Practical Tips for Negotiating and Then Living Under a Corporate Integrity Agreement
By
Laura Laemmle-Weidenfeld
Jones Day
Washington, DC

A quick look at the website for the Department of Health and Human Services Office of the Inspector General (OIG) reveals links to hundreds of Corporate Integrity Agreements (CIAs) between OIG and a broad variety of health care-related entities, including physician practice groups, durable medical equipment suppliers, ambulance suppliers, hospitals, pharmaceutical and device manufacturers, and every other type of entity in between. Entering into a CIA typically occurs at the end of a long, painful law enforcement investigation into suspected misconduct involving federal health care program reimbursement, at which time the entity that has been under investigation is looking forward to putting the entire experience in the rearview mirror. It is doubtful that any entity, ever, has been enthusiastic about entering into a CIA, which typically carries a term of five years and imposes significant structural and reporting requirements, the violation of which can lead to severe penalties including exclusion. But despite any sense of frustration at having to enter into the CIA, and a general exhaustion from the settlement process, settling entities and their counsel need to focus carefully on the future implications of the CIA before and during their negotiation of the agreement. In addition, settling entities should consider starting to ramp up their compliance programs to meet standard CIA requirements as soon as they know they are likely to be settling their case and entering into a CIA. By taking these steps, entities can avoid significant headaches and even financial penalties over the coming months and years. They hopefully will even benefit from the experience by ending the CIA term with a robust and smoothly operational compliance program.

When Will a CIA Be Required?

Until recently, the OIG required virtually every entity resolving False Claims Act (FCA) allegations to enter into a CIA, and in exchange the OIG waived its authority to seek voluntary exclusion of the entity for the conduct covered under the settlement. The OIG no longer automatically requires a CIA with every entity settling FCA allegations. Instead, the agency now evaluates on a case-specific basis whether a CIA is necessary for purposes of protecting the Medicare trust fund or other applicable federal health care programs. In making this evaluation, the OIG considers elements such as the severity of the allegations, the weight of the evidence supporting those allegations, and what steps the entity recently has taken to strengthen its compliance program and ensure that the alleged misconduct does not recur. Where the OIG is sufficiently confident that the risk posed by the entity to the future of the federal health care programs is minimal, the office does not require the entity to enter into a CIA.

The authority to require a CIA lies solely with the OIG, even though the perceived need for the CIA usually arises out of the FCA investigation led by the Department of Justice and/or U.S. Attorney’s Office (collectively, DOJ). Throughout the FCA investigation, the DOJ attorneys will have kept the OIG attorney assigned to the matter apprised of developments, but the extent to which OIG counsel is visible to defense counsel throughout the investigation can vary dramatically. Once settlement discussions begin with the DOJ, the DOJ attorney usually
will inform the entity as to whether the OIG will require a CIA and will put defense counsel in touch with the appropriate OIG attorney. If the OIG plans to require a CIA or, worse, is considering seeking exclusion of the entity and/or any of its employees, it usually behooves defense counsel to learn this as soon as possible in the settlement process. Delaying the discussion until late in settlement talks on the hope that OIG will ultimately do whatever is necessary to allow DOJ to settle the case carries significant risk.

**Pre-Negotiation Homework**

Entities that have not previously been subject to a CIA generally are unfamiliar with what is required under a CIA. For that reason, clients usually benefit from having their counsel educate them very early in the settlement process as to what a CIA is, the type of CIA that most likely will be required for the client, and what that generally will look like. A key component of this process is determining which category of CIA is likely to be required, which depends on the nature of the misconduct alleged. CIAs come in one or a combination of the following categories: claims review, focus arrangements, quality of care, and covered functions review.

Claims review CIAs are required in situations in which the alleged misconduct related to coding and/or billing functions, e.g. upcoding of claims, or billing for items or services not actually delivered. Under this category of CIA, the entity (typically using a retained Independent Review Organization (IRO)) must annually review a random sample of claims and, if the error rate for the sample is five percent or higher, conduct a statistically valid claims audit and a systems review to determine the root cause of the problems.

Focus arrangements CIAs are required for settlements in which the alleged misconduct related to financial relationships with physicians or other actual or potential referral sources. In these, the entity is required to implement formal systems that track and provide for review of such financial relationships, and typically an annual IRO review of those relationships also is required.

Quality of care CIAs are reserved for situations in which the government has alleged that the provider performed services that were of such low quality that they should not have been reimbursable and thus the billings for services to the patients constituted false or fraudulent claims. Under this CIA model, OIG requires the provider (e.g., a nursing home chain) to retain a quality monitor, which in OIG’s words “not only will address the specific issues underlying the allegations, but also will look at the entity's delivery of care and evaluate the provider's ability to prevent, detect, and respond to patient care problems.” Currently OIG has approximately a dozen of these in place nationwide, according to its own website.

And finally, OIG requires covered functions CIAs for entities for whom the alleged misconduct related to some other function within the organization, which does not fit into any of the prior three categories but nevertheless potentially impacts claims ultimately submitted to federal health care programs. Most of these “covered functions” CIAs apply to pharmaceutical or device manufacturers, for whom they can apply specifically to, *inter alia*, promotional activity such as the selling, marketing, detailing, advertising, or promoting of items reimbursable under health care programs; the provision of advice regarding the billing or coding of items that are reimbursable under federal health care programs; and marketing, formulary, contracting, or
rebate activities undertaken in connection with the sale of items or services reimbursable under federal health care programs. Outside of the manufacturer context, covered function CIAs also have covered functions like the restocking of pharmaceuticals and the provision of disease management programs under contracts with state Medicaid agencies. In each of these, the OIG identifies one or more functions within the organization in which misconduct allegedly occurred, and requires the entity to retain an IRO to perform reviews relating to those covered functions.

In organizing the CIAs into these categories, the OIG has imposed significant uniformity, while also allowing itself the flexibility to tailor the requirements of the CIA to the specifically alleged misconduct giving rise to the need for the CIA without imposing extraneous requirements (for example, it does not impose focus arrangement requirements on entities that only allegedly upcoded). Within each category, the model CIA contains sections in which the OIG works with the entity to carefully tailor the descriptions and requirements to the entity’s business, while many other sections contain uniformly prescribed language from which the OIG generally will not deviate. For this reason, once defense counsel has determined which general model the OIG is likely to require, both counsel and client likely will find it useful to review a few CIAs into which the OIG recently has entered, in the same category that will be applied to the entity. Note that the OIG’s model CIA language is constantly evolving (like a good compliance program). For that reason, it is important to focus on the most recent comparable CIAs available.

At this juncture, it is also helpful not only to look at other recent CIAs that involve similar types of alleged misconduct, but also to focus on recent CIAs with entities that engage in similar business and/or are structured similarly to the client. Up to this point in the settlement negotiations, the conversations with the client probably have been focused in the General Counsel’s office. Once entering into a CIA is contemplated, however, bringing into the conversation employees who reside in compliance and/or the business can be very helpful for identifying logistical challenges and opportunities early in the process. While in-house counsel will understand the legal requirements, compliance and business employees usually bring a much-needed understanding of how the entity performs its functions and what it can and cannot do, which will be critical in negotiating an agreement that the entity can live with.

**CIA Negotiation Process**

Once the settlement discussions seem to have gained enough traction that the possibility of settlement seems fairly real, the DOJ attorneys typically will put defense counsel in touch with the OIG attorney if the OIG will be requiring a CIA in exchange for a waiver of their voluntary exclusion authority. Occasionally the OIG attorney is involved in the early settlement discussions with defense counsel, at which point he or she will indicate directly that a CIA will be required if the entity wants a waiver. Note that the OIG will not grant a waiver without a CIA. Although historically the need for a CIA to settle an FCA case was almost a foregone conclusion, the OIG recently has backed off from that automatic position and now requires a CIA in fewer (but still numerous) situations. Where it does not require a CIA, it does not provide a release, although OIG leadership has indicated that OIG attorneys will notify the entity prior to settlement if the OIG plans to seek exclusion. The entity technically may refuse to enter into a CIA when the OIG requires it, in which case the OIG may still approve the FCA.
settlement without a waiver; but the entity then runs a real and substantial risk that the OIG will in fact seek exclusion of that entity following the settlement.

Regardless of whether an OIG attorney is already at the settlement table and initiates the discussion or whether the DOJ attorney puts defense counsel in touch with the OIG attorney, the negotiation of the CIA will be between the OIG attorney and defense counsel. DOJ is not part of the discussion.

**Standard CIA Provisions**

As indicated above, reviewing previous CIAs into which the OIG already has entered can be very informative for counsel and client alike. A number of elements are consistent across all CIAs. Every CIA requires the establishment of a compliance officer and committee, and every CIA imposes compliance obligations on the Board of Directors. Every agreement also requires the adoption of a code of conduct, applicable policies and procedures, and training and education on those policies and procedures both within the first 90 to 120 days as well as annually thereafter. Not only is the entity required to conduct internal reviews, but it also will be subject to review by an IRO that it is required to retain (at the entity’s own expense). Many CIAs over recent years have required members of management to certify that the areas under their responsibility are in material compliance with the law and the CIA. And every CIA regardless of category requires the entity to screen for ineligible persons (which includes excluded persons and convicted persons who are subject to mandatory exclusion) and to disclose violations of federal health care program law.

A key goal of the CIA, according to the OIG, is transparency. To that end, CIAs also impose significant notification requirements on entities. The entity must, within 30 days, notify OIG “in writing, of any ongoing investigation or legal proceeding” of which the entity becomes aware, that involves any allegation that the entity “has committed a crime or has engaged in fraudulent activities.” It must repay identified overpayments within the 60 days required under the Affordable Care Act.ii The entity also must report specified Reportable Events within 30 days of determining that they exist. Depending on the type of entity, these can include substantial overpayments (although “substantial” is not defined); probable violations of federal health care program law for which the entity could be subject to penalties or exclusion; probable violation of law over which the Food and Drug Administration has jurisdiction; employing or contracting an excluded person; and the filing of a bankruptcy petition by the entity. Each entity also must report any changes to business units or locations, such as the closure of a unit or location, the purchase or establishment of a new unit or location, and the sale of a unit or location. The reporting times for each of these requirements are mandated within the CIA.

In addition to these reporting requirements that are triggered by the occurrence of specific unanticipated events, the OIG also requires the entities to submit a number of scheduled reports directly to the OIG for review. Within a few months of entering into the CIA, the entity must submit an implementation report to the OIG reporting on the status of the implementation of the CIA requirements. The information required to be contained in this report is specified in the CIA itself. In addition, the entity is required to submit reports annually regarding its continued compliance with the CIA’s requirements. These reports must contain certifications by the Compliance Officer and others regarding the accuracy of the information contained in the report.
and his or her diligence in ascertaining that accuracy. Additionally, the IRO is required to submit reports on its review(s) to the OIG.

In the CIA, the entity also agrees to give the OIG more extensive inspection, audit and review rights than is required under existing law. The entity agrees to retain for inspection “all documents and records relating to reimbursement from the Federal health care programs and to compliance with this CIA for one year after the end of the last Reporting Period” or longer or required by law. If the OIG receives a Freedom of Information Act (FOIA) request for information the entity submitted to the OIG and designated as protected as a trade secret or as “commercial or financial and privileged or confidential,” the OIG shall make “a reasonable effort to notify” the entity prior to release so that the entity may avail itself of any remedies under FOIA. These provisions are among the least negotiable of the provisions in any agreement.

Also non-negotiable are the breach and default provisions contained in the CIA. These provide for a litany of stipulated penalties that the OIG may impose on the entity if it fails to comply in a timely manner with specific CIA obligations. For example, the most recent CIAs impose a stipulated penalty of $2500 per day for failing to implement the requirements to have a compliance officer in place, a written Code of Conduct, ineligible persons screening and removal requirements, and mandatory training. Similarly, failing to timely submit any CIA-required reports and failing to timely engage an IRO also can subject the entity to a penalty of $2500 per day. (Note, however, that the CIA expressly permits the entity to seek a reasonable extension of time in advance of the deadlines.) If the OIG brings an action for stipulated penalties, the entity has review rights comparable to those that would apply under 42 U.S.C. §1320a-7(f) and 42 C.F.R. Part 1005, except that the only questions at issue shall be whether the entity was in full and timely compliance with the CIA obligations as to which the OIG is dissatisfied, and the period of any noncompliance. The OIG cannot seek Departmental Appeals Board (DAB) review of an unfavorable finding, although the entity may seek such review.

Equally non-negotiable, but more potentially draconian, are the provisions allowing the OIG to exclude the entity for “material breach” of the CIA. The CIA defines a “material breach” as one of the following: (1) repeated or flagrant violations of the CIA’s requirements; (2) failing to report a reportable event, take corrective action, and make the appropriate refunds; (3) failing to engage and use the required IRO or monitor; or (4) failing to respond to a Demand Letter from the OIG regarding the imposition of Stipulated Penalties. While the OIG has not exercised this authority frequently, it entered into a five-year exclusion agreement earlier this year with a nationwide provider of dental services who, the OIG alleged, had materially breached its obligations under the CIA.

Although the CIA language provides the entity with the right to notice and opportunity to cure, the entity’s rights to challenge an action by the OIG seeking stipulated penalties or exclusion are limited to review of whether the entity was in material breach of the CIA generally and on the date of the exclusion letter, and if the alleged breach could not be cured within the CIA’s prescribed 30-day period, whether the provider had begun taking action within that time period to cure the breach, provided a timetable to cure the breach, and was following that timetable. Any exclusion imposed by the administrative law judge (ALJ) or DAB takes effect within 20 days of the decision. And finally, the DAB’s decision (or the ALJ’s if no appeal is taken) is final; the entity has no further appeal rights.
**Somewhat More Negotiable Elements**

Although the requirements discussed above generally are not negotiable, the details of some key elements of the CIA are negotiable, at least to some extent. Counsel and their clients should focus on these early, so they can identify provisions that need to be structured in a certain way or even revised to accommodate the business realities of their entity.

The first and most critical provision to analyze is the specific entity or entities to be covered by the CIA’s requirements and potential for sanctions. The OIG of course will insist on requiring the primary entity that engaged in the alleged misconduct to be subject to the CIA’s requirements. But often the entity will have parent corporations or other affiliates or even key employees that the OIG also will want to hold responsible for compliance with the CIA. Counsel should anticipate this issue and be prepared to explain why it does not make sense in this particular situation to extend the obligations to affiliates, or why only some affiliates should be included, as appropriate. Keep in mind that if an affiliate is included in the CIA, all the provisions including the training and reporting requirements, as well as the stipulated penalty and exclusion provisions, will apply equally to the affiliate (unless some exception is carved out). This puts the affiliate at significant risk, and may be particularly problematic if the affiliate has minimal actual control over the settling entity.

Although the CIA’s provisions all contain time deadlines, these usually can be negotiated. Some entities, for example, may need a longer period of time than the OIG initially proposes to develop a code of conduct or policies and procedures. Extending this and similar time requirements for another 30 or 60 days in the agreement is often possible. If they begin extending some of the dates, however, counsel should pay close attention to the interplay between the date requirements: many of the requirements are dependent on having completed other requirements earlier. For example, it typically would be of little use to negotiate a longer time in which to develop a new code of conduct if the entity does not at the same time negotiate a longer time to distribute the new code of conduct to its employees.

The definition of a Covered Person also is critical, and subject to some negotiation, under the CIA. Among other things, Covered Persons must receive training, which is both general and specific to particular subject matters. It may be most practical to specify certain categories of Covered Persons, so that employees are not required to endure training on topics that do not apply to them. There may be entire categories of employees for whom it makes no sense to provide the usual training, perhaps because they have no involvement whatsoever in any of the concerns of the CIA or in federal health care programs. It may make sense to carve out a subgroup of investors from the Covered Conduct definition, perhaps because they have no involvement in the day-to-day activities of the organization. Making these and similar determinations requires counsel to work closely with the operational employees at the entity who are closer to the practical questions of which individuals will be impacted by the specific requirements of the CIA, and whether the impact on those individuals is properly aligned with the purpose of the CIA and with business exigencies.

While including an IRO review usually is not negotiable, the details of how that review will be conducted and what it will include are subject to negotiation. The goal of the OIG, and usually of the settling entity too, is to ensure that the review is designed in alignment with the
actual potential for problems. For example, the OIG can be flexible regarding the size of the probe samples to be pulled and the selection criteria for those probe samples, so long as the entity’s rationale is sound. OIG also sometimes allows entities and IROs to conduct a verification review, in which the entity reviews a portion (often increasing over time) of the claims to be reviewed and the IRO performs a quality control check on the entity-reviewed claims results, in lieu of the IRO performing the entire review.

Various other logistical details also can be negotiable, so long as the entity can put forth a solid argument for why, as applied to it, the standard approach/language is not feasible. Such arguments will not succeed as to provisions that apply to every entity equally such as stipulated penalties or reportable events, but they can be useful in establishing definitions that ultimately affect who will be responsible for training, reporting, and oversight under that particular CIA.

Finally, note that some of the language in the CIA is less specific than many providers would like. For example, in the provider context, CIAs define Reportable Events to include “a substantial Overpayment” but provide no indication as to what constitutes “substantial.” When the entity and defense counsel press the OIG negotiating attorney to clarify this and other similarly vague terms, the OIG attorney typically will decline to clarify further but instead will advise the entity to seek clarification from the OIG Monitor after the CIA is finalized.

**Going Forward Post-Execution**

The CIA typically is signed concurrent with the civil settlement agreement (and any criminal resolution document, if appropriate). In practice, the OIG usually is the last signatory on all the documentation, so the CIA goes into effect only once the entire global settlement is finalized.

Shortly after this date, as the entity begins scrambling to meet the deadlines in a timely fashion, the OIG notifies the entity as to who its assigned OIG Monitor will be. The Monitor typically is not the same OIG attorney who was assigned to help in the investigation and negotiation of the CIA. Nor does the OIG Monitor have the same role. The role of the Monitor is to provide oversight of the entity’s implementation of the CIA requirements and respond to questions the entity may have throughout that process. Whereas the OIG attorney negotiating the CIA will have played an adversarial role, the Monitor’s role is more collaborative. The OIG’s ultimate goal is to promote best compliance practices during the term of the CIA and to make sure the entity has a solid, effective compliance program in place at the end of the CIA term, in order to minimize later compliance problems and to protect the trust fund.

Nevertheless, it is often difficult for an entity that has just undergone an investigation by the government to view yet another government attorney with anything less than suspicion and distrust. The natural tendency is to view the Monitor as a continuation of the adversary relationship that immediately preceded the CIA. Perhaps for that reason, the Monitor expects his or her primary point of contact within the entity to be the Compliance Officer, not the General Counsel or outside counsel. Some entities resist this arrangement. But the OIG’s expectation is that the Compliance Officer will establish a direct relationship with the Monitor, and will do his or her best to be transparent and timely with all the obligations under the CIA. The OIG does not expect perfection, and in fact becomes skeptical if it is not notified of any compliance problems.
under the CIA. In our experience, the Monitors are at least as concerned with ensuring that the entity’s compliance program is identifying and correcting problems as they are with ensuring the program prevents the problems in the first place.

It is always difficult, when negotiating a CIA, to anticipate the various problems that may arise under the agreement. This is particularly true because most CIAs extend for five years. During those years, Compliance Officers may come and go, other key management may come and go, counsel may change, and the ownership and structure of the entity will evolve. Even the OIG monitor assigned to the entity may change. Despite the entity’s and counsel’s best efforts to negotiate CIA language specifically tailored to the entity’s needs, inevitably at some point during the term of the CIA an obligation will seem impracticable or even impossible to those within the entity who are required to implement it. The entity either will need clarification on how to apply that provision in its own business reality, or will want to explain to the OIG that the requirement to which the parties originally agreed simply is unworkable and should be modified.

When this occurs, the OIG Monitor will expect the entity to request clarification or even some modification promptly. Although the OIG strongly prefers for all proposed modifications to be discussed before the CIA is finalized, the Monitors seem fairly accustomed to receiving and considering occasional requests as the CIA term goes on. Note, however, that just as with the initial negotiations, the entity should be prepared to explain in detail to the Monitor why this situation differs from the standard and why it is unworkable, or contrary to the spirit of the CIA, or otherwise not sensible. Although the Monitor will get to know the entity better over time, the entity should never expect the Monitor to know the arcane details of how the entity operates, and should be prepared to explain in detail all the relevant facts that it wants the Monitor to consider in connection with its request.

**Conclusion**

No health care entities enter into CIAs because they affirmatively want to. They do it because they want to resolve an investigation or litigation, and entering into the CIA is better than the alternative of defending against an exclusion action. But entities can take steps before the CIA is finalized to negotiate an agreement whose obligations they can meet over the next five years and, even, that can help them ensure better compliance (and less potential for enforcement actions) over the term of the CIA and even beyond.

---


\(^ii\) Before enactment of 42 U.S.C. §1320k as part of the Affordable Care Act, the OIG required these to be reported and repaid within 30 days.