Corporate Integrity Agreements: Practical Impact and Lessons Learned
Steve Nickelsburg and Adam Klauder – October 2014
Agenda

Overview 3
Other Enforcement Mechanisms 15
Recent Trends 18
Lessons Learned 26
What is a Corporate Integrity Agreement?

Corporate Integrity Agreements (CIAs) are agreements between (1) the Office of Inspector General (OIG) of the U.S. Department of Health and Human Services (HHS) and (2) health care providers and other entities that resolve U.S. Federal health care program investigations arising under a variety of civil false claims statutes.

In exchange for providers or entities agreeing to the obligations under a CIA, OIG agrees not to seek exclusion from participation in Medicare, Medicaid, or other U.S. Federal health care programs.

OIG uses CIAs to ensure that health care providers and other entities implement effective compliance programs going forward and to prevent a recurrence of improper practices.

CIAs provide a roadmap to OIG’s current view of best practices for corporate compliance programs.
Overview of a CIA

CIAs are **negotiated** agreements between OIG and providers/entities that are under investigation.

- CIAs are not administered by a court or a law enforcement authority.
- OIG administers CIAs using the administrative process (i.e., CIAs are not “criminal” settlements, although they may be referenced in parallel criminal resolutions).
- Typical term is 5 years.

Most CIAs contain common elements, but each is **tailored** to the provider/entity and the specific conduct investigated.

- Providers/entities can and should advocate for favorable terms.

Many CIAs require monitoring by an Independent Review Organization (IRO) or other compliance monitor.

- IROs/Monitors serve as OIG’s “eyes on the ground” and periodically report to OIG regarding the status of compliance with the CIA.
Legal Authorities

OIG imposes CIAs under its general authority to detect and prevent fraud, waste, abuse, and violations of law. (see The Inspector General Act of 1978 (5 U.S.C. App))

CIAs are often imposed in connection with the settlement of health care program investigations arising under a variety of civil false claims statutes (e.g., violations of the False Claims Act (FCA))

The underlying allegations often implicate other U.S. Federal health care laws, such as the:

- Federal Food, Drug, and Cosmetic Act
- Federal Anti-Kickback Statute
- “Stark” Anti-Referral Laws
- Medicare/Medicaid Fraud Statutes
- Statutes prohibiting false statements to regulators
Legal Authorities (continued)

OIG works with the U.S. Department of Justice (DOJ) on healthcare investigations.

- But, OIG has the exclusive authority to negotiate, sign and administer CIAs.
- OIG has the authority to exclude individuals and entities from Federally funded health care programs.

In determining whether to file or defer criminal charges against a provider/entity, DOJ often considers whether a CIA is in place.

- CIAs are often part of a "global settlement" among various enforcement authorities to resolve civil and/or criminal investigations.

Non-compliance with CIAs can have serious consequences.

- Monetary penalty provisions.
- Potential that breaches may constitute new False Claims Act violations.
Factors OIG Will Consider

OIG has published the criteria it considers when determining whether to impose a CIA:

- Did the provider self-disclose the alleged misconduct?
- What was the monetary damage to Federal health care programs?
- Did the case involve successor liability?
- Is the provider still participating in the Federal health care programs or in the line of business that gave rise to the conduct?
- Is the alleged conduct capable of repetition?
- When did the conduct occur?
- Does the provider have an effective compliance program?
- Would the provider agree to limited compliance or integrity measures and would it annually certify such compliance to the OIG?
  - see, e.g., OIG-HHS, Open Letter to Health Care Providers (Nov. 20, 2001).
Terms of a CIA

CIAs contain many standard terms and provisions, which are enhanced with more specific terms that reflect the conduct at issue and remediation required.

Term and Scope

- Generally 5 years
- “Covered Persons”

Corporate Integrity Obligations

- Requirement to establish and maintain a compliance program
  - Covers the elements of an effective compliance program from the Federal Sentencing Guidelines
- Information on compliance responsibilities of certain personnel (Compliance Officer, Compliance Committee, etc.)
- Written standards (Code of Conduct and polices)
- Training and education requirements
Terms of a CIA (continued)

Independent Monitor
- Independent Review Organization (IRO)

Disclosure Program
- Confidentiality; anti-retaliation provisions

Ineligible Person
- Details types of persons that must be excluded from dealing with the provider

Reporting
- Overpayments, reportable events, and ongoing investigations/legal proceedings

Implementation and Annual Reports
- Reporting requirements to inform the OIG on the status of the entity’s compliance activities
Who is a “Covered Person”?

Definitions of “covered persons” and “relevant covered persons” are set forth in all CIAs

- Identify which individuals and entities are subject to CIA requirements
- "Covered persons" include the company, its subsidiaries or affiliates, employees, and contractors who perform certain functions on behalf of the entity. All receive basic training.
- "Relevant covered persons" have specific responsibility for the programs at issue and must receive specialized training on defined subject areas.

Confusion over who is covered

- Vendors and contractors?
- Risk that companies “over-train” to ensure that they do not breach the CIA requirements

Definitions may be tailored through negotiation

Example:
Merck’s 2011 CIA contains a carve-out for employees and others of the company’s manufacturing, animal health, and consumer products divisions, and individuals from Merck Research Laboratories, so long as they do not perform certain specified functions
Independent Review Organizations (IROs)

IROs are accounting, auditing, or consulting firms that have expertise in billing, coding, reporting, and other requirements of the U.S. Federal health care program at issue.

- IROs evaluate the effectiveness of corporate compliance programs.
- Chosen (and paid for) by the providers/entities, not OIG
  - OIG reserves the right to approve/reject the choice

OIG “independence” and “objectivity” requirements

- “Objectivity” includes “avoiding conflicts that may, in fact or appearance, impair auditors’ objectivity in performing the audit or attestation engagement is essential to retaining credibility.”
- “Independence” has two main principles:
  - “audit organizations must not provide nonaudit services that involve performing management functions or making management decisions” and
  - “audit organizations must not audit their own work or provide nonaudit services in situations where the nonaudit services are significant or material to the subject matter of the audits.”
Things to consider when engaging an IRO

- Ensure that the IRO does not have any conflicts of interest, and that it meets the Government Accountability Office's "Generally Accepted Government Audit Standards"
- The IRO should have substantive experience in the areas that are within the scope of the CIA; try to avoid hiring multiple IROs
- Firms that have served as IROs several times have credibility with OIG and can better help guide companies through the process in an efficient manner.
- Assign a point person within the provider/entity to manage the IRO relationship; helps avoid inefficiencies
- Be prepared for time consuming and resource draining requests for data and document collection
- Costs/fees
Independent Review Organizations (IROs) (continued)

What do IROs do? Scope of review is set forth in the CIA – includes:

**Arrangements Review**
- Focuses on arrangements with referral sources (e.g., physicians) and arrangements entered into by a health care provider/entity with other health care providers, practitioners, suppliers, and vendors.

**Performance/Claims Review**
- Focuses on accuracy of claims to U.S. Federal healthcare programs with respect to specific transactions.
- Begins with initial "discovery sample".
- Additional sampling and Systems Review may be required if error rate is too high.

**Systems Review**
- Review of systems, processes, policies, and procedures to track, monitor and verify claims, arrangements, pricing, and marketing and sales activities.
Compliance Program

If a company does not have an effective compliance program, OIG will require one to be implemented.

The elements of an effective compliance program include:

- Written policies and procedures
- Designation of compliance officers and compliance committee
- Effective training and education
- Effective lines of communication between compliance function and employees
- Enforcement of standards through well-publicized disciplinary guidelines
- Auditing and monitoring
- Responding to detected offenses and taking necessary corrective action
  - See, e.g., OIG Compliance Program Guidance for Pharmaceutical Manufacturers
Other Enforcement Mechanisms
Deferred Prosecution Agreements (DPAs)

A DPA is a voluntary alternative to trial under which the prosecutor agrees to defer prosecution for a period of time. Assuming cooperation and no further misconduct the complaint is dismissed at the end of that period.

- Defendants are required to fulfill certain requirements including the payment of fines, implementation of corporate reforms and in some cases, appointment of an independent monitor to oversee compliance.
- Generally the DOJ files criminal charges in court against the corporation but agrees to waive the charges once the corporation meets the terms of the DPA.
- The terms of a corporate DPA typically include new or enhanced compliance and reporting measures, an agreement to cooperate with the ongoing investigation, an admission of wrongful conduct, internal reforms and restitution payments.
- These agreements usually span several years.
Non-Prosecution Agreements (NPAs)

An NPA is similar to a DPA in that the DOJ and corporate defendant enter into an agreement wherein the corporation agrees to cooperate with the government and take remedial actions to correct the wrongdoing.

- However, no charges are filed against the defendant so long as there is no breach in the agreement.
- An NPA does not typically require an admission of wrongdoing.
- In addition, NPAs are generally less detailed than DPAs and do not require a corporate monitor.
Recent Trends
Trends – Overview

- Expansion of Board of Director oversight requirements
- Additional obligations for executives to “certify compliance”
- Increased oversight of non-promotional activities (e.g., research-related activities, medical education grants)
- Divestiture as a way to avoid exclusion
- Clawbacks / financial recoupment
Compliance obligations for Boards of Directors are not new, but there has been a shift in tone as OIG seeks to make Boards more proactive participants in compliance oversight

- Increased personal accountability for individuals who set the “tone at the top”

Oversight responsibilities for Board Members include:

- Quarterly Board meetings regarding the compliance program.
- Periodic Chief Compliance Officer reports to the Board.
- Annual resolution, signed by each Board member, summarizing review and oversight of compliance with U.S. Federal health care programs and the CIA.
- Board certification that it has made a reasonable inquiry into the operations of the compliance program and, based on its inquiry, the Board concludes that, to the best of its knowledge, the company has implemented an effective compliance program.
Trends – Executives and Managers

“Certifying Employees” must monitor and annually certify that their unit(s) are compliant with federal health care program requirements, FDA requirements, and the obligations of the CIA.

- Includes presidents, vice-presidents, business unit heads, etc.

Typical certifications include affirmation that:

- They have been trained on and understand compliance requirements related to their area of responsibility.
- Their job duties include ensuring compliance within those areas.
- That they have taken steps to promote compliance.
- They have referred any issues of potential noncompliance in accordance with the company’s reporting processes/procedures.
- Other than the referred issues, they are not aware of any violations of applicable U.S. Federal health care program requirements, obligations of the CIA, or company policies.
Trends – Monitoring and Management of Non-Promotional Activities

CIAs have imposed compliance measures focused on systems and controls for non-promotional activities that have the potential for compliance risk.

- Consultant arrangement activities
- Research-related activities
- Publication activities
- Medical educational grants
Practical examples from recent CIAs include:

- Use of written agreements describing the scope of the work, fees paid, and compliance obligations.
- Fees must be determined according to a centrally managed, pre-set rate structure based on a fair market value analysis.
- Establishment of an annual budget (approved by the company’s compliance team) that considers business and scientific need justifications.
- Needs assessments justifying the activities.
- Monitoring/auditing of arrangements with healthcare professionals, consultants, etc.
  - Auditing selections made on both a risk-based and sampling approach
  - Focus on whether activities were supported/performed consistent with company policies and procedures
- For medical education grants, establishment of a “grants management system”
  - Prevents sales/marketing employees from having involvement in the awarding of grants
- Transparency and public disclosure requirements (grants, charitable contributions, etc.)
Trends – Divestiture as a Way to Avoid Exclusion

Material breach of a CIA provides the basis for OIG to seek exclusion

Providers/entities are given an opportunity to cure the breach (typically 30 days)

In 2012, Church Street Health Management (CSHM) was required by OIG to divest its subsidiary in order to cure a breach of its CIA

- OIG issued Notice of Material Breach and Intent to Exclude Notice to CSHM
- CSHM was unable to resolve all of the breaches within the cure period
- OIG required CSHM to divest a subsidiary as a condition for the parent to avoid exclusion.

Potential for OIG to require companies to divest product lines in order to cure a breach?
In 2012, GlaxoSmithKline (GSK) entered into a $3 billion settlement to resolve criminal and civil liability regarding its pharmaceutical sales, marketing, and contracting practices.

The CIA is notable for many reasons, including the establishment of a "clawback" mechanism (formally called the "Executive Financial Recoupment Program"):

- Potential for forfeiture and recoupment of an amount equivalent to up to three years of annual performance pay (annual bonus, plus long term incentives) for any GSK executive who is discovered to have been involved in any significant misconduct.
- Applies to all members of GSK’s corporate executive team and to any vice presidents and senior vice presidents who are based in the U.S. who are current GSK employees or former GSK employees at the time of a Recoupment Determination.
Lessons Learned

Ensure that internal compliance and disclosure systems are properly designed and functioning

- “Tone from the top” is important in creating a “culture of compliance”
- Detection and prevention of wrongdoing can lead to reduced obligations and possibly the need for a CIA
- Responsive and confidential reporting systems encourage buy-in from all employees

Review and update policies and procedures annually using a risk-based approach:

- Take into consideration any risk mitigation or identification programs required by the OIG or undertaken voluntarily by the company
- Demonstrates a focus on best practices and a proactive approach to identifying challenges and new risks
Lessons Learned (continued)

Retrain employees to ensure that concerns, confusion or questions about compliance are adequately addressed

- Online testing and surveys and internal compliance hotlines are one way to measure the impact of employee understanding of policies and procedures
- Companies also need to engage employees with interactive ways to communicate concerns that are potential CIA violations

Revisit polices about documentation related to compliance

- Because CIA documentation may become public, companies should establish best practices for compliance-related document creation to ensure that documented compliance issues or internal responses are appropriate
- Compliance officers and in-house and outside counsel must be prepared to explain and describe to government agencies how internal compliance officers identified compliance infractions or deviations and corrected such violations
Lessons for Boards

- Emphasize individual accountability at the executive and board levels.
- Measure compliance programs against expectations reflected in CIAs, the Federal Sentencing Guidelines and (to a lesser extent) the DOJ Principles of Federal Prosecution of Business Corporations.
- Tailor provisions to the organization’s specific profile, risks and challenges, and avoid a “check the box” approach to compliance structure and implementation.
  - Periodic, board-directed compliance plan updates and refinement.
- The positions of general counsel and compliance officer should be separate and held by different individuals.
  - The compliance officer should (1) be independent and protected from executive level conflict of interest, (2) have appropriate reporting relationships with the CEO and the board, and (3) be positioned as a member of senior management.
- Include achievement of compliance-related targets within executive and management-level incentive and compensation arrangements.
- Ensure adequate staffing and funding for legal, compliance and ethics programs.
- Periodically evaluate the effectiveness of internal whistleblower/“hotline” programs and related organizational responses.
Worldwide contact information
36* offices in 24 countries

Abu Dhabi
Clifford Chance
9th Floor
Al Sila Tower
Sowwah Square
PO Box 26492
Abu Dhabi
United Arab Emirates
Tel +971 (0)2 613 2300
Fax +971 (0)2 613 2400

Amsterdam
Clifford Chance
Droogbak 1A
1013 GE Amsterdam
PO Box 251
1000 AG Amsterdam
The Netherlands
Tel +31 20 7119 000
Fax +31 20 7119 999

Bangkok
Clifford Chance
Sindhorn Building Tower 3
21st Floor
130-132 Wireless Road
Pathumwan
Bangkok 10330
Thailand
Tel +66 2 401 8800
Fax +66 2 401 8801

Barcelona
Clifford Chance
Av. Diagonal 682
08034 Barcelona
Spain
Tel +34 93 344 22 00
Fax +34 93 344 22 22

Beijing
Clifford Chance
33/F, China World Office 1
No. 1, Jiangguangmenwai Daje
Chaoyang District
Beijing 100004
China
Tel +86 10 6535 2288
Fax +86 10 6505 9028

Brussels
Clifford Chance
Avenue Louise 65 Box 2
1055 Brussels
Belgium
Tel +32 2 533 5911
Fax +32 2 533 5959

Bucharest
Clifford Chance Badea
Excelsior Center
28-30 Academiei Street
12th Floor, Sector 1
Bucharest, 010016
Romania
Tel +40 21 66 66 100
Fax +40 21 66 66 111

Casablanca
Clifford Chance
169, boulevard Hassan 1er
Casablanca 20000
Morocco
Tel +212 520 132 080
Fax +212 520 132 079

Doha
Clifford Chance
QFC Branch
Suite B, 30th floor
Tornado Tower
Al Fudanq Street
West Bay PO Box 32110
Doha
State of Qatar
Tel +974 4491 7040
Fax +974 4491 7050

Dubai
Clifford Chance
Building 6, Level 2
The Gate Precinct
Dubai International Financial Centre
PO Box 9380
Dubai
United Arab Emirates
Tel +971 4 362 0444
Fax +971 4 362 0445

Düsseldorf
Clifford Chance
Königsallee 59
40215 Düsseldorf
Germany
Tel +49 211 40 55 0
Fax +49 211 43 55-5600

Frankfurt
Clifford Chance
Mainzer Landstrasse 46
60325 Frankfurt am Main
Germany
Tel +49 69 71 99-01
Fax +49 69 71 99-4000

Hong Kong
Clifford Chance
27th Floor
Jardine House
One Connaught Place
Hong Kong
Tel +852 2852 8888
Fax +852 2825 8800

Istanbul
Clifford Chance
Kanyon Ofis Binasi Kat 10
Boşbakan Cadd. No. 185
34394 Levent
Istanbul
Turkey
Tel +90 212 339 0001
Fax +90 212 339 0098

Jakarta
Linda Widyati & Partners
DBS Bank Tower,
28th Floor, Citiputra World One
Jl. Prof. Satrio Kav 3-5
Jakarta 12940
Indonesia
Tel +62 21 2988 8300
Fax +62 21 2988 8310

Kiev
Clifford Chance
75 Zhylanska Street
01032 Kyiv
Ukraine
Tel +380 44 390 5885
Fax +380 44 390 5886

Kyiv
Clifford Chance
75 Zhylanska Street
01032 Kyiv
Ukraine
Tel +380 44 390 5885
Fax +380 44 390 5886

London
Clifford Chance
10 Upper Bank Street
London, E14 4JX
United Kingdom
Tel +44 20 7006 1000
Fax +44 20 7006 5555

Luxembourg
Clifford Chance
10 boulevard G.D. Charlotte
B.P. 1147
L-1011 Luxembourg
Grand-Duché de Luxembourg
Tel +352 48 50 50 1
Fax +352 48 13 85

Munich
Clifford Chance
Theresienstrasse 4-6
80333 Munich
Germany
Tel +49 89 216 32-0
Fax +49 89 216 32-6000

New York
Clifford Chance
31 West 52nd Street
New York, NY 10019-6131
USA
Tel +1 212 878 8000
Fax +1 212 878 8375

Paris
Clifford Chance
9 Place Vendôme
CS 5018
75038 Paris Cedex 01
France
Tel +33 1 44 05 52 52
Fax +33 1 44 05 52 00

Perth
Clifford Chance
Level 7, 190 St Georges Terrace
Perth, WA 6000
Australia
Tel +61 8 9262 5555
Fax +61 8 9262 5522

Prague
Clifford Chance
Jungmannova Plaza
Jungmannova 24
110 00 Prague 1
Czech Republic
Tel +420 222 555 222
Fax +420 222 555 000

Riyadh
Clifford Chance
Building 15, The Business Gate
King Khaled International Airport Road
Cordoba District, Riyadh
P.O. Box: 90239, Riyadh 11163,
Kingdom of Saudi Arabia
Tel +966 11 481 9700
Fax +966 11 481 9701

Sydney
Clifford Chance
Level 16
No. 1, 0’Connell Street
Sydney NSW Australia
Tel +61 2 8922 8000
Fax +61 2 8922 8088

Tokyo
Clifford Chance
Akasaka Tameike Tower, 7th Floor
1-7-7 Akasaka 2-Chome
Minato-ku, Tokyo 107-0052
Japan
Tel +81 3 5561 6600
Fax +81 3 5561 6699

Washington, D.C.
Clifford Chance
2001 K Street NW
Washington, DC 20006-1001
USA
Tel +1 202 912 5000
Fax +1 202 912 6000

* Clifford Chance’s offices include a second office in London at 4 Coleman Street, London EC2R 5JH.
** Linda Widyati & Partners in association with Clifford Chance.