



Health Care Compliance Association
Enforcement and Compliance Conference 2018

Anatomy of a Corporate Integrity Agreement

Felicia E. Heimer
Senior Counsel
Office of Counsel to the Inspector General

Judy A. Ringholz
Vice President of Compliance and Ethics, Chief Compliance Officer
Jackson Health System





Background on CIAs

- OIG enters into CIAs in connection with the settlement of health care fraud cases
 - False Claims Act (FCA)
 - Civil Monetary Penalties Law (CMPL)
- CIA in exchange for OIG’s release of its permissive exclusion authority
 - 1128(b)(7) (fraud, kickbacks and other prohibited activities)

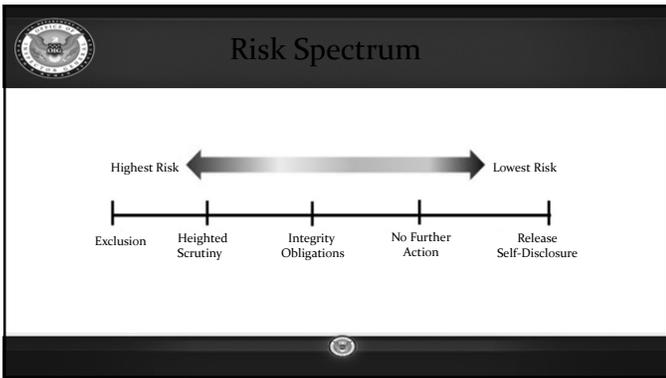




Section 1128(b)(7) Criteria

- Criteria for Implementing Section 1128(b)(7) Exclusion Authority, issued April 18, 2016
- Resolution of exclusion authority is based on assessment of future risk to the FHCPs.
- “Risk spectrum” from low to high risk based on: (1) nature and circumstances of conduct; (2) conduct during government investigation; (3) significant ameliorative efforts; and (4) history of compliance
- Highest risk will result in exclusion; below highest risk, OIG may require integrity obligations or take no further action





OIG's Fraud Risk Indicator

- OIG announced that in October 2018, it will begin publishing a list of individuals and entities it considers to pose a high-risk of healthcare fraud.
- These high-risk providers have refused to enter into corporate integrity agreements.
- Prior to the publication of this list, the provider and beneficiary community has been unable to know whether a settling entity belonged on the high-risk end of the spectrum—having refused to enter a CIA—or on the opposite end of the spectrum—having been determined by OIG to be low risk.
- The list provides transparency and information. It is not intended to change the manner in which providers operate.

Background on CIAs

There are benefits to operating under a corporate integrity agreement:

- Cultural change
- Mandated structure
- Formal reporting process
- Compliance Officer's heightened standing
- Increased resources
- Organizational interest in corporate compliance



Background on CIAs

What a CIA is: an agreement in which the provider agrees to implement the foundational elements of an effective compliance program and to comply with other requirements.

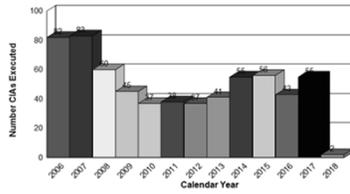
What a CIA is not: a mechanism through which all fraud may be detected or prevented.

- The CIA lays out what a compliance program must include. Providers may do more, but certainly should not do less.
- Examples of compliance obligations that go beyond standard CIA requirements:
 - Refined use of analytics (public and internal data) to assess risk
 - Survey instruments
 - Connecting compensation and compliance
 - Engaging all areas of the business in the compliance process



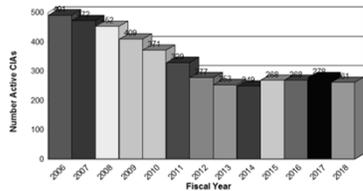


Number of New CIAs



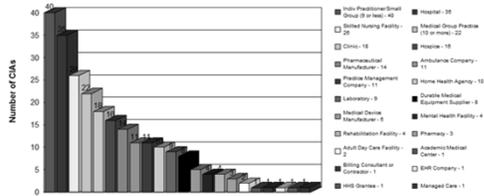


Number of Active CIAs





CIA by Subject Type





CIA Requirements

- All CIAs contain the same basic terms.
- Specific provisions and obligations may be tailored to the underlying conduct in the FCA case, the provider type, or to address other concerns by OIG.
 - Billing Fraud
 - Kickbacks or improper referral relationships
 - Medical Necessity
 - Failure of care/provision of worthless or poor-quality services
- OIG is not restricted by the underlying conduct in requiring specific compliance provisions under the CIA



CIA Term

- CIAs have a 5 year term
- IAs have a 3 year term
- Terms may be extended



Standard CIA Elements

- Compliance Officer
- Compliance Committee
- Management and Board Obligations
- Written Standards
- Training and Education





Standard CIA Elements

- Review Procedures
 - Claims Review
 - Arrangements Review
- Screening for Ineligible Persons
- Risk Assessment





Standard CIA Elements

- Notification of Government Investigations
- Overpayments
- Reportable Events
- Implementation Report/Annual Reports
- Breach and Default Provisions
 - Stipulated Penalties
 - Exclusion for Material Breach





IRO/Monitor

Independent Review Organization (“IRO”)

- Selected by provider with approval of OIG
- Billing Review and Oversight
- Legal/Financial Arrangements Oversight

Independent Monitor

- Selected by the OIG, paid by entity
- Performs Quality Reviews or other Specific Reviews
- Broad Access, Independent Authority
- May conduct independent investigations





Recent Developments

- Board Compliance Obligations
 - Review and Oversight
 - Submit Description of Materials Reviewed
 - Resolution
 - Training
 - Compliance Expert





Expanded Board Requirements

- “The Board of Directors has made a reasonable inquiry into the operations of [Provider]’s Compliance Program, including the performance of the Compliance Officer and the Compliance Committee. Based on its inquiry and review, the Board has concluded that, to the best of its knowledge, [Provider] has implemented an effective Compliance Program to meet Federal health care program requirements and the requirements of this CIA.”





Management Certifications

"I have been trained on and understand the compliance requirements and responsibilities as they relate to [insert name of department], an area under my supervision. My job responsibilities include ensuring compliance with regard to the [insert name of department] with all applicable Federal health care program requirements, obligations of the Corporate Integrity Agreement, and [Provider] policies, and I have taken steps to promote such compliance. To the best of my knowledge, the [insert name of department] of [Provider] is in compliance with all applicable Federal health care program requirements and the obligations of the Corporate Integrity Agreement. I understand that this certification is being provided to and relied upon by the United States."





CEO Certification

- The CEO must certify:
- to the best of his or her knowledge, except as otherwise described in the report, [Provider] has implemented and is in compliance with all of the requirements of this CIA;
 - he or she has reviewed the report and has made reasonable inquiry regarding its content and believes that the information in the report is accurate and truthful; and
 - he or she understands that the certification is being provided to and relied upon by the United States.





Risk Assessment and Internal Review Process

- Providers are required to:
- Identify and prioritize risks
 - Develop work plans related to identified risks
 - Implement work plans
 - Ensure that corrective action plans are developed in response to audits
 - Track implementation of corrective action plans





Claims Reviews

- Eliminated discovery sample/full sample and error rate threshold
- Review sample of paid claims for medical necessity, appropriate documentation, coding, and billing
- For any paid claim that results in an overpayment, IRO to review systems and processes and identify problems and weaknesses





Claims Reviews

- Repayment of identified overpayments
- Evaluate claims review results under CMS overpayment rule to determine if repayment of extrapolated overpayment is required
- Claims review report must provide an estimate of the actual overpayment in the population at the midpoint





IRO Requirements

- Must assign licensed nurses or physicians with relevant education, training, and specialized expertise to make the medical necessity determinations
- Provider must ensure that IRO has access to all records and personnel necessary to complete the required reviews





Risk-Based Claims Review

- OIG may limit the population to one or more subsets of paid claims
- Provider or IRO may submit proposals for the subsets of paid claims to be reviewed
- OIG also may select facilities that will be subject to the claims review





Other Recent Developments

- Provider-Specific Claims Reviews
 - Hospice
 - MDS Review
- Quarterly Claims Reviews in IAs
 - 30 paid claims per quarter
 - Repay identified overpayments and evaluate sample results under 60 day rule
 - IRO must identify actual overpayment in the population at the midpoint





Other Recent Developments

- Independent Monitor requirements in non-quality of care cases
- First of its kind CIA with electronic health record software developer to assess the quality and safety of the product





OIG Oversight & Monitoring

- CIAs permit the OIG to have inspection, audit, and review rights.
- Many entities under CIAs have one or multiple onsite visits and inspections by the OIG (routine, non-routine).





Common Site Visit Inquiries

- Information to validate Compliance Officer's standing and authority within the organization
- Disclosure Log and underlying investigation or review reports
- Dedication of resources to compliance program
- Assessment of compliance "placement" within the organizational structure
- Details of communication between Compliance Officer and Board of Directors
- Compliance Committee Meeting Minutes
- History of development and implementation of corrective action plans





CIA Enforcement

CIAs have breach and default provisions.

Stipulated Penalties (Monetary Penalties):

- Failure to use an IRO
- Failure to submit Implementation/Annual Reports
- Failure to identify Unallowable Costs
- Failure to grant the OIG access for investigation
- False Certification
- Failure to adhere to the terms of the applicable CIA





CIA Enforcement

Exclusion for Material Breach:

- Repeated or Flagrant Violations of the CIA;
- Failure to report a Reportable Event;
- Failure to pay Stipulated Penalties;
- Failure to comply with the Board Expert, IRO, and/or Independent Monitor provisions.





CIA Enforcement

- CMPL settlements of Reportable Event disclosures
 - Employment of excluded individuals
 - Kickbacks and self-referral violations
 - Improper billing
- <https://oig.hhs.gov/fraud/enforcement/cmp/reportable-events.asp>





Negotiable Terms

- CIAs are standardized and many provisions are non-negotiable, in order to “level the playing field” across entities operating under CIAs.
- CIA provisions may be negotiated to reflect the specific structure and/or operations of an organization.
- Scope of IRO Review in Claims Reviews
- Required certifications “although certifications will be required, the source of the certifications may be negotiable.”
- Opportunities to work with OIG monitor to address any changing or evolving issues throughout the term of the CIA.