Corporate Integrity Agreements: Understanding Compliance Risk and Obligations to the Government

By: Kimberly J. Commins-Tzoumakas and GinaMarie F. Geheb
Hall, Render, Killian, Heath & Lyman, PLLC

Editor: Patricia A. Stamler
Hertz Schram PC

Corporate Integrity Agreements: Understanding Compliance Risk and Obligations to the Government

The Department of Health and Human Services' Office of the Inspector General ("OIG") and the Department of Justice ("DOJ") investigate and enforce fraud and abuse violations committed against federal health care programs[1] under a robust rubric of federal laws aimed at eliminating fraud, abuse and waste in the health care system. These laws include the federal False Claims Act,[2] the Civil Monetary Penalties Law,[3] the Anti-Kickback Statute,[4] and the Program Fraud Civil Remedies Act[5] (collectively, "fraud and abuse laws"). The DOJ's and OIG's investigations and enforcement actions focus, in part, on whether the health care entity had more globally implemented and maintained a comprehensive compliance program to minimize or eliminate the perpetration of fraud and abuse on federal health care programs.

The OIG has published compliance guidance outlining the key elements of an effective compliance program for (1) nursing facilities, (2) recipients of PHS research awards, (3) hospitals, (4) pharmaceutical manufacturers, (5) ambulance suppliers, (6) individual and small group physician practices, (7) Medicare+Choice organizations, (8) hospices, (9) durable medical equipment, prosthetics, orthotics, and supply industry, (10) third-party medical billing companies, (11) clinical laboratories, and (12) home health agencies.[6] In March 2017, the OIG published additional guidance for providers on the method for measuring compliance program effectiveness (the elements and measurement guidance are collectively referred to as "OIG Compliance Guidance").[7] Additionally, the DOJ has published a list of sample questions it uses during investigations when it is evaluating corporate compliance programs.[8] It is extremely helpful for a health care entity to be able to demonstrate its compliance with this guidance – both in its written policies and procedures and its operational reality – when the government is assessing whether a Corporate Integrity Agreement ("CIA") is needed following resolution of a particular compliance matter.

Implementing all the elements of an OIG recommended compliance program, understanding how to assess this compliance program and understanding the DOJ's assessment during an investigation will put a health care organization in the best position to demonstrate its commitment to and implementation of compliance, in the event of a government audit or investigation. Even with a robust compliance program, health care organizations live in a world of increasing government scrutiny and enforcement of the fraud and abuse laws. After an investigation and/or enforcement action has occurred, a CIA is one tool in the OIG's arsenal used to validate claims submitted by a health care entity to federal health care programs.[9]

This white paper provides an overview of (1) the purpose and scope of CIAs, (2) negotiating and understanding the terms of a CIA, (3) operating under a CIA, and (4) considerations of contracting with an entity under a CIA. It is intended as a general guide for attorneys counseling health care entities. While this white paper may be informative for non-attorneys and health care entities, each are strongly encouraged to seek the advice of an experienced health care attorney regarding the issues discussed herein.

I. Background on Corporate Integrity Agreements

A CIA may be part of a settlement arrangement between the OIG, the DOJ and a health care entity to resolve allegations that the health care entity violated federal fraud and abuse laws. During government

investigations into allegations of fraud and abuse, the DOJ and OIG evaluate the potential risk of future violations and risk to federal health care programs, weighing whether exclusion, heightened scrutiny, or integrity obligations may be warranted.

The OIG has issued guidance detailing[10] when and how it evaluates exercising its permissive authority to exclude a health care entity from participation in federal health care programs[11] or to impose integrity obligations on the health care entity. The OIG has indicated that it evaluates (1) the severity of the allegations, (2) the comprehensiveness of the entity's existing compliance program and what steps were taken to improve that compliance program to prevent repeat and future misconduct, (3) whether a voluntary self-disclosure was made, and (4) the weight of the evidence supporting the allegations of fraud.[12]

If the OIG concludes that exclusion is not necessary but that integrity obligations are needed to mitigate further risks, the OIG will require a CIA. In recent years, CIAs have typically involved a five-year term, unless the entity's settlement payment obligations to the DOJ are longer, and typically address one or more of the following issues, depending on the type of health care entity.

a. **Corporate Compliance Program Requirements**. Most CIAs impose reporting and operational requirements on the entity with the intention of promoting compliance with federal health care program standards. This is often accomplished by attempting to build a more robust compliance program and to address misconduct in coding/billing functions to prevent, identify, report, or correct fraud and abuse. Further, the OIG monitors certain safeguards from the OIG Compliance Guidance, including:

- Hiring or designating a Compliance Officer and/or a Compliance Committee;
- Developing written standards, policies, and procedures;
- Implementing comprehensive training for employees and, potentially, the entity's Board of Directors;
- Retaining an independent review organization ("IRO") to conduct annual reviews (if applicable and as further described below);
- Establishing a confidential disclosure program;
- Restricting employment of ineligible persons;
- Reporting overpayments, reportable events, and ongoing investigations/legal proceedings to the OIG; and/or
- Providing implementation and annual reports to OIG on the status of the entity's compliance activities.[13]

The OIG expects existing voluntary compliance programs to be tailored to the relevant OIG Compliance Guidance for the entity's specific provider type and take into account the size and scope of the entity. For example, the OIG has acknowledged that an anonymous reporting hotline for compliance violations is feasible for hospitals but may be cost prohibitive for small physician group practices where an anonymous drop-box may be more practicable.[14]

b. **Claims Review.** If the issues resolved involve allegations of false claims due to billing or coding errors, the CIA will generally include requirements that the entity engage an IRO to conduct an annual review of certain claims and report those findings to the OIG at the end of the year.

c. **Quality of Care**. The OIG may require a "quality of care" component to a CIA when the allegations against the health care provider are that the services were of such poor quality that they should not have been submitted for reimbursement. These "quality of care" CIAs require that the health care provider retain external clinical expertise to:

- Perform quality reviews of the services performed by the health care provider, including potentially assessing the health care provider's ability to prevent, detect, and respond to patient care concerns;
- Evaluate the health care provider's peer review and medical credentialing systems; and/or
- Review the medical necessity and appropriateness of certain admissions and medical procedures.[15]

d. **Referral Sources**. Certain CIAs address allegations of misconduct in referral sources, focusing on the financial relationships between the entity and actual or possible referral sources. Specifically, the CIA may contain certain monitoring requirements related to the relationships between referral sources and the entity and require improved policies and procedures regarding referral arrangements.

e. **Covered Functions or Non-Provider Entities**. CIAs for non-provider entities in the health care industry, such as pharmaceutical and device manufacturers, are becoming more common. Typically, these CIAs are put in place when allegations of fraud and abuse center on Anti-Kickback Statute violations related to the selling, marketing, or promoting of goods that are reimbursable by federal health care programs. These allegations include off-label promotion or violation of regulations promulgated by the federal Food and Drug Administration ("FDA"), provisions of billing or coding advice or inappropriately structured rebate or discount programs. These CIAs may also cover entities performing non-clinical services that are reimbursable by federal health care programs, including disease management programs or inventory restocking programs (such as durable medical equipment, pharmaceuticals, and consignment relationships). In such cases, the OIG will identify the misconduct and require the use of an IRO to monitor the non-compliant risk area(s) and report back to the OIG.

Each CIA is tailored to address the alleged specific violations related to a particular investigation and settlement. Thus, CIAs are not "one size fits all" and may not include all the above elements or address the same considerations.[16] The entity is in the best position to explain to the OIG what proposed requirements may or may not work based on its size and scope of the entity. The negotiations surrounding the scope and content of the CIA are critical to success over the lengthy government monitoring process. The OIG has a template that it tailors to the specific situation; however, entities should carefully review and negotiate specific nuances and changes, as warranted.

II. Negotiating a CIA

At the point in which a health care entity has agreed to enter into the CIA with the OIG, it has likely spent a long time defending against a DOJ investigation of allegations of violating one or more fraud and abuse laws. The entity is now looking towards the future with a keen eye focused on improvement of its compliance program. The first step in this process is negotiating the terms of the CIA with the OIG – an important step for the entity as it sets the stage for the relationship with the OIG and can be vital to avoiding complications and penalties for the duration of the CIA. As the entity engages in the negotiation process, the entity and its counsel should consider the following issues.

a. **Identify Likely Components of the CIA and Review Existing CIAs**. Review the DOJ's and OIG's allegations and inquiries to identify the scope of the alleged misconduct at issue and the elements of the CIA that will likely be included based on the alleged misconduct. Once these items are identified, review the CIAs that the OIG makes publicly available on its website[17] for similarly situated entities and allegations. This will be beneficial to the entity since the OIG strives to apply a consistent standard based on allegation and entity type. However, since the OIG's CIAs are constantly evolving, it is prudent to review the most recent comparable CIAs to better understand the OIG's current thought process.

b. **Identify the Negotiating Team**. It is important to identify a key individual in the legal department (whether in-house or outside counsel) and the Compliance Officer who will lead negotiations with the OIG. Behind the scenes, a team should be identified to carefully review each element of the CIA and the entity's ability to comply with each proposed requirement. Those involved should typically include members of the legal and compliance departments and members of management/operations responsible for implementing the requirements, thereby, establishing a team who effectively understands the entity's current operations and limitations and recognizes that adjustments to such departments will likely be made under the CIA. It is also important to work with the entity's finance department to identify the increased costs that will be incurred during implementation. Costs often include the engagement of (1) a third party to assess and monitor the compliance program, (2) an IRO on an annual basis, (3) a third party to perform pre-testing, and (4) additional resources for the compliance department to address any weaknesses identified in the program through the investigation process.

c. **Communicate the Intent and Purpose of the CIA to the Leadership Team**. In order to ensure success in finalizing and implementing a CIA, it is crucial to educate all members of entity's leadership regarding the risks of exclusion from participation in federal health care programs, the impact of the CIA and what benefits the CIA may bring. The CIA benefits may include a more robust compliance program that could avoid future government investigations, fines, and penalties by identifying and remedying risk areas before the government becomes involved. Financially, it is also important that the entity has a firm understanding of the resources necessary to meet the expectations of any imposed CIA obligations. These financial obligations may include paying for training, audits, consultants, external legal fees, monitors, and the IRO.

d. **Provisions of a CIA**. As noted above, the OIG generally ties the CIA back to the OIG Compliance Guidance elements, so legal counsel should be prepared to review the following terms for inclusion in the CIA based on the entity's existing compliance program.

1. **Identifying Entities Covered by the CIA**. For organizations with layers of affiliates and subsidiaries, it is vital to ascertain which specific entities the CIA covers. The OIG is likely to start with the position that the CIA applies to all entities within an organizational framework. However, entities can negotiate the scope of CIA based on the entity where the conduct occurred. Counsel should identify the affiliates and/or subsidiaries which it believes should be subject to the CIA and be prepared to discuss with the OIG why limiting the CIA to such entities is appropriate. This analysis is imperative because failure to limit the CIA to the specific entities at issue may result in imposing the CIA on all entities within the organization (which can be particularly significant for large organizations), including all the costs of complying with the CIA and increased scrutiny by the OIG on entities which may have little or no control over the affiliated entity settling the allegations.

2. **Identifying Covered Persons**. Each CIA will set forth to whom it applies and denote such individuals as "Covered Persons" under the CIA. Covered Persons usually must receive training, both general and specific to the job and subject matter. Counsel should identify operational departments and individuals that align with the purpose of the CIA and work with the OIG to narrowly define, as much as possible, Covered Persons. This will aid in limiting the scope of training and other obligations to individuals who have involvement in the entity's daily operations and will guard against including staff that are not involved in the daily operations. Additionally, counsel should further define whether third parties with which the entity contracts may be considered a Covered Person under the CIA such that the entity is obligated to provide those third parties training (further discussed below from the third party's perspective).

3. **Compliance Officer and Committee**. Most CIAs will include a provision identifying the requirements and obligations of the Compliance Officer and his or her oversight by a Compliance Committee or the entity's leadership. Compliance Officers are expected to have a direct line of access to the Board of Directors and report directly to the Chief Executive Officer or organizational leader. Most CIAs will require at least quarterly reporting to the entity's Board of Directors and will require that the Compliance Officer serve as part of senior leadership within the organization. Likewise, the Compliance Committee will typically be required to meet quarterly and be comprised of members of senior leadership.

4. **Code of Conduct**. Each CIA will require the entity to develop a code of conduct or enhance an existing code of conduct, policies and procedures, and implement training and education within the first 90 to 120 days and on an annual basis thereafter. The timeframe for training is often negotiable to some degree, if there are compelling factors. The codes of conduct and policies and procedures should align with the OIG Compliance Guidance for the type of entity, as they will require the approval of the assigned OIG Monitor (as discussed below).

5. **Board of Director Engagement**. CIAs generally require the entity's Board of Directors to receive training and oversee the Compliance Officer and program. The Board of Directors may also be required to present an annual resolution representing that the Board actually oversaw the compliance program activities and that the entity complied with fraud and abuse laws and the CIA. Educating the Board of Directors on the significance of its attestation at the beginning of the CIA is important to ensure that there are not concerns with signing the CIA attestation at the end of each year. This is critical, because the government could allege that such a certification was false, which could result in a new False Claims Act inquiry and potential liability for the individuals involved.

6. **Reviews and Certifications**. The CIA will require the entity to conduct annual reviews and risk assessments, including reviews by the IRO. These reviews can be expensive and can lead to mandates to correct any errors the IRO discovers and the need for refunds to be made to federal health care programs. If significant errors are found in any reporting year, additional auditing, training, and monitoring can be imposed and can be costly. Depending on the nature of the CIA, managerial personnel (e.g., Chief Executive Officers, Chief Financial Officers, Chief Medical Officers, or directors of business units) of the entity may be required to certify that their business units are in material compliance with the CIA and fraud and abuse laws.

7. **Independent Review Organizations or Independent Monitor**. While the inclusion of an IRO is not negotiable, the OIG will work with the entity to establish the details of the review,

which are typically aimed at reducing the potential for actual problems to arise (IRO selection and details are further described below). For quality of care CIAs, an independent compliance monitor may be required to observe the ongoing operations of the entity and review the entity's compliance with the CIA's requirements and the fraud and abuse laws. Both IROs and independent monitors are obligated to report their findings to the OIG. The OIG typically reserves the right to require the entity to engage a new IRO if the objectivity of the initial IRO become questionable.

8. **Screenings and Disclosures**. Every CIA, regardless of the entity type, will require the screening for ineligible persons (individuals excluded from federal health care programs) and require disclosure to the OIG of any violations of the fraud and abuse laws and/or other applicable laws.

9. **Notification Obligations**. CIA entities must notify the OIG of certain events under short timeframes as required by the CIA. Some examples of notifiable events include (1) any investigation or legal proceeding related to crimes or fraudulent activities, (2) any identified overpayments and repay such payments within 60 days, (3) certain reportable events, including overpayments, violations of fraud and abuse laws, or violation of federal FDA laws or regulations, (4) employing or contracting with an ineligible person, (5) filing for bankruptcy, and (6) changes in business operations, such as location changes, unit closures, sales, or purchases of certain health care assets as part of the provider entities. It is important to engage the OIG Monitor and to be transparent (as discussed below), while the entity decides whether a particular overpayment is significant or a particular matter is reasonably considered to be a violation of fraud and abuse laws, which may trigger a reporting obligation.

10. **Reports**. The CIA will outline the types of scheduled reports the OIG expects to receive from the entity. These reports include annual reports regarding compliance with the CIA requirements and certifications of accuracy from the Compliance Officer and others. Typically, in the first reporting year, the Compliance Officer will be required to submit an implementation report which will include an assessment of work done to date and the entity's activities to begin achieving the benchmarks outlined in the CIA. Thereafter, annual reports are required. Annual reports typically include (1) an account of any reviews, audits, or analyses related to the compliance program, (2) a response by the entity to such reviews, audits, or analysis, and (3) a summary of any overpayments refunded during the reporting period.

11. **Audit and Inspection Rights**. Under the CIA, the OIG will have expanded audit rights to inspect and review the entity's records and conduct interviews – a right greater than the law mandates – to assess the entity's compliance with the CIA and the fraud and abuse laws.

12. **Penalties**. All CIAs now include stipulated penalties for failure to comply with the CIA. These penalties may include daily penalties for failure to have (1) a Compliance Officer, (2) a code of conduct, (3) perform training, (4) failure to timely submit reports or engage the IRO, and (5) providing false certifications under the CIA. In the event the OIG seeks such penalties, the entity has the same rights it would have during the initial investigation of the allegations except the focus is on the entity's alleged failure to comply with the CIA.[18] Inclusion of such penalties in the CIA is typically non-negotiable.

13. **Material Breach and Exclusion from Federal Health Care Programs**. Each CIA contains a provision related to "material breach" of the CIA. A material breach can result in the entity's exclusion from federal health care programs. CIAs traditionally define "material breach" as (1) repeated or flagrant violations of any of the CIA's obligations, (2) failure to report a reportable event, take corrective

action, or make appropriate refunds, (3) failing to respond to a demand letter regarding stipulated penalties, and (4) failing to engage an IRO. The entity will receive notice of such breach and it has a right to cure the identified material breach – typically within 30 days. Inclusion of this material breach provision is typically non-negotiable in the CIA.

14. **Dispute Resolution**. The entity may appeal a stipulated penalty or exclusion from federal health care programs to an administrative law judge and then to the Departmental Appeals Board. The ruling by an administrative law judge or the Departmental Appeals Board (if appealed) is final.

15. **Additional Terms**. Each CIA is unique and thus there may be additional or logistical terms addressed in the CIA due to the facts and circumstances or the evolution of the CIA process.

Successful negotiation of a CIA requires the entity to understand the terms and scope of the CIA with the understanding that the OIG expects transparency, and that the adversarial role with the OIG during an investigation shifts to one of collaboration as the CIA takes effect and is implemented with the oversight of an OIG Monitor.

III. Operating Under a Corporate Integrity Agreement

The entity, after negotiating the CIA, must implement the terms expeditiously to ensure ongoing compliance with the expectations of the OIG. Operationally, this includes identifying an implementation team to track and assess the ongoing compliance of the entity. Absolute compliance in the early days of a CIA, along with full transparency, is key to a successful completion of the CIA. Importantly, the entity should establish the required policies and procedures addressed in the CIA, and policies and procedures that will maintain compliance with the expectations of the CIA. As the entity implements the CIA, it should consider the following issues.

a. **OIG Monitor**. Shortly after the effective date of the CIA, the OIG will assign an OIG Monitor responsible for overseeing the implementation of the CIA's requirements, answering the entity's questions, and facilitating the development and efficacy of the compliance program that must be capable of identifying and remedying compliance issues. With these responsibilities, the OIG Monitor is an important component of the CIA and is fundamental to assisting the entity to "right-size" its operations. The OIG Monitor is typically an attorney, but not the same attorney who negotiated the CIA and is viewed as a collaborator by the OIG. The OIG Monitor establishes a relationship with the Compliance Officer and should anticipate that the CIA implementation will not be perfect. Thus, it is critical that the Compliance Officer develop a good working relationship with the OIG Monitor and maintain an open line of communication. As a result, the OIG Monitor acts as a liaison between the entity and the OIG throughout the duration of the CIA. OIG Monitors oversee the effectiveness of the compliance program and the process the entity uses to resolve compliance issues to ensure the same or similar issues are prevented in the future. When issues arise, the entity should proactively reach out to the OIG Monitor to prevent the assessment of penalties. Furthermore, the OIG Monitor expects the entity to apprise him or her of key events occurring within the entity, including leadership changes and new investigations or issues. OIG Monitors expect adherence to timeframes for report obligations. The OIG Monitor is the person in the best position to provide leniency or clarification on items required by the CIA. Thus, establishing a dialogue early on is critical to successful CIA implementation and compliance.

b. **Engagement of Leadership**. Successful compliance with a CIA also requires the entity to have a culture change and engagement from the "top down." The leadership, including the executive team and the Board of Directors, should foster a culture of compliance – and not just because the CIA requires them to do so. The OIG looks for transparency and cooperation in transforming the entity into an entity that has a robust compliance program. The entity's cooperation and transparency starts with its leadership engaging in the compliance program, assisting with risk identification, mitigation, and selection of the IRO.

c. **Independent Review Organizations/Monitoring**. After establishing a relationship with the OIG Monitor and engaging the entity's leadership, the entity needs to select an IRO. IROs are typically an accounting, auditing, law, or consulting firm that provides independent and objective review of the entity's compliance with the CIA and the fraud and abuse laws. The OIG views the IRO as an extension of the OIG's auditing and monitoring function (since the OIG does not have the resources to perform such task for all CIA entities) and the IRO submits its findings to the OIG. Objectivity and independence are vital components of the IRO's function. Thus, the IRO must not have had a prior working relationship with the entity and cannot employ individuals who are related to anyone at the entity. The OIG has issued guidance on an IRO's independence and objectivity which focuses on compliance with the ethical principles and standards outlined in the *GAO Government Auditing Standards (2011 Revisions)* (a.k.a., the Yellow Book).[19] While the entity selects the IRO, the CIA typically requires the OIG to approve the IRO and, if necessary, to replace the IRO should it determine that the IRO is not acting independently and with objectivity. The entity's selection of an IRO should be done cautiously and should include interviews to ensure the IRO has the requisite experience and understanding of the entity's issues. In our experience, entities who do not perform this due diligence may have to replace the IRO during the term of the CIA. The replacement of an IRO results in additional expense in locating a second IRO and requires resolution of issues related to the first IRO.

When engaging in an IRO for services, the entity should consider the following factors:

- The scope of the CIA, including which specific incident(s) triggered the need for a CIA.
- The IRO's familiarity with OIG Compliance Guidance and compliance efforts related to the specific incident(s) that triggered the CIA.
- The IRO's prior work as an IRO in a similar capacity to the entity's needs under its specific CIA and prior approval by the OIG to perform IRO services.
- Whether there are conflicts of interest with the IRO (e.g., the IRO cannot review any work or areas it developed for the entity prior to the CIA).
- Whether the IRO will offer the entity written representation and warranty that it will comply with the Yellow Book and identify the exact individuals with experience who will provide IRO services.
- The cost of hiring an IRO and the need to engage in robust auditing well in advance of the IRO process to ensure errors are caught and corrected before the IRO conducts its review.

As noted above, the IRO will report any, and all findings to the OIG, so it is important to establish a collaborative and transparent relationship with the IRO.

d. **Reportable Events**. The entity should develop a mechanism to track reportable events and other obligations under the CIA that require disclosure to the OIG. This tracking mechanism will ensure that incidents are timely reported to the OIG in accordance with the CIA. Including the Compliance

Officer in key meetings, to ensure that information is shared timely, is critical to allow appropriate reporting of all required events. It is recommended to have a back stop (typically someone in the legal department) who is also monitoring reportable events. These reportable events and obligations should be identified and communicated to key leadership personnel. The process to report such matters to the Compliance Officer should also be communicated to key leadership. Routine reporting to the Board of Directors or a committee thereof on reportable events should occur as well. It is also important to advise the OIG when a confidential item is filed and that the entity is requiring that the report be exempt from Freedom of Information Act ("FOIA").[20] This will ensure that the confidential item is not disclosed publicly. The OIG has noted that all information provided under the CIA reporting process is not exempt from FOIA. Thus, the entity must work with counsel to determine what information is appropriate for exemption under FOIA.

e. **Implementing Training Programs**. Typically, within 90 to 120 days after the CIA is effective, the entity must develop and implement training programs for Covered Person(s) and, likely, its Board of Directors. The entity should determine quickly whether it will prepare such materials in-house or engage a third party to provide such training, keeping in mind that some training will require familiarity with the terms of the CIA. The entity will need to track who received the training, the type received, and further establish a plan for ongoing annual training as required by the CIA and recommended by the OIG Compliance Guidance. Termination of employees who refuse to comply with training requirements is expected. It is also important to train staff on the certification requirement early in the process so the executive leadership understands the certification expectations and will be willing to comply. Establishing an internal sub-certification process is often beneficial to achieving full compliance. As stated above, it is critical for management to be actively involved and knowledgeable about what they are certifying given the potential risks associated with an uninformed or false certification.

Complying with the terms of the CIA require a robust managerial approach to compliance that manages the relationship with OIG, the IRO, and within the entity. Furthermore, the entity can expect to expend significant internal and external resources (e.g., consultants, auditors, etc.) at its own expense.

IV. Entering into an Arrangement with an Entity Under a Corporate Integrity Agreement

CIAs are becoming very common among reputable health care providers. They are no longer akin to the scarlet letter. Nevertheless, there are certain considerations entities should make when deciding to enter into arrangements with an entity subject to a CIA. The contracting party should scrutinize the CIA to assess risk and the reach of the CIA, including the following topics.

a. **Review by the IRO and/or OIG of the Transaction or Agreement**. As outlined above, CIAs can include requirements for IRO review and monitoring, which may contain arrangements between the entity and third parties with whom it does business. As a result, the IRO could review the contracting party's arrangement with the entity. The IRO's review results are provided to the OIG. Release of information to the OIG could lead to further inquiries about the contracting party by the OIG, or other government agencies, since government agencies often collaborate or share information.

b. **The Circumstances of the CIA**. Typically, the CIA results from investigations by the OIG and the DOJ, so a contracting party should take care to perform thorough due diligence of the circumstances leading to the CIA. The due diligence should include analyzing whether the arrangement with the contracting party implicates any of the practices for which the entity was sanctioned.

c. **The Nature of the Services or Goods provided by the Entity**. In vetting any risk associated with the entity, the nature of the goods or services being purchased by the contracting party should be reviewed.

d. **Reach of the CIA to the Contracting Party**. CIAs can require the entity to insert language in certain contractual arrangements identifying corporate compliance obligations. The OIG requires the entity to identify "Covered Persons" to which the entity has a more robust obligation, such as training. The scope of Covered Persons may extend beyond the entity's personnel to the contracting party's personnel. In such circumstances, the contracting party should:

- Review whether the CIA imposes any obligations on parties with which the entity contracts; and
- Establish who determines whether the contracting party's personnel are considered "Covered Persons" under the CIA and seek clarification from entity as to whether a contracting party's personnel are considered Covered Persons and request that the entity confirm with the OIG that the contracting party's personnel are Covered Persons.

If the contracting party's personnel are Covered Persons and the entity is required to perform training for Covered Persons, then the contracting party should consider how this training will be implemented; including (1) the content of the training provided to contracting party's personnel and whether it conflicts with the contracting party's interpretations of the covered laws, (2) whether the training will need to be provided to each of contracting party's personnel, and (3) ensuring the cost of the training is at the expense of the entity subject to the CIA.

e. **Geography**. As health care companies continue to become more national (e.g., long-term pharmacy care outsourcing, perfusion services, dialysis services, etc.), with subsidiary or affiliate entities providing services throughout the country, contracting parties should review whether the CIA targets the entity as a whole or specific subsidiaries, affiliates, or locations.

f. **Risk if the Entity Violates its CIA or is Excluded**. If the entity violates its CIA, the OIG may review all arrangements the entity has with third parties. This puts other parties under the lens of the OIG. If the entity materially breaches the CIA without cure, then it could be excluded from participation from federal health care programs. If this occurs, it could have a significant adverse effect on the contracting entity depending on the nature of the goods or services provided by the entity who breached its CIA (e.g., billing for an excluded provider's services or subjecting the contracting entity to government scrutiny for its own practices). As noted above, the CIA should be carefully reviewed to determine what conduct triggers potential exclusion from federal health care programs, focusing on potential exclusion of subsidiaries and affiliates that are in the geographic location of the contracting party. At a minimum, the contracting party will need to have language in its arrangement with the entity allowing it to terminate its agreement if the entity is excluded from participation for any reason.

After reviewing the scope of the CIA and its potential impact on the contracting party, the contracting party should evaluate its arrangement with the entity to ensure that:

- Any proposed language included in the arrangement aligns with the requirements and obligations in the CIA.

- That the parties have a clear understanding of the CIA and its impact on the arrangement and on the contracting party's operations, business and personnel.
- The contracting party has included contractual protections for breach of the CIA, including, notification, indemnification, and immediate termination for any breach of the CIA or exclusion from participation in federal health care programs.

Each contracting party will need to evaluate its circumstances and risk tolerance for OIG or other government agencies' scrutiny based on the factors above. This evaluation should occur before entering into a relationship with an entity subject to a CIA or after receipt of notice that an entity has entered into a CIA. As noted above, the OIG maintains copies of current CIAs on its website for public review that can assist the contracting party with performing due diligence.[21] The DOJ typically releases press releases summarizing the allegations and misconduct for which the entity is being held accountable. However, DOJ settlements are not available online. It is important to note that many entities settle allegations that it may fully dispute in order to move on from the investigation. Thus, a settlement or a CIA does not always mean the entity engaged in wrongdoing. In addition, such entities are often operating as a "best practices" organization and thus may well be the best entity to do business with, depending on the facts and circumstances.

V. Conclusion

While there is no firm guidance on interpreting CIAs (other than the CIA itself), the OIG has conducted roundtables to obtain feedback on the CIA process and implementation of CIAs.[22] Additional guidance may be forthcoming based on the roundtable feedback. Even though no entity voluntarily elects to enter into a CIA with the OIG, attorneys should encourage their clients to embrace the benefits of a CIA. These benefits include being able to self-identify a risk area before a whistleblower (e.g., a *qui tam* relator) or the government does and thus avoiding another investigation. Legal counsel can help their clients navigate the complexity of compliance requirements proactively by educating their clients about CIAs and encouraging periodic audits of existing compliance programs to address compliance concerns before additional allegations of fraud and abuse violations are made.

[1] *See* 42 USC 1320a–7b(f) which defines "Federal health care program" as: "(1) any plan or program that provides health benefits, whether directly, through insurance, or otherwise, which is funded directly, in whole or in part, by the United States Government (other than the health insurance program under chapter 89 of title 5); or (2) any State health care program, as defined in section 1320a–7(h) of this title."

[2] 31 USC 3729 through 3733.

[3] 42 USC 1320a-7a.

[4] 42 USC 1320a-7b.

[5] 31 USC 3801 through 3812.

[6] *See DEP'T OF HEALTH & HUMAN SERVICES, OFFICE OF THE INSPECTOR GENERAL, COMPLIANCE GUIDANCE*, https://oig.hhs.gov/compliance/compliance-guidance/index.asp.

[7] *See DEP'T OF HEALTH & HUMAN SERVICES, OFFICE OF THE INSPECTOR GENERAL, MEASURING COMPLIANCE PROGRAM EFFECTIVENESS: A RESOURCE GUIDE* (Mar. 27, 2017), https://oig.hhs.gov/compliance/101/files/HCCA-OIG-Resource-Guide.pdf.

[8] *See DEP'T OF JUSTICE, CRIMINAL DIV., FRAUD SECTION, EVALUATION OF CORPORATE COMPLIANCE PROGRAMS*, https://www.justice.gov/criminal-fraud/page/file/937501/download.

[9] 74 Fed. Reg. 52964, 52965 (Oct. 9, 2009).

[10] *See DEP'T OF HEALTH & HUMAN SERVICES, OFFICE OF THE INSPECTOR GENERAL, CRITERIA FOR IMPLEMENTING SECTION 1128(B)(7) EXCLUSION AUTHORITY* (April 18, 2016), https://oig.hhs.gov/exclusions/files/1128b7exclusion-criteria.pdf.

[11] 42 USC 1320a-7b(7).

[12] *CRITERIA FOR IMPLEMENTING SECTION 1128(B)(7) EXCLUSION AUTHORITY*, *supra* note 10.

[13] *See* 74 Fed. Reg. at 52965; *DEP'T OF HEALTH & HUMAN SERVICES, OFFICE OF THE INSPECTOR GENERAL, CORPORATE INTEGRITY AGREEMENTS*, https://oig.hhs.gov/compliance/corporate-integrity-agreements/index.asp.

[14] *See* 70 Fed. Reg. 4858, 4875 (Jan. 31, 2005), *at* https://oig.hhs.gov/fraud/docs/complianceguidance/012705HospSupplementalGuidance.pdf; 63 Fed. Reg. 8987, 8989 (Feb. 23, 1998), https://oig.hhs.gov/authorities/docs/cpghosp.pdf; and 65 Fed. Reg. 59434, 59444 (Oct. 5, 2000) https://oig.hhs.gov/authorities/docs/physician.pdf.

[15] *See DEP'T OF HEALTH & HUMAN SERVICES, OFFICE OF THE INSPECTOR GENERAL, QUALITY OF CARE CORPORATE INTEGRITY AGREEMENTS*, https://oig.hhs.gov/compliance/corporate-integrity-agreements/quality-of-care.asp.

[16] *CORPORATE INTEGRITY AGREEMENTS*, *supra* note 13.

[17] *See DEP'T OF HEALTH & HUMAN SERVICES, OFFICE OF THE INSPECTOR GENERAL, CORPORATE INTEGRITY AGREEMENT DOCUMENTS*, https://oig.hhs.gov/compliance/corporate-integrity-agreements/cia-documents.asp.

[18] *See* 42 USC 1320a-7(f) and 42 CFR 1005.

[19] *See DEP'T OF HEALTH & HUMAN SERVICES, OFFICE OF THE INSPECTOR GENERAL, OIG GUIDANCE ON IRO INDEPENDENT AND OBJECTIVITY*, https://oig.hhs.gov/fraud/cia/docs/iro-guidance-2016.pdf; and *U.S GOV'T ACCOUNTABILITY OFFICE, GOVERNMENT AUDITING STANDARDS* (2011 REVISIONS), http://www.gao.gov/assets/590/587281.pdf.

[20] 5 USC 552.

[21] *See CORPORATE INTEGRITY AGREEMENT DOCUMENTS*, *supra* note 17.

[22] *See DEP'T OF HEALTH & HUMAN SERVICES, OFFICE OF THE INSPECTOR GENERAL, FOCUS ON COMPLIANCE: THE NEXT GENERATION OF CORPORATE INTEGRITY AGREEMENTS*, https://oig.hhs.gov/compliance/compliance-guidance/docs/Focus_on_Compliance.pdf.