid unfair and counterproductive uses. Consistent with that theme, in May 2018, the DOJ adopted a new policy to prevent "piling on,"[7] which occurs when one agency starts an investigation, and other agencies join in to seek punishment for the same alleged misconduct.[8] It is not uncommon for a company to pay a large penalty to one agency, only to also be forced to pay another large penalty to another agency for the same offense. The May policy aims to reduce duplicative penalties against corporations. The policy espouses four basic principles:

1. *No Abuse of Power:* "Department attorneys should remain mindful of their ethical obligation not to use criminal enforcement authority unfairly to extract, or to attempt to extract, additional civil or administrative monetary penalties."

2. *Coordinate with Other Agencies:* "Department attorneys should coordinate with one another" with the "goal of achieving an equitable result."

3. *Consider Other Penalties:* Not only should DOJ attorneys consider other agencies, but they should also consider other penalties. They should "endeavor, as appropriate, to…consider the amount of fines, penalties, and/or forfeiture paid to other federal, state, local, or foreign enforcement authorities that are seeking to resolve a case with a company for the same misconduct."

4. *Fully Vindicate the Interests of Justice:* Lastly, the policy identifies factors the DOJ should consider in determining whether coordination with other agencies allows the "interests of justice to be fully vindicated."[9]

4 United States Department of Justice, Office of the Associate Attorney General, *Limiting Use of Agency Guidance Documents in Affirmative Civil Enforcement Cases* (Jan. 25, 2018), https://www.justice.gov/file/1028756/download.

5 *See Christensen v. Harris Cty.*, 529 U.S. 576, 587 (2000).

6 *See* United States Department of Justice, Office of the Attorney General, *Prohibition on Improper Guidance Documents* (Nov. 16, 2017), https://www.justice.gov/opa/press-release/file/1012271/download.

7 *See* United States Department of Justice, Office of the Deputy Attorney General, *Policy on Coordination of Corporate Resolution Penalties* (May 9, 2018), https://www.justice.gov/opa/speech/file/1061186/download.

8 *See, e.g.*, United States Department of Justice, *Deputy Attorney General Rod Rosenstein Delivers Remarks at the New York City Bar Association White Collar Crime Institute* (May 9, 2018), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-rosenstein-delivers-remarks-new-york-city-bar-white-collar.

9 *See* WilmerHale, *New DOJ Policy to Prevent "Piling-On"* (May 30, 2018), https://www.wilmerhale.com/en/insights/client-alerts/2018-05-30-new-doj-policy-to-prevent-piling-on.

With these principles in mind, as Deputy Attorney General (DAG) Rod Rosenstein has explained, the DOJ hopes that by discouraging "disproportionate enforcement of laws by multiple authorities," it can reinforce "its relationships with good corporate citizens."[10]

In a related development, in July President Trump issued an Executive Order establishing a new Working Group on Corporate Enforcement and Accountability (the Working Group).[11] The order superseded a similar Working Group established by President Obama in 2009.[12] The new Working Group—like the Obama group before it—includes members from the DOJ and its agencies (including law enforcement agencies like the FBI), and will coordinate enforcement with relevant agencies outside the DOJ.

## *Moving Toward Greater Individual Accountability and Corporate Compliance*

The DOJ's interest in improving its "relationships with good corporate citizens," reflected in some of the policies previously mentioned, connects with an articulated interest, at high levels within DOJ, to incentivize increased corporate compliance, while focusing punishment on individual wrongdoers within companies. In 2017, DAG Rosenstein observed that high corporate fines "do not necessarily directly deter individual wrongdoers," because "at the level of each individual decision-maker, the deterrent effect of a potential corporate penalty is muted and diffused."[13] Thus, like Sally Yates, his predecessor as DAG, he made clear the Department's continuing commitment to hold individuals accountable for corporate wrongdoing. Importantly, DAG Rosenstein further noted that "many companies deserve great credit for taking the initiative to develop truly robust corporate compliance programs," and that "[c]ompliance programs promote" the DOJ's primary goal of deterring wrongdoing and encouraging prompt disclosure of violations to enforcement authorities.[14] This is a welcome and renewed recognition that corporate enforcement should "incentivize corporations to establish effective compliance programs,"[15] both by punishing more severely corporations that do not do enough to comply with the law, and "making certain that responsible corporate citizenship is encouraged and rewarded."[16]

Historically, tools like the Sentencing Guidelines[17] and the U.S. Attorney's Manual have sought to create pro-compliance incentives, but more may be required.[18] It appears that senior officers at the DOJ may be evolving toward the same view and may consider additional steps to increase those important incentives.

---

10 *See* Rosenstein Remarks, *supra* n. 8.

11 The White House, Executive Order 13844, *Establishment of the Task Force on Market Integrity and Consumer Fraud* (July 11, 2018), https://www.federalregister.gov/documents/2018/07/16/2018-15299/establishment-of-the- task-force-on-market-integrity-and-consumer-fraud.

12 The White House, Executive Order 13519, *Establishment of the Financial Fraud Enforcement Task Force* (Nov. 17, 2009), https://www.federalregister.gov/documents/2009/11/19/E9-28022/establishment-of-the-financial-fraud- enforcement-task-force. One of the authors served as the Deputy Attorney General at the time policy was issued.

13 Rod Rosenstein, Deputy Attorney General, United States Department of Justice, *Remarks at NYU Program on Corporate Compliance & Enforcement* (Oct. 6, 2017), http://www.law.nyu.edu/sites/default/files/upload_documents/Rosenstein%2C%20Rod%20J.%20Keynote%20Addr ess_2017.10.6.pdf.

14 *Id.*

15 Former Deputy Attorney General Larry Thompson, The Blameless Corporation at 4, *available at* https://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=2036&context=fac_artchop (quotation marks omitted).

16 Deputy Attorney General David W. Ogden at the Compliance Week Keynote Address (2009), *available at* http://www.justice.gov/dag/speeches/2009/dag-speech-090604.html.

17 United States Sentencing Guidelines (USSG).

18 *E.g.*, U.S. Chamber Institute for Legal Reform, *Fixing the False Claims Act* (2013); U.S. Chamber Institute for Legal Reform, *The Exclusion Illusion: Fixing a Flawed Health Care Fraud Enforcement System* (2012).

## *Aggressive Enforcement*

The increasing focus on enforcement against responsible individual wrongdoers, begun in the Obama Administration, appears to be bearing fruit. For example, in July 2017, the DOJ announced what was, at the time, the largest healthcare fraud enforcement action by the Medicare Fraud Strike Force against 412 individuals in 41 districts involving $1.3 billion in alleged fraud.[19] Charges included medically unnecessary treatments, treatments that were never provided, and kickbacks.[20] Many of the charges focused on opioid prescriptions and distribution.[21] Just a few months ago, the DOJ broke that record when it announced charges against 601 individuals in 58 districts involving more than $2 billion in alleged fraud.[22] Meanwhile, huge corporate recoveries have continued. Overall, in fiscal year 2017, the DOJ recovered $3.7 billion from FCA cases, including $2.4 billion from the healthcare industry.[23] From October 2017 through March 2018, the OIG reported expected investigative recoveries of $1.46 billion.[24]

## *DOJ Tools to Incentivize Robust Corporate Compliance*

It is important to understand what tools DOJ prosecutors have at their disposal to incentivize good corporate citizenship. Two such tools are the Deferred Prosecution Agreement (DPA) and the Non-Prosecution Agreement (NPA). A DPA is a type of voluntary, pre-trial agreement used to resolve investigations into corporate misconduct without a guilty plea by the corporation. The agreement is between the company and the government, and it is designed to avoid the penalties of conviction. The government agrees to defer—and ultimately forego—prosecution of the matter pending the company's complying with the requirements of the DPA during a specified term. A DPA is formally filed with a court along with charging documents. Like the DPA, an NPA is a voluntary pre-trial agreement used to resolve investigations into corporate misconduct. However, an NPA is not formally filed with a court. For this reason, NPAs are viewed as more favorable to the corporation than DPAs.

Key provisions of a DPA (or NPA) typically include: acceptance of responsibility; a statement of facts, which outlines the alleged misconduct; a prohibition against public statements contradicting the acceptance of responsibility; a requirement to cooperate in government investigations; a requirement to self-report evidence or allegations of certain misconduct; and the agreement to appointment of a monitor and the terms of that appointment. More about monitorships to follow.

In deciding whether to impose an NPA or DPA, the prosecutors consider the underlying misconduct, the root cause of that misconduct, the company's prior history, and remediation efforts taken by the company. The company's

---

19 United States Department of Justice Press Release No. 17-768, *National Health Care Fraud Takedown Results in Charges Against Over 412 Individuals Responsible for $1.3 Billion in Fraud Losses* (July 13, 2017), https://www.justice.gov/opa/pr/national-health-care-fraud-takedown-results-charges-against-over-412-individuals-responsible.

20 *See id.*

21 *See id.*

22 United States Department of Justice Press Release No. 18-866, *National Health Care Fraud Takedown Results in Charges Against Over 601 Individuals Responsible for $2 Billion in Fraud Losses* (Jun. 28, 2018), https://www.justice.gov/opa/pr/national-health-care-fraud-takedown-results-charges-against-601-individuals- responsible-over.

23 United States Department of Justice Press Release No. 17-1467, *Justice Department Recovers over $3.7 Billion From False Claims Act Cases in Fiscal Year 2017* (Dec. 21, 2017), https://www.justice.gov/opa/pr/justice- department-recovers-over-37-billion-false-claims-act-cases-fiscal-year-2017.

24 United States Department of Health and Human Services, *Semi-Annual Report to Congress* 4 (Mar. 31, 2018), https://oig.hhs.gov/reports-and-publications/archives/semiannual/2018/sar-spring-2018.pdf. One of the authors has elsewhere urged DOJ to take greater care to ensure that penalties are fair and proportionate to actual violations, while also increasing its focus on individual wrongdoers and restitution to victims. David Ogden, Former Deputy Attorney General, United States Department of Justice, Remarks at U.S. Chamber of Commerce Institute for Legal Reform and National Association of Criminal Defense Lawyers Symposium (May 26, 2016), https://www.wilmerhale.com/en/insights/news/2016-06-09-david-ogden-calls-for-doj-to-return-to-a-punishment- fits-the-crime-settlement-approach.

cooperation with the investigation is an important factor. And the strength of the company's corporate compliance program will also play an important role. As a matter of policy—both to incentivize corporate compliance and as a matter of fairness—companies with strong compliance programs ought to be treated better than those with a weak compliance commitment.[25] In evaluating the corporate compliance program, the government focuses on factors such as compliance autonomy, compliance resources, oversight, the strength of compliance policies and procedures, compliance controls, training, audits and risk assessments, compliance incentives, confidential reporting and investigations, disciplinary measures, and compliance testing.

In addition to NPAs and DPAs, the government has many other enforcement tools at its disposal, including: (1) plea agreements; (2) civil settlements; (3) debarment/exclusion; and (4) monitorships and CIAs.

1 *Plea Agreements.* A plea agreement is an agreement by which the company accepts a conviction and receives a bargained-for penalty.

2 *Civil Settlements.* The government may resolve allegations of misconduct through civil settlement agreements, often involving substantial monetary penalties consisting of damages and/or civil monetary penalties. These agreements are commonly used to resolve alleged violations of the FCA.

3 *Debarment and Exclusion.* Debarment prohibits a company or individual from entering into contracts (or obtaining licenses, etc.) with the government for a period of years. For a defense contractor, for example, debarment could literally destroy the business. Exclusion prohibits indirect providers, such as pharmaceutical and medical device companies, from receiving reimbursement from federal healthcare programs for a period of years. Given the market share of those programs, exclusion is also often viewed as a corporate death sentence. CIAs and/or Monitorships may be imposed in lieu of debarment or exclusion, on the theory that imposing an improved compliance structure on a company that produces important products or services is a far better approach than destroying it entirely. Exclusion and debarment remain powerful tools in the government's arsenal.

4 *Monitorships and CIAs.* A monitor is an individual typically working at a law firm, accounting firm, or firm specializing in monitorships, who verifies compliance with a DPA or NPA through observations, tests, and reports. Monitors make targeted recommendations for improvement of corporate compliance and ethics systems, which companies are highly incentivized to adopt. CIAs are commonly used in healthcare enforcement actions. In contrast to a monitorship, a CIA is agency-enforced. CIAs are usually more detailed and prescriptive than monitorship agreements, and CIAs are addressed later in this paper.

25 For proposals to make that better treatment more objective and clearer, *see generally* U.S. Chamber Institute for Legal Reform, *Fixing the False Claims Act* (2013); U.S. Chamber Institute for Legal Reform, *The Exclusion Illusion: Fixing a Flawed Health Care Fraud Enforcement System* (2012).

## *Spotlight on Monitorships*

Monitorships are typically required as an aspect of an NPA, DPA, or other consensual resolution where the government is concerned that a company may have a weaker compliance program. The monitorship process is intended to be collaborative. Typically, the government and company will jointly select the monitor, with the company offering a slate of monitors and the government accepting one or asking for additional options before accepting a nominee. Monitors may be compliance experts, former prosecutors, or other individuals trusted by both sides to help the company avoid repeat violations.

The imposition of a monitor is an important decision that is not taken lightly. In October 2018, Assistant Attorney General (AAG) Brian Benczkowski issued new guidance regarding the decision whether to require a corporate monitor and the selection process in Criminal Division matters (the "Benczkowski Memo").[26] AAG Benczkowski said the memo is intended to "further refine the factors that go into the determination of whether a monitor is needed, as well as to clarify and refine the monitor selection process."[27] The Benczkowski Memo supersedes the 2009 "Breuer Memo" on the same topic[28] and supplements the 2008 "Morford Memo," which addressed the selection of monitors in the contexts of DPAs and NPAs.[29]

The new guidance makes clear that "the imposition of a corporate monitor is never meant to be punitive,"[30] and that the imposition of a monitor should be "the exception, not the rule."[31] In that vein, the Benczkowski Memo outlines "principles for determining whether a monitor is needed."[32] Among other factors, Criminal Division attorneys should consider the following principles in determining whether to impose a corporate monitor:

- Whether the underlying misconduct involved the manipulation of corporate books and records or the exploitation of an inadequate compliance program or internal control systems
- Whether the misconduct at issue was pervasive across the business organization or approved or facilitated by senior management
- Whether the corporation has made significant investments in, and improvements to, its corporate compliance program and internal control systems; and
- Whether remedial improvements to the compliance program and internal controls have been tested to demonstrate that they would prevent or detect similar misconduct in the future[33]

26 United States Department of Justice, Office of the Assistant Attorney General, *Selection of Monitors in Criminal Division Matters* (Oct. 11, 2018), https://www.justice.gov/opa/speech/file/1100531/download (hereinafter "Benczkowski Memo").

27 United States Department of Justice, *Assistant Attorney General Brian A. Benczkowski Delivers Remarks at NYU School of Law Program on Corporate Compliance and Enforcement Conference on Achieving Effective Compliance* (Oct. 12, 2018), https://www.justice.gov/opa/speech/assistant-attorney-general-brian-benczkowski-delivers-remarks-nyu-school-law-program (hereinafter "Benczkowski Remarks").

28 *Id.*

29 *Id.* The Benczkowski Memo clarifies that its principles also apply to court-approved plea agreements that impose a monitor. Benczkowski Memo at 1 n.3.

30 Benczkowski Remarks, *supra* n. 27.

31 *Id.*

32 Benczkowski Memo at 1.

33 *Id.* at 2.

The new guidance "also considers whether misconduct took place under different corporate leadership, and recognizes the unique risks and compliance challenges of the particular region and industry in which a company operates."[34] When a monitorship is needed, financial costs of the monitorship are a central consideration—in other words, DOJ attorneys should consider whether the monitorship's scope is narrowly tailored "to avoid unnecessary burdens to the business's operations."[35]

Further, the Benczkowski Memo announced the creation of a new standing committee—the Standing Committee on the Selection of Monitors.[36] The committee is comprised of the Deputy Assistant Attorney General with supervisory responsibility for the Fraud Section (or his/her designee); the Chief of the Fraud Section or other relevant section (or his/her designee); and the Deputy-Designated Agency Ethics Official for the Criminal Division."[37] The committee is an integral part of the monitor selection process, and it will review all recommended monitor candidates.[38]

The monitor has several responsibilities, including overseeing, reviewing, and proposing modification of a company's compliance program. In furtherance of those goals, monitors review policies, test system controls, and assess compliance risks. The monitor provides periodic reports of its findings and recommendations to the government and the company.

34 Benczkowski Remarks, *supra* n. 27.

35 Benczkowski Memo at 2.

36 *Id.* at 3.

37 *Id.* If the Deputy Designated Agency Ethics Official for the Criminal Division is recused from a particular case, he/she will be replaced by the Alternate Deputy Designated Agency Ethics Official for the Criminal Division or his/her designee. *Id.* at n.6.

38 *See id.* at 3; 7.

Legal issues are obviously central, and so monitors are often lawyers, sometimes former government lawyers. Monitors often employ forensic accountants as well. A forensic accounting team works with the monitor to evaluate the effectiveness of internal accounting controls, record-keeping, and financial reporting procedures as they relate to compliance. The forensic accounting team makes recommendations reasonably designed to improve the effectiveness of the tested areas.

At the end of a monitorship, the monitor's investigations and assessments all lead to what could be the most important aspect of a monitorship—certification. The terms of certification vary from case to case. For example, some negotiated resolutions require the monitor to certify effectiveness of the compliance program related to the specific alleged misconduct that gave rise to the agreement,[39] while others require the monitor to certify the effectiveness of the company's program to prevent and detect fraud broadly.[40] The certification is required and must be in writing. If the monitor cannot complete the certification, the monitorship may be extended.[41]

A monitor should ensure that its recommendations are consistent with evolving standards for effective compliance and appropriate to the circumstances of the company at issue. Monitorships are extensive, expensive, and time-consuming. But they offer the opportunity—albeit not one looked for by the company in the first instance—to improve a company's compliance and ethical culture, and therefore, if done right, should be highly valuable in the long run. For a host of reasons, companies under monitorships should cooperate with the monitor as fully as possible, engage in open dialogue with the monitor about strengths and weaknesses of compliance and ethics culture, and embrace monitor recommendations to improve them. In the end, a monitor's ability to execute the certification will depend on confidence that he or she understands the company, and that it has genuinely addressed its issues. Companies should work diligently to provide the monitor with the confidence he or she needs to certify compliance.

39 *See* Order Instituting Cease-and-Desist Proceedings, *In re Biomet, Inc.*, SEC Rel. No. 79780, Proc. File No. 317771, Attachment A ¶ 24 (Jan. 12, 2017) ("Biomet Order – 2017").

40 *See* Deferred Prosecution Agreement, *United States v. Deutsche Bank AG*, No. 3:15CR61, Attachment C ¶ 20 (D. Conn. Apr. 23, 2015) (ECF No. 6-3).

41 *See* Biomet Order – 2017, Attachment A ¶¶ 24-28.

## Corporate Integrity Agreements

The Federal Sentencing Guidelines of 1995 are the foundation for today's CIAs and are designed to drive compliant behavior through defined minimum standard compliance elements. CIAs between the government and a healthcare provider/entity are typically entered into as a result of a civil settlement agreement; however, the decision to enter into a CIA is based solely on the discretion of the OIG. While not every settlement will result in a CIA, entities should review existing CIAs for insight into the government's current enforcement efforts.

Stipulated penalties are enforced for failure to comply with CIA obligations, and an entity's noncompliance can result in exclusion from participation in federal healthcare programs. Although the foundational elements of a compliance program have not evolved significantly over the years, CIAs can provide a current perspective on the OIG's and DOJ's priorities and concerns in a particular sector. Therefore, providers should pay close attention to recently signed CIAs to remain aware of the government's emphasis and to design a truly effective compliance program that meets its requirements.

### *Individual Accountability*

Since they were first implemented in 1994, CIAs have evolved into more complex and dynamic agreements, containing enhancements such as greater emphasis on board and management accountability, including certifications and annual board reporting. Additionally, the entity subject to the CIA must make all of its board reporting available for review by the OIG. Thus, the effectiveness of board oversight is paramount to the OIG's mission to hold entities accountable for compliance. Annual reporting provisions require an entity's board to demonstrate active compliance program oversight. Such activities include, but are not limited to, the following:

- Documentation—such as minutes, notes, and any taken actions—to support the appropriate level of the compliance officer's reporting to the board
- Lists of approved policies and procedures
- Risk assessment results such as work plans, performed audits, and implemented action plans to mitigate the identified risks

CIAs require the following elements:

- Board accountability
- Compliance officer stature and board reporting process
- Board and management certifications
- Definitions of "ineligible persons"
- Requirement for an Independent Review Organization (IRO)
- Periodic and annual reporting provisions

More recent CIAs also contain certain negotiable elements, including preamble wording that may reference the entity's past compliance efforts, auditing, and monitoring elements that may be unique to the entity's line of business (e.g., hospitals, physician practices, long-term care). Also, recent CIA trends include a requirement for the board to consult with a "compliance expert" to conduct an independent assessment of the effectiveness of the compliance program. This requirement signals the OIG's expectations for such an assessment at least on a periodic basis, if not annually.

Board and management certifications further illustrate the OIG's emphasis on individual accountability. The list of certifying individuals has expanded and can vary depending upon the nature of the issue that gave rise to the CIA. For example, CIAs related to billing and coding violations could result in required certifications by the Vice President of Revenue Cycle and the Billing Manager. Typical certifications include an individual's affirmation that training has occurred specific to his or her areas of responsibility; he or she has promoted compliance within the department; potential compliance issues have been communicated in accordance with the entity's reporting policies and procedures; and he or she is not aware of any violations of federal healthcare program requirements, the CIA, or any entity policies (unless disclosed).

Entities should assess whether their existing training programs are robust enough in high-risk areas and whether their employees would be able to complete similar certifications if called upon to do so. An example of a management certification statement taken from an actual CIA follows:

> "I have been trained on and understand the compliance requirements and responsibilities as they relate to [insert name of department], an area under my supervision. My job responsibilities include ensuring compliance with regard to the [insert name of department] with all applicable federal healthcare program requirements, obligations of the Corporate Integrity Agreement, and [insert name of entity] policies, and I have taken steps to promote such compliance. To the best of my knowledge, except as otherwise described herein, the [insert name of department] of [insert name of entity] is in compliance with all federal healthcare program requirements and the obligations of the Corporate Integrity Agreement. I understand that this certification is being provided to, and relied upon, by the United States."

## *Parties to CIAs Are Growing*

Healthcare entities should take notice of the types of providers that are now subject to CIAs and review the CIAs for opportunities to strengthen their existing compliance programs. While most CIAs have been entered into by hospitals and health systems, the types of providers have expanded to include: physician practices; long-term care facilities, such as skilled nursing facilities; life science companies including medical device manufacturers, pharmaceutical companies, and durable medical equipment suppliers; ambulance companies; laboratories; and rehab and therapy providers, such as wound care.

Each of these types of providers is also subject to specific requirements applicable to its compliance exposure pressure points. For example, one CIA for a medical device manufacturer included obligations regarding travel and expense reimbursement for training and product demonstration purposes. Another CIA required the establishment of a grants management system to prevent sales and marketing employees from being involved in the awarding of grants. Quality-of-care CIAs have also been utilized for long-term care providers with emphasis on medical necessity to demonstrate the appropriateness of provided clinical services.

## *Compliance Span of Control*

The nature and number of "covered persons" has also expanded in recent CIAs to include not only employees but active medical staff, vendors, and subcontractors, as well as "arrangements covered persons." These individuals are involved with the development, approval, management, or review of an entity's focused arrangements. Essentially, through its expansion of the nature of covered persons included in CIAs, the OIG is making it clear that it holds entities responsible for actions carried out by anyone under the entities' control. This expectation may also include global operations, subsidiaries or affiliates, complex supply chains, outsourced functions or departments, and corporate compliance structures and joint ventures. The expansion of covered persons has also increased compliance officers' span of control regarding the entity's compliance risks. Historically, many entities took a siloed approach and philosophy regarding the areas under their compliance department's purview. Today, compliance risks, particularly with regard to complex healthcare entities, are present in information technology, quality, real estate, physician contracting, marketing, procurement, and finance, to name a few. Accordingly, it is the OIG's expectation that the compliance officer will be a senior-ranking position with direct reporting to the board. This reporting relationship, accompanied by the appropriate level of authority, is expected to facilitate a culture of compliance.

## *Incentivizing Compliant and Ethical Behavior*

Recent trends in settlement agreements have also included claw-backs and financial recoupment for annual performance or incentive programs. In 2012, GlaxoSmithKline entered into a $3 billion settlement regarding pharmaceutical sales, marketing, and contracting practices. The agreement contained a claw-back provision that allows for potential recoupment of executive incentive compensation for up to three years for any executive involved in misconduct. Additionally, other entities have utilized compliance modifiers in their annual performance evaluations of all employees. For example, an employee, department, or business unit can either receive additional compensation for activities that demonstrate sound compliance principles or may be subject to reductions in compensation for compliance violations. Some companies have also re-evaluated their "balanced scorecards" to include compliance goals and objectives along with strategic, financial, and operational metrics.

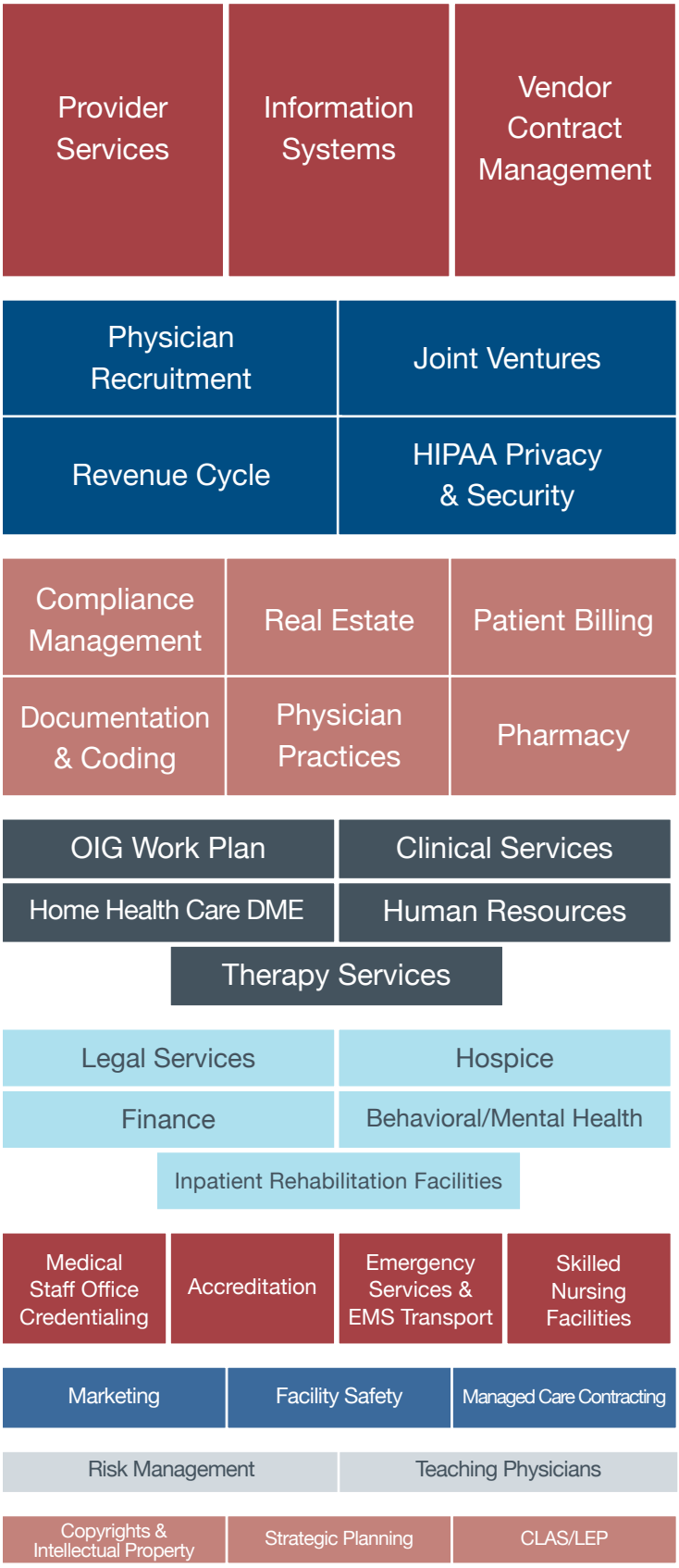
## *Code of Conduct 2.0*

Entities subject to CIAs and DPAs should evaluate and revise their Code of Conduct to ensure that it reflects the requirements outlined in these agreements. A robust Code of Conduct should require:

- An entity's commitment to all regulations and agreement requirements.
- The reporting of suspected violations to the appropriate parties.
- The entity's assurance of non-retaliation for reporting.

Third-party contracts should also be assessed to identify whether the entity's expectations for compliance are clearly articulated and monitored, and that the third party is held accountable for any compliance violations. Training programs should be enhanced to include topics such as Ethical Decision Making, Anti-Kickback Statute, False Claims Act, Stark Law, and Relationships with Referral Sources, and should be provided to all employees as well as contractors.

## Risk Areas for Healthcare Organizations




### *Evolution of Risk Assessments*

CIAs require a comprehensive risk assessment and internal review process designed to "require compliance, legal, and departmental leaders, at least annually, to (1) identify and prioritize risks, (2) develop internal audit work plans related to the identified risk areas, (3) implement the internal audit work plans, (4) develop corrective action plans in response to the results of any internal audits performed, and (5) track the implementation of the corrective action plans in order to assess the effectiveness of such plans."[42] An effective risk assessment process that meets the requirements of any CIA must first ensure that the risk assessment universe is comprehensive and includes all entities, subsidiaries, and joint ventures. Compliance, legal, and internal audit (e.g. internal "assurance" providers) should collaborate in conducting the risk assessment and partner with outside counsel and external audit (e.g. external "assurance" providers) to develop a comprehensive inventory of risk areas for further evaluation.

42 Mercy Hospital Springfield, Mercy Clinic Springfield Communities, MHM Support Services Corporate Integrity Agreement (https://oig.hhs.gov/fraud/cia/agreements/Mercy_Hospital_Springfield_Mercy_Clinic_Springfield_Communities_and_MHM_Support_Services_05022017.pdf).

## *New Positions, Functions, and Systems*

The OIG further emphasizes the importance of an active and effective compliance infrastructure through its requirement of entities to develop focus arrangements systems. These systems, such as those used to monitor relationships with referral sources, include requirements such as:

1. Implementation of a central tracking system and repository.

2. A mechanism to ensure:
   - All arrangements have been properly approved (and activities within are verified and supported).
   - Remuneration is accurate.
   - The transactions are at fair market value.
   - The transactions are also commercially reasonable.

Entities in the process of implementing contract management systems should consult recent CIAs to assess whether the system under consideration can meet the OIG's expectations.

### *Emphasis on Auditing and Monitoring in High-Risk Areas*

The scope of an IRO's work varies depending upon the nature of the enforcement action, however the aforementioned examples provide great insight into whether an entity's compliance work plan adequately covers these high-risk areas. IRO activities include the auditing and monitoring of referral source relationships, quality of care, marketing and sales activities, drug-restocking practices, research and grant funding, real estate, and inpatient medical necessity. Compliance officers should review the scope and coverage of the IROs to determine whether work plans need adjustment to include "mock audits" (using the audit criteria noted in the CIAs) in applicable sectors.

## Conclusion

As corporate enforcement actions continue to increase in both number and scope, it is important that compliance remains at the forefront. Effective compliance programs not only serve as shields against potential compliance risks, they also afford a strong defense against any government inquiry and/or enforcement action. The key takeaways that follow reflect the fundamental topics covered in recent CIAs. Becoming and remaining familiar with both the government's perspective and response to these areas, as well as areas the government may add in future CIAs, will allow entities to develop robust compliance programs that effectively provide proper risk assessment, prevention, and mitigation.

PYA offers a number of services that help organizations identify and prioritize compliance risks. Our executives have decades of experience with the wide-ranging scope of regulatory requirements in order to assist with compliance program development and assessment, risk assessment, project management and implementation, education, and advisory services. For more information contact:


### Shannon Sumner

PYA Chief Compliance Officer and Nashville Office Managing Principal
ssumner@pyapc.com
(800) 270-9629

### David W. Ogden

Former Deputy Attorney General of the United States
Partner and Chair of WilmerHale's Government and Regulatory Litigation Practice Group
david.ogden@wilmerhale.com
(202) 663-6440


### Key Takeaways

Board and Management Accountability

Review of Recent CIAs

Assessment of Compliance Program Coverage

Assessment of Training Programs

Compliance Officer Span of Control

Assessment of Compliance Incentives

Review of Code of Conduct

Breadth of Compliance Risk Assessments

Assessment of Current Contract Management System

Compliance Program Independent Effectiveness Assessment

## About PYA

For more than 35 years, PYA, a national healthcare consulting firm, has helped clients navigate and derive value amid complex challenges related to regulatory compliance, mergers and acquisitions, governance, business valuations and fair market value assessments, multi-unit business and clinical integrations, best practices, tax and assurance, business analysis, and operations optimization.

PYA's steadfast commitment to an unwavering client-centric culture has served the firm's clients well. PYA consistently is ranked among the Top 20 healthcare consulting firms in the U.S. by *Modern Healthcare*. PYA's five affiliated companies offer clients world-class data analytics, professional real estate development and advisory resources for healthcare providers, comprehensive claims audits for self-insured Fortune 500 companies, wealth management and retirement plan administration, and business transitions consulting.

PYA assists clients in all 50 states from offices in Atlanta, Kansas City, Knoxville, Nashville, and Tampa. For more information, please visit www.pyapc.com.

## About Wilmer Cutler Pickering Hale and Dorr LLP

WilmerHale provides legal representation across a comprehensive range of practice areas that are critical to the success of its clients. The law firm's leading Intellectual Property, Litigation/Controversy, Regulatory and Government Affairs, Securities, and Transactional Departments participate in some of the highest-profile legal and policy matters. With a staunch commitment to public service, the firm is renowned as a leader in pro bono representation. WilmerHale is 1,000 lawyers strong with 12 offices in the United States, Europe, and Asia. For more information, please visit www.wilmerhale.com.