HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

COMPLIANCE TODAY

Volume Eleven
Number Six
June 2009
Published Monthly

Broad whistleblower provisions in the new Stimulus Bill

PAGE 4

Meet

John Landreth, CPA, CFE, CHC

Managing Director and Founder of Atoll ~ Compliance and Controls

PAGE 14

Feature Focus:

Walking the line: When providers "go wrong" under Corporate Integrity Agreements

PAGE 28

Earn CEU Credit

WWW.HCCA-INFO.ORG/QUIZ, SEE PAGE 39

Opening Day, HCCA 13th Annual
Compliance Institute
Caesars Palace, Las Vegas

feature focus

Walking the line: When providers "go wrong" under Corporate Integrity Agreements

By Felicia Heimer, JD and Judy Waltz, JD

Editor's note: Felicia Heimer is Senior Counsel in the Administrative and Civil Remedies Branch of the Office of Inspector General, United States Department of Health and Human Services. Felicia may be reached by e-mail at Felicia.Heimer@oig.hhs.gov.

Judy Waltz is a partner in the San Francisco office of Foley & Lardner LLP, where she is co-chair of the firm's Life Science Industry Team. Judy may be reached by e-mail at jwaltz@foley.com.

As part of the resolution of an action brought under the civil False Claims Act or the Civil Monetary Penalty Law, the Office of Inspector General of the United States Department of Health and Human Services (OIG) will consider, given the specific conduct of the defendants, whether or not to exclude the offending health care provider, manufacturer, or supplier from participation in federal health care programs. An excluded individual or entity cannot participate in or receive funds from any federal health care program, including Medicare and Medicaid, for the period of the exclusion up to and until such time as OIG affirmatively agrees to reinstatement.

In lieu of exclusion, OIG may agree to a waiver of its exclusion authority in exchange for the defendant's agreement to enter into a Corporate Integrity Agreement (CIA). The CIA provides the entity the opportunity to regain the government's trust by implementing and maintaining specified compliance obligations over a number of years. The term of a CIA is, in essence, a probation period, and a violation of the CIA during this period could lead to stipulated penalties or, for the most severe violations, exclusion from federal health care programs. The consequences of noncompliance with the OIG's expectations are grave; therefore, an understanding of how to navigate the provisions of a CIA is of paramount importance.

This article attempts to provide health care entities with some practical advice on how to ensure compliance with a CIA through developing and managing a successful working relationship with OIG. The article also provides some insight into the manner in which OIG evaluates compliance with CIA obligations, as well as specific case examples of how some providers have "gone wrong" and failed to comply with CIA provisions.

Overview of CIA obligations

Although each CIA is tailored to the specific health care entity and conduct at hand in the underlying settlement, most CIAs require the entity to meet the following types of obligations throughout the term of the CIA:

- Designation of a compliance officer and a Compliance Committee;
- Development of compliance-related policies and procedures;
- Education of employees and other key parties (e.g., contractors);
- Engagement of an independent review organization (IRO) to perform annual audits and reviews, and to report findings and observations to OIG;
- Development and maintenance of a confidential disclosure program;
- Development and maintenance of a process to screen for excluded individuals;
- Submission of implementation and annual reports;
- Reporting of other information at specified intervals;
- Reporting and refunding identified overpayments; and
- Reporting the occurrence of "material deficiencies" or "reportable events," and developing and implementing corrective action plans in response to those events.

OIG requires providers to comply with the express requirements of the CIA, and will not impose additional obligations once the CIA has been executed. However, if an entity becomes the subject of a new False Claims Act investigation and settlement during the course of the CIA, OIG may agree to waive its permissive exclusion authority in the new case through the negotiation of amendments to the initial CIA, or through negotiation of a new standalone CIA.

Maximizing a good working relationship with OIG

Once a CIA is negotiated and executed between the entity and OIG,

the agreement is assigned to OIG attorneys and staff who serve as monitors. A designated OIG monitor is not only responsible for evaluating the extent to which the entity is in compliance with the terms of the CIA, but also serves as the point of contact for any questions, submissions, notifications, or the disclosures of reportable events which the entity may make during the term of the CIA. Because most CIAs last for five years, most entities operating under CIAs develop a good working relationship with the OIG monitor(s). An understanding of how to develop and maintain a positive working relationship is fundamental to CIA success.

Cooperative communication

OIG is committed to working collaboratively with entities that operate under CIAs by carefully monitoring the entity's CIA compliance and engaging in constructive communication when problems or issues arise. Accordingly, the most effective approach that an entity can take to build a positive working relationship with OIG is to be cooperative and communicate candidly with the OIG monitor responsible for its agreement.

Although it may seem like painfully mundane advice, basic business courtesies should be the norm. Compliance officers are advised to answer e-mails promptly and thoughtfully, and return phone calls as soon as possible. If OIG requests information from the entity that cannot be quickly provided, a deadline should be discussed and that deadline should be met.

When entities are accommodating of OIG's requests for information, and when entities maintain open lines of communication throughout the term of the agreement, the relationship between OIG and the entity is generally positive and productive, even (and perhaps especially) when out-of-the-ordinary events occur that might otherwise threaten its "probationary" status.

Preemptive communication

It is imperative that entities notify OIG in advance of any compliance challenges that the organization may be experiencing. This requires foresight on the part of designated compliance officers and keeps OIG aware of the entities' continuing efforts to ensure compliance.

Entities that keep those communication channels open tend to operate more successfully under a CIA than those organizations that fail to call OIG's attention to identified compliance problems. For example, OIG occasionally receives notification from entities that struggle to meet CIA requirements during the initial, implementation period. Based upon the nature of the challenges and the timeliness of the entities' notification to OIG of those issues, OIG will often agree to provide an extension of time for the provider to complete its obligations under the CIA.

Having monitored a wide variety of providers under CIAs, OIG also has some indication of the types of questions, notices, or disclosures that can be expected from providers or entities during the ordinary course of implementing and maintaining CIA compliance obligations. When such disclosures are not being submitted, it might send warning signs to, or raise questions with, OIG.

Early notification of problems and active dialogue could also prevent the later imposition of stipulated penalties. For example, OIG conducted a site visit to a provider and found that the entity was not in full compliance with certain provisions of the CIA, despite the fact that the provider gave no indication to OIG that it was not in full compliance with the terms of the agreement. In response to this identified breach, OIG assessed stipulated penalties against the provider for its failure to comply with the express provisions of the CIA. Had that provider notified OIG of any challenges associated with meeting its specific obligations, that penalty likely might have been avoided. It should be underscored, nonetheless, that an entity that consistently fails to meet CIA objectives will face consequences, even though it makes a good faith attempt to keep those lines of communication open.

There are "red flags" that may alert OIG that an entity is struggling to comply with its CIA obligations. Generally, the first sign that actual problems exist is when providers miss the filing deadlines for their implementation and annual reports and fail to request an extension. The CIA relationship is not a situation in which "no news is good news." A general lack of communication from an entity is a consistently accurate indicator that problems might be surfacing on the horizon.

The corollary to OIG expectations for entity disclosures is that entities must be willing to communicate reasonably and openly with OIG. That is not to suggest that the OIG monitor should be treated as the equivalent of a member of the entity's compliance staff. OIG is precluded from getting involved with, or providing advice to, a provider regarding its day-to-day compliance and/or operational activities. However, if an entity is unwilling to disclose its significant challenges or delays to OIG, that is often viewed by OIG as reflective of a possible culture of non-compliance at that organization.

The following sections detail the manner in which OIG evaluates compliance with certain key provisions of the CIA, and highlight

Continued on page 30

Walking the line: When providers "go wrong" under Corporate Integrity Agreements

...continued from page 29

problems or issues that some providers have experienced with respect to implementing the specific obligations of the CIA.

Compliance officer requirements

Compliance officers are required by the terms of the CIA to implement and oversee the obligations of the agreement across their organizations. OIG takes very seriously its requirement that compliance officers be members of senior management, and that compliance officers not be subordinate in any way to the general counsel (GC) or chief financial officer (CFO) at their organizations. The principle underlying this provision is self-evident — a compliance officer subordinate to the GC or CFO would have little leverage through which to enforce compliance policies and practices. It is equally important that providers select a compliance officer who thoroughly understands the terms of the CIA, as well as the seriousness of complying fully with that agreement.

The following example illustrates the manner in which OIG evaluates the compliance officer's role within an organization, specifically within the context of a CIA site visit, which is described in more detail below. OIG recently conducted a site visit and requested an interview with the compliance officer, as is routine during such visits. Although OIG generally interviews the compliance officer individually, this provider's GC and CFO insisted on being present for that interview. As OIG engaged the compliance officer in discussion, it became apparent that he was not able to answer basic questions regarding the provider's operations under the CIA, or to address specific questions regarding general compliance issues. The GC and CFO then began to answer the questions that the compliance officer should have been, but was unable to, address. It became clear to OIG that the compliance officer was subordinate to the GC and CFO in function and duty, and that the compliance officer was incapable of overseeing CIA implementation efforts. In this situation, OIG requested that the provider hire a new compliance officer to fulfill CIA-related obligations and responsibilities.

Training and certification provisions

CIAs generally include provisions for training employees and other covered persons on CIA requirements, as well as training on a provider's compliance program, code of conduct and policies and procedures. CIA training provisions generally indicate the substantive areas that providers must cover during training sessions. The OIG monitor will verify that those areas have been included and sufficiently addressed during the relevant training sessions and in the training materials. OIG will also review training materials to evaluate the quality, relatability, and comprehensiveness of those materials.

CIAs also require providers to obtain certifications from covered persons to evidence their attendance at these training sessions. OIG will, on occasion, request those certifications to determine whether the provider has trained covered persons pursuant to the requirements of the CIA.

Selection and performance of independent review organizations

CIAs generally require an entity to engage an independent review organization (IRO) to conduct annual audits and reviews, and to report its findings and observations from such reviews to OIG. The CIA not only requires the IRO to demonstrate the appropriate level of qualification and expertise to perform the engagement, but also requires the IRO to certify as to its objectivity and independence, pursuant to the standards for auditor independence set forth in the General Accountability Office (GAO) Government Auditing Standards (referred to as the "Yellow Book").

When an entity identifies its selected IRO in the CIA implementation report, OIG will review the IRO materials to determine whether the selection is appropriate and in compliance with CIA requirements. OIG will raise questions if an IRO does not demonstrate the requisite level of qualification, expertise, independence, and objectivity to perform the review under the CIA.

In a recent situation, OIG had concerns about the fundamental qualifications of an IRO selected by an entity. OIG requested more information regarding the IRO's qualifying experience but, despite the additional information provided by the IRO, OIG remained concerned that the IRO did not have the expertise or experience to perform the review as required by the CIA. OIG then requested that the provider identify an IRO that was more clearly qualified to perform the CIA review.

OIG will review the reports it receives from the IRO each year and explore any questions or concerns regarding the IRO's methodology, qualitative and quantitative findings, and overall recommendations. It might be expected that OIG will have follow-up questions and concerns with IRO reports that fail to identify any errors or recommendations for improvement.

There also have been occasions where OIG has not been able to determine from the IRO's report whether or not the IRO has performed the engagement pursuant to the express terms of the CIA. When these situations occur, OIG often will require clarification, or it may request the IRO's actual work papers to retrace the review process and work steps on its own. In at least one other instance, OIG has required that a provider replace its IRO, based upon OIG's substantive review of that IRO's annual review reports under the CIA. If OIG has reason to believe that the IRO's review fails to conform to the requirements of the CIA, or that the IRO's findings are inaccurate, OIG may, at its sole discretion, conduct its own review to determine whether the IRO review complied with all CIA requirements, or if the findings are inaccurate.

OIG site visits

OIG frequently conducts on-site evaluations of an entity's compliance with the terms of a CIA. On-site visits typically involve meeting with board members, senior management, and compliance staff in order to provide the organization with an opportunity to present on the status of compliance and CIA-related efforts. OIG monitors may conduct interviews, review documentation, and tour the facility in an effort to observe and explore how well the provider has implemented CIA obligations across the organization. The duration of the site visit varies, depending upon the size of the entity or the complexity of its business. Typically, site visits last from one to three days.

Site visits may be scheduled in advance with the entity; however, OIG may conduct an unannounced site visit, which may or may not be an indication that OIG suspects problems with an entity's CIA implementation and compliance. Each year, OIG will randomly select some providers for site visits, but other visits are scheduled specifically in response to an OIG-identified concern.

Stipulated penalties

If it is suspected that an entity may have committed a breach of its CIA, OIG will investigate the matter and may impose stipulated penalties, if the suspicions are verified. For the imposition of stipulated penalties, OIG relies upon the contractual remedies that exist for breach or default of the provisions of the CIA. To date, OIG has imposed stipulated penalties against 41 providers and has collected nearly $600,000 in penalties. A commonly assessed stipulated penalty is for failure to submit implementation and annual reports as required by the CIA.

If an entity has committed repeated or flagrant violations of the terms of a CIA, OIG may issue a Notice of Material Breach and Intent to Exclude. This notice provides the entity with the opportunity to avoid exclusion by demonstrating that it was either (1) never in breach or (2) that it has cured or will cure the breach within a specified time frame and to OIG's satisfaction. If the entity fails to do so, OIG will issue a Notice of Exclusion. These notices are intended to communicate that OIG will not hesitate to pursue an action against entities that fail to abide by their

Continued on page 32

Walking the line: When providers "go wrong" under Corporate Integrity Agreements *...continued from page 31*

integrity agreement obligations. To date, OIG has issued 21 Notices of Material Breach and Intent to Exclude and Notices of Failure to Comply. In all but two cases, the providers cured the underlying breach that gave cause to OIG's action.

OIG first exercised its contractual right to exclude a provider for breach of a CIA in 2006. South Beach Community Hospital (South Beach), a non-profit community hospital in Miami Beach, Florida, was excluded after OIG found it had repeatedly and flagrantly violated its obligations under the agreement. Specifically, OIG found that South Beach had failed to submit its implementation and annual reports by the due dates specified in the CIA, and never sought extensions to those submission deadlines. When South Beach ultimately submitted those reports, they failed to include a significant amount of required information pursuant to the express terms of the CIA. OIG also found that South Beach had failed to comply with the CIA's IRO requirements, because OIG did not receive all the cost reporting review reports over the term of the CIA, and because South Beach failed to retain an IRO during one year of the CIA. South Beach also failed to provide notification of its sale to another entity as required by the CIA. Days before OIG issued its Notice of Exclusion, South Beach filed for bankruptcy.

In 2007, OIG excluded an individual physician for material breach of a CIA, after OIG found he was in material breach of his agreement due to (1) his failure to submit an Annual Certification as required by the agreement, despite the fact that OIG issued repeated reminders and notices that the Annual Certification was past due, and (2) his failure to respond to OIG's Stipulated Penalties Demand letter.

Renegotiation of CIA provisions

OIG will generally not agree to renegotiate terms of the CIA. If there are legitimate and truly unforeseeable circumstances that prevent an entity from fully complying with the terms of the CIA, a provider can present that situation to OIG for discussion and resolution. Sometimes the CIA itself will allow the parties to revisit certain requirements during the term of the CIA. OIG may also be willing to discuss interpretation of certain terms if implementation proves to be unexpectedly onerous.

Conclusion

Providers who make an effort to meet CIA obligations in a diligent, responsible, and professional manner can expect to have a positive working relationship with OIG. Compliance officers charged with the responsibility of ensuring compliance with CIA obligations should be aware that prompt and open communication is key, as well as maintaining an appropriate level of appreciation for the ramifications that a CIA breach may have for the organization. Although OIG may routinely exercise its rights to impose penalties against recalcitrant entities, OIG does hope for a cooperative partnership with entities that operate under CIAs, to prevent any future harm to the federal health care programs. ■