10 Steps To Modernizing Corporate Integrity Agreements

By **John Bentivoglio, Jennifer Bragg and Elizabeth Berry** (June 20, 2018, 11:40 AM EDT)

John Bentivoglio

Jennifer Bragg

Elizabeth Berry

A recent report by the U.S. Government Accountability Office, or GAO, highlights the important role that corporate integrity agreements, or CIAs, play in protecting federal health care programs when companies and individuals violate federal law.[1] From July 2005 through July 2017, the GAO found that the U.S. Department of Health and Human Services' Office of Inspector General entered into 652 CIAs — approximately 50 each year — with a high of 83 to a low of 37. A clear majority — 631 — of these agreements accompanied a health care fraud settlement with the U.S. Department of Justice, and these settlements recovered more than $16 billion, according to the GAO.

Given the central role that CIAs play in the OIG's efforts to promote compliance, it is time for the OIG to update its CIA templates and approach in order to make these agreements more effective. Three principles should guide such a review. First, CIAs should be made shorter and more simple so they are easier to negotiate and interpret. This would conserve limited OIG resources and promote compliance within the companies being overseen. Second, CIAs should require that compliance programs be dynamic and incorporate risk-based changes and enhancements to reflect the inevitable change in business practices that occur over the five-year course of a CIA. Finally, companies should be given incentives to implement effective, high-performing programs to replace the current approach that effectively rewards companies for doing the minimum to meet CIA requirements.

This article describes 10 ways the OIG could improve the basic CIA template. We have also developed a reformatted and reorganized model CIA template that will make CIAs easier to negotiate and interpret, more effective in promoting compliance by companies under CIAs, and more useful in providing de facto standards and best practices for other companies in the health care industry.[2]

1. Develop a model CIA template based on modern commercial contracting conventions.

Today's CIAs are an amalgamation of provisions that are poorly formatted, internally consistent and hard to follow. For example, definitions can be scattered throughout the document. Does a definition buried within a specific section apply

to only that section or throughout the entire CIA? These problems have accumulated over time because companies negotiating a CIA do not want to spend negotiating capital on fixing formatting or structure problems when they are more concerned about substantive obligations. The OIG, in turn, has limited resources to negotiate 50-plus CIAs annually and monitor the approximately 250 CIAs that are open at any one time.[3]

The template should: include a preamble section that includes the parties to the agreement, as well as a section with all defined terms; group like provisions in the same place (e.g., one section with all external reporting requirements); and be formatted consistent with standard corporate contracts.

2. Reorganize CIAs around well-established standards for effective ethics and compliance programs.

After the preamble and definitions section, the remaining provisions of the template CIA should be organized around and follow the well-established elements of a compliance program: program organization and oversight; policies and procedures; training and education; internal reporting mechanisms; auditing and monitoring; requirements for internal discipline and accountability; and external reporting. Current CIAs largely follow this approach, but over time one-off provisions have been added with little regard to the typical elements of a compliance program.

3. Strengthen reporting requirements to the board of directors.

Recent CIAs have strengthened board oversight and reporting requirements.

Although burdensome, board and senior management certification provisions emphasize that promoting compliance is not solely the job of the compliance officer, but rather must be endorsed and supported at the highest levels of an organization. This is one area where more detail in a CIA could be helpful. For example, CIAs could specify that, in addition to reporting to the board at least four times annually, the compliance officer should have one or more in-person meetings with the board (or a board committee). Each meeting should include an executive session that excludes members of management and allows for the compliance officer to report on, and the board to ask questions about, whether the compliance officer is receiving adequate support, what challenges he/she faces, and whether the board should be aware of compliance-related issues involving senior management. Executive sessions would bolster the current provisions in CIAs that authorize compliance officers to report to senior management and/or the board on significant compliance-related topics.

4. Streamline policies and procedures requirements.

The policies section of many CIAs is too long and often duplicative: A recent pharmaceutical CIA requires policies covering 20-plus areas and activities.[4] CIAs following settlements addressing "new" areas of misconduct often require policies to address those new areas. Over time, this has resulted in policy proliferation. A simpler approach would better promote compliance. For a pharmaceutical company, this would include requiring policies addressing any significant activity in which the company engages in several broad areas. Within 30 days of the effective date, the company would need to provide the OIG with a list of policies it will implement (a "30-day report"). The OIG could, but would not be required to, comment on the list. If a new activity were undertaken, the company would need (perhaps at the time of launch) to have in place policies governing such activity, educate and train relevant personnel, and implement reasonable monitoring of such activity. The CIA could require that each annual report list the current policies and note which ones were adopted during the prior year. The first-year independent review organization, or IRO, engagement could include a requirement to review the list of policies in light of the company's business practices and risk areas.

5. Eliminate the disincentive to adopt or enhance compliance policies.

CIAs routinely provide that the adoption of new policies may trigger a systems review by the IRO.[5] This creates a major disincentive for companies to update their policies and incentivizes static rules over dynamic, continuously improving programs. The remaining systems review provisions (usually during years one and four of the CIA) are more than sufficient.

6. Update training requirements to reflect modern understanding of adult learning.

Most CIAs require all covered persons to receive one or two hours of general compliance training and personnel with specific (presumably higher risk) responsibilities to receive additional hours. To its credit, the OIG has allowed companies to substitute the required number of "normative" hours of computer-based training, as that term is used in the computer-based training industry. But specifying the number of hours is both over- and under-inclusive, and many companies offer mediocre training sessions that check the necessary box in a single (even if lengthy) session. Modern studies of adult learning show that numerous short, more entertaining messages are more likely to achieve the educational purpose than longer training modules. But tracking the completion of five 10-minute training sessions across an organization with thousands of people is a challenge, particularly in the early months of a new CIA.

The template CIA should simply require the 30-day report (see above) or the implementation report (now standard in all CIAs) to include a plan by the chief compliance officer (CCO) for compliance training that ensures personnel receive effective compliance training in their areas of responsibility. Companies under CIAs already have adequate incentives to get training right. The type of training and completion rates should be tracked and included in subsequent annual reports. The IRO's systems reviews in years one and four (the typical sequence) should include some testing of employee knowledge of compliance policies within their area of responsibility, and the results of such IRO testing should be included in the IRO's reports. Superior training programs would accrue to a company's benefit and be considered in whether certain CIA requirements (or the CIA itself) are sunsetted early (see recommendation 10 infra).

7. Adopt monitoring and auditing provisions that reflect a company's size, business model, and current and future business activities.

Recent CIAs have embraced the notion that effective compliance programs require back-end monitoring and testing, but the requirements are often both too specific and too narrow. Several relatively straightforward changes should be incorporated into future CIAs. First, CIAs should require companies to adopt monitoring and auditing programs for each major area of activity in which the company engages. The OIG could publish, perhaps annually or every other year, the key risk areas for major sectors of the health care industry. Companies under CIAs would need to implement monitoring and auditing requirements for any OIG-identified area in which they conduct significant activities. If the OIG is unable or unwilling to be this ambitious, it could require companies to propose auditing and monitoring programs in their implementation reports. For example, for a pharma company that does speaker programs (an activity widely recognized as high-risk), the CIA should specify a percentage of programs to be monitored for each reporting period. The OIG would be given some time (30 days) in which to provide comments or object. Companies would then need to implement monitoring and auditing programs in subsequent years.

Importantly, the OIG should allow companies (perhaps at the two- and three-year marks) to update their monitoring and auditing programs based on changing activities, business

models and risks. Company-proposed changes (perhaps with a compliance officer certification regarding the justification for the changes) would be submitted to the OIG under provisions that allow the changes to take effect after a period for the OIG to comment and/or object.

8. Incorporate risk assessment.

Risk assessment has been called the "eighth element" of an effective compliance program since the U.S. Sentencing Commission added risk assessments to its definition of an effective corporate compliance program.[6] The OIG has incorporated risk assessments (in varying forms) in recent CIAs, and this concept should be taken one step further. An annual risk assessment should be included in all CIAs with organizations of substantial size and activity. The assessment should be overseen by the chief compliance officer, include the participation of senior management and be briefed to the board of directors. In addition, the compliance officer should include some description in each annual report of the results of the risk assessment and what specific steps the company has taken to update its compliance controls (e.g., policies, training, auditing and monitoring) in light of the annual assessment.

9. Provide an avenue to raise concerns about overreaching by IROs and/or external oversight entities.

Outside reviewers and experts, most commonly in the form of independent review organizations, have played an important role in CIAs for decades. While the benefit of such external reviews is widely (though perhaps not uniformly) understood, companies operating under CIAs have expressed concerns about the cost and activities of IROs and other CIA-required third-party reviewers[7], and these concerns can and should be addressed. The widely criticized experience with monitors imposed by the DOJ should serve as a cautionary lesson on what can go wrong.

Reasonable provisions should be incorporated into CIAs to prevent IRO and/or outside oversight entity overreach. First, the role of such entities should be specified and limited to compliance oversight activities. IRO provisions are reasonably specific in this regard; outside oversight organizations should operate under similarly defined parameters. In turn, outside entities should be required to operate under predetermined budgets and work plans absent a demonstrated need and approval by the OIG (after consultation with the company). Third, CIAs should provide a more effective mechanism for companies to express concerns to the OIG about oversight entity overreach. This may require more time and attention from the OIG, but the incentives for outside entities to expand their scope (and related fees) is simply too great and requires reasonable safeguards. The OIG should act soon to avoid the problems that the DOJ experienced with externally imposed monitors. The DOJ's guidance on the selection and oversight of monitors continues to be useful. [8]

10. Provide incentives for robust compliance programs and demonstrated adherence to CIA requirements.

It may seem counterintuitive to argue that companies under CIAs (which, in civil cases, are alleged to have engaged in health care fraud; in criminal cases, have pleaded guilty to such misconduct) should be given incentives to implement effective programs, but the current CIA template incentivizes companies to do no more than meet the CIA's minimum requirements. If fostering truly effective and dynamic compliance programs is the goal, the OIG should consider adding some reasonable incentives for companies to implement best-in-class programs.

Here are some suggestions:

- Allow companies to take some functions (e.g., some of the work currently done by IROs) in-house under a function independent of any commercial business unit after two or three years of clean reviews by the IRO and OIG. This would provide both an incentive for exceptional adherence to the CIA in the early years and institutionalize the capability that is brought in-house (e.g., compliance auditing).

- Allow companies to propose alternative approaches to achieve a compliance requirement under the CIA. The alternative would be submitted to the OIG with a certification by the CCO (and/or the compliance committee) that the alternative will be at least as effective as the control in the CIA. Absent objection from the OIG, the company could proceed with change. Incentives would provide the impetus for compliance officers (and, more importantly, boards and senior management) to implement dynamic, highly effective compliance programs.

Conclusion

CIAs can and should remain an important mechanism of fostering robust compliance programs in companies that have (or are alleged to have) violated federal health care laws and regulations. Over time, however, the format and substantive provisions of CIAs have become unwieldy, with new provisions added to old in a haphazard and sometimes counterproductive fashion. The OIG should adopt a new template that is easier to negotiate and interpret, is more dynamic and flexible to address changing business practices and associated risks, and provides meaningful incentives for companies to do more than the bare minimum in implementing comprehensive compliance programs. The new template we've drafted would be a good place to start.

John T. Bentivoglio is a partner at Skadden Arps Slate Meagher & Flom LLP. He previously served as associate deputy attorney general and special counsel for health care fraud at the U.S. Department of Justice.

Jennifer L. Bragg is a partner and Elizabeth Berry is an associate at Skadden.

[1] U.S. Gov't Accountability Office, GAO-18-322, Office of The Inspector Genergal's Use of Agreements to Protect the Integrity of Federal Health Care Programs (2018), https://www.gao.gov/products/GAO-18-322.

[2] We recognize that the suggestions in this article are focused on CIAs involving large health care companies (e.g., large pharmaceutical manufacturers; major health care systems) and that more modest and streamlined provisions may be appropriate for smaller health care organizations. To jump start the adoption of the suggestions in this article, we have developed a **model CIA template** that we urge the OIG to consider and adopt (perhaps after a notice and comment process) for future CIAs.

[3] In 2017 alone, the OIG entered into 46 CIAs related to heath care fraud. Between 2012 and 2017, the OIG entered into 260 CIAs. See Memorandum From Skadden Arps Slate Meagher & Flom LLP, Health Care Investigation Trends: Corporate Integrity Agreements No Longer a Given (March 26, 2018), https://www.skadden.com/insights/publications/2018/03/health-care-investigation-trends.

[4] Par Pharmaceutical Cos. Inc. & Par Pharmaceutical Inc., HHS CIA § III.B.2 (March 4, 2013), https://oig.hhs.gov/fraud/cia/agreements/Par_Pharmaceutical_03042013.pdf (listing 22 areas that must be addressed in policies — without including a separate requirement for a Code of Conduct).

[5] See, e.g., id. § III..E.1.b ("If Par materially changes its relevant systems, processes, policies, and procedures, the IRO shall perform Systems Reviews for the Reporting Period in which such changes were made in addition to conducting a Systems Review for the first and fourth Reporting Periods, as set forth more fully in Appendices B and C.").

[6] U.S. Sentencing Guidelines Manual § 8B2.1(c) (U.S. Sentencing Comm'n 2016) ("In implementing subsection (b), the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement set forth in subsection (b) to reduce the risk of criminal conduct identified through this process.").

[7] Concerns were expressed by participants in a 2012 roundtable re IROs. See Office of Inspector Gen. Focus On Compliance: The Next Generation of Corporate Integrity Agreements (2012), oig.hhs.gov/compliance/compliance-guidance/docs/Focus_on_Compliance.pdf.

[8] See Memorandum From Craig S. Morford, Acting Deputy Attorney Gen., to Heads of Dept. Components U.S. Attorneys (March 7, 2008), https://www.justice.gov/usam/criminal-resource-manual-163-selection-and-use-monitors; see also Memorandum From Gary G. Grindler, Acting Deputy Attorney Gen., to Dept. of Justice (May 25, 2010), https://www.justice.gov/usam/criminal-resource-manual-166-additional-guidance-use-monitors-dpas-and-npas (providing additional guidance on the use of monitors).
