

**“Building a Partnership for Effective Compliance”  
The Third Government-Industry Roundtable**

*A Report on the July 30, 2001 Roundtable Discussion on Corporate Integrity Agreements.*

**Background and Introduction**

On Monday, July 30, 2001, the Office of Inspector General (OIG) of the U.S. Department of Health and Human Services and the Health Care Compliance Association (HCCA) co-sponsored the third Government-industry roundtable. The roundtable discussions were an opportunity for health care providers operating under a corporate integrity agreement (CIA) to inform the OIG of the issues surrounding the implementation and maintenance of compliance programs. The meeting also offered the OIG the opportunity to present its CIA policy objectives and receive providers’ unique insights on ways to accomplish these objectives.

Over 50 compliance professionals and 30 government representatives attended the day long event, which was organized into a large group discussion and then a series of breakout sessions. The compliance professionals represented a wide spectrum of institutional and provider organizations and the Government participants included members of the OIG, Department of Justice, and the Centers for Medicare and Medicaid Services (CMS). The objective of the meeting was not to reach consensus on the many issues that surround compliance with health care program requirements, but rather share perspectives on implementing and maintaining effective compliance programs. All participants gained new insights into the challenges associated with maintaining effective compliance programs.

The OIG agreed to prepare a written summary of the discussions that took place at the roundtable throughout the day. We have consolidated the summary into four topic areas: independent review organizations (IROs), training and education, compliance infrastructure, and reporting to the OIG.

**Independent Review Organization Issues**

The meeting began with a group discussion of issues related to the OIG’s requirement that entities under a CIA retain an IRO to perform a billing, systems and compliance review. Among the issues addressed were the history and purpose of the IRO, the OIG’s consideration of a proposal to amend its billing review requirement to use a discovery sample instead of a probe sample, the advantages and disadvantages of the IRO, and how to make the IRO more cost effective and efficient.

***History and Purpose of IRO.*** Many CIAs or settlement agreements with integrity provisions require the entity to retain an IRO to perform a billing, systems and compliance review. Among the factors that determine if a provider is required to obtain an IRO are the existence of a voluntarily established and effective compliance program, a history of voluntary self-disclosure, and the demonstrated expertise and ability of the provider's internal audit staff to conduct independent reviews. The OIG requires IROs because the OIG does not have the resources to conduct the level of review necessary to determine if a provider is meeting the requirements of the CIA as well as other Federal health care program requirements. Additionally, a review by an independent entity provides the OIG with assurances that a provider's compliance program and billing systems are objectively reviewed.

***The Discovery Sample.*** The compliance professionals raised concerns about the cost of the IRO in performing the multi-level sampling and claims reviews. The OIG indicated that it is considering revising the IRO billing engagement to include the use of a discovery sample to determine what additional sampling might be necessary. The use of the discovery sample would offer a cost effective review for providers, while providing a comfort level to the OIG that providers have sufficient billing oversight. Under this methodology, providers would retain an IRO when internal audit systems were inadequate to conduct a review of a discovery sample of 45-50 claims. If the financial error rate determined by the discovery sample is less than 5 percent, the review would be complete and the provider would not be required to do any further IRO claims review for that year. If the financial error rate is above 5 percent, the provider would engage the IRO to conduct a statistically valid random sample (SVRS) of claims, using the discovery sample as the probe sample. If the financial error rate as determined by the SVRS is below 5 percent, no additional work is required for that reporting period and the provider would repay the identified overpayments in the SVRS.

If the financial error rate attributable to overpayments in the SVRS is 5 percent or greater, the error rate would be extrapolated to the universe and the provider would reimburse the relevant Federal health care program. Such providers would also be required to engage an IRO to perform a review of internal controls and systems. The objective of this review would be to identify and correct the cause of the billing irregularities.

Once a final determination is made with respect to a change in the CIA billing review requirements, any material changes made to the IRO requirement will be offered to providers who have already executed CIAs.

***Advantages and Disadvantages of the IRO.*** Considerable time was spent discussing the overall advantages and disadvantages of the IRO, and more specific discussions focused on each of the three components of a typical CIA IRO review: 1) billing engagement, 2) compliance engagement, and 3) systems review.

***Advantages.*** Numerous advantages of the IRO were cited. In particular, participants noted that IROs provided a broad industry perspective and expertise, are independent, helped identify system weaknesses, made helpful recommendations, and their reviews served as a useful benchmark for future reviews conducted by the provider. Providers recounted the benefits of the IRO in the first year of the CIA. For instance, one participant said that, although not required to do so by the CIA, their organization hired an IRO to perform training the first year, so they could benefit from the IRO's expertise and then conduct the training on their own in future years. Another provider said the systems review was invaluable, and only wished the overall assessment of internal controls had been performed earlier, so that they would have been able to make improvements to the system immediately, rather than a year after the CIA was executed. Providers had varying needs in the beginning of the CIA implementation process, but agreed that a "good" IRO definitely helped "jump start" their compliance program.

***Disadvantages.*** Participants also spent considerable time discussing their concerns about the cost incurred in using IROs. Smaller providers felt the cost of an IRO was not always consistent with the providers' size or the False Claims Act settlement. There also were concerns about the expertise of IROs. A provider of mental health services from a large metropolitan area observed it was difficult to find an IRO with expertise in mental health.

Other compliance professionals stressed that IROs have economic interests of their own, and might seek an engagement with a provider as a means for learning a new line of business. One compliance officer felt the IRO's services were duplicative of reviews performed by CMS. Others felt the IRO did not always understand the provider's business and were inefficient.

***Participants did not always agree with the IRO's findings.*** Government representatives recommended that providers raise disputes over audit findings with the IRO, and that if these issues can not be resolved, the provider should document the discrepancies and submit them with its annual report to the OIG. One compliance officer said the most valuable experience of the CIA's implementation was sitting down with the IRO for three days to examine the results of the claims

review. Although a grueling experience, at the end of the effort they were able to resolve disagreements over the IRO's findings, and the provider was better able to identify several areas for improvement to avoid problems from reoccurring.

### ***Cost Effectiveness and Efficiency of the IRO***

***Compliance Engagement.*** Many felt the compliance engagement was a good investment in the first year, but provided diminishing returns in the following years. Some felt the compliance engagement was not necessary, especially if the provider's compliance program had been in operation for a while. Others rationalized that it was not necessary to hire an external entity to perform a review of what is essentially the compliance officer's primary job function.

Participants embraced the idea of giving the compliance officer or chief executive officer, after the first year, the ability to conduct the compliance review internally (i.e., not retain an IRO) and personally certify that the provider complied with its CIA obligations.

***Billing Engagement.*** In general, participants expressed few problems with the billing engagement requirement and understood why the OIG would want some form of billing reviewed required for each year of the CIA. However, participants shared concerns and had some interesting ideas regarding the billing engagement.

***Underpayments vs. Overpayments.*** Most providers seemed frustrated by the lack of direction from OIG and CMS on the netting of underpayments against overpayments. Providers were heavily in favor of netting, but wanted more consistent direction on the netting out policy from CMS contractors. A CMS representative said contractors have been instructed to allow providers to net out appropriate underpayments when calculating overpayments. Further discussion took place as to the definition of underpayments. The OIG acknowledged that current CIAs define overpayments but do not define underpayments. OIG representatives explained that non-adjudicated services (services never billed) did not count as underpayments, but recognized the OIG may need to define how underpayments are to be considered during the billing audit.

Many providers noted they have conservative billing practices, especially when it comes to Evaluation and Management (E&M) coding, which many view as a subjective system. Providers felt the ability to net underpayments against overpayments was important to show both sides of the equation. As one provider put it, "netting would help alleviate some of the vagaries in E&M coding."

***Combining the Billing and Systems Review.*** The group discussed the idea of combining the systems review and billing engagement and conducting them at the onset of the CIA. This would give providers benchmarks at the beginning of the CIA period and help them address problem areas immediately, rather than waiting for results a year after the CIA was executed. The systems review was viewed as one of the most valuable functions performed by the IRO, but providers concluded a systems review conducted separate from the billing review is not as useful and is more expensive. Many agreed that combining the reviews is a good idea, but it would be beneficial if the OIG was more specific about the systems review requirements.

***Summary of IRO Discussion.*** Participants generally felt that even though the IRO engagement was expensive, and providers did encounter some difficulties, the IROs served a valuable role in the compliance and CIA process. Most participants said the IRO added value to their compliance program and they would use IROs periodically even after the CIA expired. Only one provider said that after the CIA expired it would do all compliance related functions internally. The majority of compliance officers felt IROs helped organizations highlight the importance of compliance and often gave the compliance officer the ability to get buy-in from senior management and employees.

Despite the benefits of the IRO, participants felt that organizations should be encouraged to develop the in-house audit expertise to enable the organization to perform independent and verifiable internal audits once the CIA term expired. Many believed that the IRO related expenses would not be funded by their management in years following the expiration of the CIA.

### **Training and Education**

A typical CIA requires providers to conduct general compliance education and specific substantive training for covered employees. Participants agreed that compliance training should cover topics such as: code of conduct, ethics, compliance program requirements, and corporate policies and procedures. Comprehensive training in the areas of billing and coding was viewed as imperative for the relevant employees and contractors. The training and education discussion was valuable to providers, as it allowed them to exchange ideas and learn what methods other providers are using to train their employees. Providers discussed challenges, shared innovative techniques and raised additional issues about the CIA training requirement.

***Training Challenges.*** Participants discussed the numerous challenges faced by providers who are trying to maintain effective training programs. Challenges included:

- developing and maintaining training programs that meet the requirements of the CIA;
- keeping employees interested in compliance training year after year;
- success in having employees (especially physicians) attend training; and
- tracking employee training (especially part-time, contract, and new employees).

***Innovative Techniques.*** Providers shared numerous techniques and made recommendations on how to overcome the challenges presented by training employees in large and small entities with varying resources. Techniques included initiatives such as:

- including compliance officers in CIA negotiations, as they best understand the training needs of the organization;
- using computer/web based training, interactive games (e.g., *Compliance Jeopardy*), case scenarios, and videos to keep employees interested in training from one year to the next; and
- providing short trainings (i.e., a maximum of 15-30 minutes) to physicians at their convenience at medical director meetings, during lunch, etc.

Because physicians have demanding schedules and are usually not direct employees of the hospital, compliance officers are continually challenged with the ability to persuade physicians to attend compliance training. Compliance officers suggested CMS implement a regulation that requires resident physicians to receive compliance training with a focus on documentation and coding issues during their residency programs.

***Potential Changes.*** Providers had numerous questions and ideas on how the OIG could improve the training requirement included in CIAs. Providers would like more flexibility to develop and tailor their training programs to their specific needs, rather than the requirements set forth in their CIAs.

For instance, providers would like the OIG to give providers the flexibility to determine the type of training and number of hours needed by the employees in their organizations. One compliance officer felt like the provider was simply “killing time” training certain employees, whose function did not necessarily warrant the type of training required by the CIA. Providers thought it would be more effective if they had the ability to develop and revise training based on problems discovered through the course of yearly audits. This way the training would focus on problem areas on which employees need to be educated. It was also suggested that the OIG consider language to require a “reasonable number of hours” or “minimum number of hours” of training for each year of the CIA.

In addition, some providers would like the OIG to develop training materials and/or training guidelines tailored specifically to types of employees. For example, doctors, nurses, nurses aides, billers, and coders all have different compliance training needs and providers would like more direction on how to train individuals with various needs. Government representatives mentioned that CMS offers training modules available on their website and providers who utilized this resource found it helpful.

***Additional Issues.*** Some providers questioned the OIG's rationale for requiring the content of compliance training to include the details of the CIA. The OIG believes building support from employees and senior management early on for the compliance program is a crucial component to implementing and maintaining an effective compliance program. Educating employees on the CIA helps to build support for the compliance program by raising an awareness of the CIA and its requirements. This training also helps employees appreciate the consequence for failing to comply with Federal healthcare program requirements. Most compliance officers agree with the concept of gaining support for the compliance program early on, especially from senior management and the Board of Directors; one compliance officer even suggested the OIG should require the Board of Directors to sign the annual report each year.

### **Compliance Infrastructure**

The purpose of the compliance infrastructure breakout session was to address common problems providers face while trying to maintain compliance programs. Topics included maintaining the compliance program after the CIA expired, dealing with high staff turnover, the confidential disclosure program and screening for ineligible employees.

***What happens after CIA expiration.*** Providers generally plan to continue their compliance programs after the CIA expires, but acknowledged some changes would probably occur. Potential changes include reductions in the amount of training, eliminating the use of IROs, and reducing the numbers of compliance staff.

Some compliance officers said the CIA provided support to allow them to convince the organization to embrace compliance and take it seriously. Providers who received senior management buy-in based on the CIA had concerns that the compliance program would lose momentum and funding after the CIA expired. Other compliance officers tried to downplay the CIA during the implementation of their compliance programs so the commitment to compliance would not wane once the CIA expired.

Providers also sought direction from the OIG on what happens when the CIA expires, given that almost none of the participants had reached that point in their CIAs. The OIG explained that once the OIG receives and reviews the last annual report from a provider, the OIG will send the provider a letter if any additional information is needed. If no outstanding issues exist, the OIG sends out an official release letter that relinquishes the provider from any future CIA obligations. In the close out letter, providers are informed that although the term for the CIA has concluded, the OIG still has the right to pursue violations of the CIA if the OIG learns the provider has breached its corporate integrity obligations during the term of the CIA, or has determined that the provider's annual reports were based on false or inaccurate information.

***Confidential Disclosure Program.*** Providers had two major concerns related to the CIA requirement that the provider establish a confidential disclosure program. Most providers have outsourced their compliance hotline and have found that because most hotline calls are human resource related, they did not feel they were getting their money's worth. Although CIAs require a confidential disclosure program, they do not specifically require that the provider outsource this function. One compliance officer revealed she installed an additional phone line for minimal cost and checked the voice mail daily to see if any reports had been made. Providers also voiced concerns about the type/scope of information required under the confidential disclosure program. The OIG requires that the compliance officer maintain a disclosure log, which includes a record and summary of each disclosure received, the status of the respective reviews, and any corrective action taken in response to the internal reviews.

***Screening for Ineligible Persons.*** Compliance officers also voiced concerns about the requirement to screen new and existing employees against the General Services Administration's (GSA) List of Parties Excluded from Federal Programs and the HHS/OIG List of Excluded Individuals/Entities. Participants acknowledge the OIG list is even easier to use since social security numbers have been added to the match list. However, most providers noted significant problems with the GSA list and asked why the Government could not combine the two lists.

### **Reporting to the OIG**

The Inspector General assigns one of its staff members to each provider operating under a CIA. This person is responsible for monitoring the provider's compliance with the CIA and acts as a liaison to the provider's compliance officer. A typical CIA requires the provider to submit a 120 day implementation report, an annual report, and separate reports regarding the circumstances of any ongoing investigations, legal proceedings, or material deficiencies. The Compliance Unit assesses each report to determine whether the

provider has complied with its requirements. As appropriate, the OIG follows up with the provider through written and oral communications and site visits to the provider's facilities.

***Working with the OIG.*** Several participants expressed interest in working more closely with the OIG regarding issues that arise under a CIA. Some expressed concern that if they raised issues, the OIG may try to use that against the provider. However, those compliance officers who have contacted the OIG's Compliance Unit reported that such contacts had been helpful and non-confrontational.

***OIG Site Visits.*** In addition to monitoring written reports, the OIG also conducts site visits of providers operating under CIAs. The OIG meets with compliance staff, management and others at the facility to try to gauge the effectiveness of the provider's compliance efforts. A participant who recently experienced such a visit relayed positive comments about the visit and the opportunity to educate the OIG as to the organization's operations. Such an opportunity allows the OIG to more effectively monitor a provider's compliance efforts in the context of its day-to-day operations.

***Scope and Format of the Annual Report.*** Some providers suggested the OIG provide a template that describes what should be included in the annual report. OIG representatives explained the OIG does have an Annual Report Content checklist on its website. Since the OIG deals with multiple provider types with various CIA requirements, its main concern is that the items outlined in the annual report section of the CIA are submitted, and not necessarily the format in which the report is submitted. If a provider has questions about the annual report format, it should contact the OIG Compliance Unit monitor for that particular provider.

***Disclosure of Material Deficiencies.*** The group discussed the definition of a "material deficiency" that would trigger reporting requirements to the OIG and the fact that the standard has evolved over time. However, the definition is still somewhat subjective. Several categories of matters are required to be reported: 1) large overpayments, 2) overpayments related to systemic weaknesses in the provider's controls, 3) conduct that appears to violate the law, and 4) in some cases, quality of care issues. Providers said they would like the ability to report overpayments to the OIG quarterly, rather than the 30 days now required. They explained that this requirement has created accounting problems, since the contractors only require quarterly reconciliations.

***The Application of FOIA to a CIA Annual Report.*** Submissions pursuant to a CIA are subject to the Freedom of Information Act (FOIA). The OIG representatives explained that providers may assert that certain documents are exempt from disclosure under FOIA

(e.g., trade secrets). Providers should only designate documents as FOIA-exempt if there is a good faith basis for such a designation. The OIG will handle requests for documents submitted under a CIA under the normal FOIA process set forth in the regulations.

### **Conclusion**

The participants agreed that the outcome of this collaborative effort between the OIG and providers operating under CIAs was a positive one. Participants explored many of the issues confronting compliance officers and staff. They gained new insights into the challenges of creating effective compliance programs and had the opportunity to experience perspectives on compliance from both the Government and others in the health care industry. The outcome of the roundtable discussions will increase communication between the Government and the provider community to foster their ability to work together to protect the integrity of the health care system. Given the constructive discussion among the participants, consideration will be given to creating additional opportunities for Government-industry exchanges on these and other issues surrounding health care compliance programs.